STRATEGY OF THINGS

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

January 2025

Funded by a Cooperative Agreement from

National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Prepared by

Strategy of Things
Benson Chan
Renil Paramel
Christopher Reberger

Check for updates

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

NIST GCR 25-059
https://doi.org/10.6028/nist.gcr.25-059

January 2025

Funded by a Cooperative Agreement from

National Institute of Standards and Technology
100 Bureau Drive
Gaithersburg, MD 20899

Prepared by

Strategy of Things
Benson Chan
Renil Paramel
Christopher Reberger

Table of Contents

Acknowledgements xv
Executive Summary EX-1
1. Introduction 1
1.1. Purpose and overview 1
1.2. Research objectives 2
2. Research Approach 3
2.1.1. 25 Technology gap collection framework 4
2.1.2. Economic modeling approach 5
2.1.3. Portfolio Approach 9
3. High Level Findings Mapped to Objectives 11
4. The Internet of Things (IoT) 16
4.1.1. IoT technology stack 17
4.1.2. Economic benefits of IoT 18
4.2. State of IoT 21
4.2.1. IoT evolution 22
4.2.2. IoT evolution drivers and enablers 24
4.2.3. Emerging IoT trends driving IoT evolution 29
5. Technology and Non-Technology Challenges 34
5.1. Technology challenges 34
5.2. Non-Technology challenges 40
5.3. Industry findings 44
5.3.1. Agriculture 45
5.3.2. Manufacturing 48
5.3.3. Construction 51
5.3.4. Insurance 54
5.3.5. Smart Cities 57
5.3.6. Transportation and Logistics 60
5.3.7. Healthcare 63
5.3.8. Retail 67
5.3.9. Renewable Energy 70
6. IoT Technology Infrastructure Gaps 75
6.1. Core gaps 77

© Strategy of Things, 2025. All rights reserved.

6.1.1. Core: Interoperability 77
6.1.2. Core: Cybersecurity 79
6.1.3. Core: Privacy 85
6.1.4. Core: Connectivity 87
6.2. Intelligence gaps 92
6.2.1. Intelligence: Data management 93
6.2.2. Intelligence: AI Trust 95
6.2.3. Intelligence: Intelligent device capabilities 97
6.3. Hyper-Deployed gaps 99
6.3.1. Hyper-Deployed: Enabling an IoT data ecosystem 100
6.3.2. Hyper-Deployed: Communications and network infrastructure 101
6.3.3. Hyper-Deployed: Advanced computing paradigms 106
6.3.4. Hyper-Deployed: Facilitating human centric IoT systems 108
7. Economic Analysis of Gaps 112
7.1.1. Public sector technology investments 113
7.1.2. Surplus estimates by single technology component 113
7.1.3. Surplus estimates by core and intelligence gaps 118
8. Opportunities for Government 124
8.1. IoT Considerations for policymakers 125
8.2. Framework for IoT policymaking 126
8.3. Government opportunities to address key gaps 128
8.3.1. Government opportunities: Core gaps 129
8.3.2. Government opportunities: Intelligence gaps 134
8.3.3. Government opportunities: Hyper-Deployed gaps 139
8.4. Implications for government leaders and policymakers 142
8.4.1. Government opportunities 142
9. Recommendations 147
10. Conclusion 152
11. Appendix: The Internet of Things 11-1
11.1. Introduction 11-1
11.2. IoT examples 11-2
11.3. IoT product and service opportunities 11-2
11.4. IoT technologies 11-4
11.4.1. Devices and things 11-5

© Strategy of Things, 2025. All rights reserved.

11.4.2. Connectivity and gateway components 11-5
11.4.3. Messaging protocols 11-5
11.4.4. Platform components 11-6
11.4.5. Presentation components 11-6
11.5. IoT classifications 11-7
12. Appendix: Appendices Structure 12-1
13. Appendix: Agriculture 13-1
13.1. Industry overview 13-1
13.1.1. Key facts 13-1
13.1.2. Industry challenges 13-2
13.2. IoT in the agriculture industry 13-5
13.2.1. IoT use cases 13-7
13.2.2. Market views of IoT in agriculture 13-13
13.3. IoT gaps and findings in agriculture 13-15
13.3.1. Top technology challenges 13-15
13.3.2. Other challenges 13-24
14. Appendix: Manufacturing 14-1
14.1. Industry overview 14-1
14.1.1. Key facts 14-1
14.1.2. Industry challenges 14-2
14.2. IoT in the manufacturing industry 14-6
14.2.1. IoT use cases 14-6
14.2.2. Market views of IoT in manufacturing 14-13
14.3. IoT gaps and findings in manufacturing 14-14
14.3.1. Top technology challenges 14-15
14.3.2. Other challenges 14-22
15. Appendix: Construction 15-1
15.1. Industry overview 15-1
15.1.1. Key facts 15-1
15.1.2. Industry challenges 15-2
15.2. IoT in the construction industry 15-5
15.2.1. IoT use cases 15-6
15.2.2. Market views of IoT in construction 15-13
15.3. IoT gaps and findings in construction 15-15

© Strategy of Things, 2025. All rights reserved.

15.3.1. Top technology challenges 15-15
15.3.2. Other challenges 15-18
16. Appendix: Insurance 16-1
16.1. Industry overview 16-1
16.1.1. Key facts 16-1
16.1.2. Industry challenges 16-2
16.2. IoT in the insurance industry 16-6
16.2.1. IoT use cases 16-8
16.2.2. Market views of IoT in insurance 16-12
16.3. IoT gaps and findings in insurance 16-14
16.3.1. Top technology challenges 16-14
16.3.2. Other challenges 16-21
17. Appendix: Cities 17-1
17.1. Industry overview 17-1
17.1.1. Key facts 17-1
17.1.2. Industry challenges 17-3
17.2. IoT in Cities 17-17
17.2.1. IoT use cases 17-18
17.2.2. Market views of IoT in cities 17-28
17.3. IoT gaps and findings for cities 17-29
17.3.1. Top technology challenges 17-30
17.3.2. Other challenges 17-40
18. Appendix: Transportation and Logistics 18-1
18.1. Industry overview 18-1
18.1.1. Key facts 18-1
18.1.2. Industry challenges 18-2
18.2. IoT in the transportation and logistics industry 18-14
18.2.1. IoT use cases 18-16
18.2.2. Market views of IoT in transportation and logistics 18-26
18.3. IoT gaps and findings in transportation and logistics 18-28
18.3.1. Top technology challenges 18-29
18.3.2. Other challenges 18-38
19. Appendix: Healthcare 19-1
19.1. Industry overview 19-1

© Strategy of Things, 2025. All rights reserved.

19.1.1. Key facts 19-1
19.1.2. Industry challenges 19-4
19.2. IoT in the healthcare industry 19-20
19.2.1. IoT use cases 19-22
19.2.2. Market views of IoT in healthcare 19-29
19.3. IoT gaps and findings in healthcare 19-31
19.3.1. Top technology challenges 19-32
19.3.2. Other challenges 19-41
20. Appendix: Retail 20-1
20.1. Industry overview 20-1
20.1.1. Key facts 20-1
20.1.2. Industry challenges 20-2
20.2. IoT in the retail industry 20-8
20.2.1. IoT use cases 20-11
20.2.2. Market views of IoT in retail 20-17
20.3. IoT gaps and findings in retail 20-19
20.3.1. Top technology challenges 20-20
20.3.2. Other challenges 20-28
21. Appendix: Renewable Energy 21-1
21.1. Industry overview 21-1
21.1.1. Key facts 21-1
21.1.2. Industry challenges 21-2
21.2. IoT in the renewable energy industry 21-12
21.2.1. IoT use cases 21-13
21.2.2. Market views of IoT in renewable energy 21-20
21.3. IoT gaps and findings in renewable energy 21-20
21.3.1. Top technology challenges 21-21
21.3.2. Other challenges 21-31
22. Appendix: IoT evolution 22-1
22.1. Four stages of IoT evolution 22-1
22.1.1. Stage 1: “Things” become smart 22-1
22.1.2. Stage 2: AI algorithms take action 22-2
22.1.3. Stage 3: Utilities and outcomes 22-2
22.1.4. Stage 4: Hyperconnected autonomy 22-2

© Strategy of Things, 2025. All rights reserved.

22.2. IoT evolution drivers and enablers 22-3
22.2.1. Interoperability and standards 22-4
22.2.2. Ubiquitous connectivity 22-5
22.2.3. Ubiquitous computing 22-5
22.2.4. Trustworthy IoT 22-6
22.2.5. Analytics and intelligence 22-6
22.2.6. Convergence of IT, OT and enterprise systems 22-7
22.2.7. Policies and regulations 22-7
22.2.8. Innovative businesses and operating models 22-8
22.3. Emerging IoT trends 22-8
22.3.1. Emergence of the edge 22-9
22.3.2. Development of "low code" and "no code" software tools 22-10
22.3.3. Increased open-source IoT ecosystem of users and developers 22-10
22.3.4. Developing cybersecurity standards and regulations for IoT 22-12
22.3.5. Next generation satellite IoT connectivity services 22-14
22.3.6. Rollout of 5G will accelerate and enable IoT 22-15
22.3.7. AI and machine learning capable IoT devices 22-17
22.3.8. Energy harvesting technologies deployed 22-17
22.3.9. Adoption of digital twin models 22-18
23. Appendix: Cross industry Gaps Analysis 23-1
23.1. Core 23-4
23.1.1. Core: Interoperability 23-4
23.1.2. Core: Cybersecurity 23-7
23.1.3. Core: Privacy 23-15
23.1.4. Core: Connectivity 23-20
23.2. Intelligence Gaps 23-28
23.2.1. Intelligence: Data management 23-30
23.2.2. Intelligence: AI trust 23-33
23.2.3. Intelligence: Intelligent device capabilities 23-38
23.3. Hyper-Deployed gaps 23-40
23.3.1. Hyper-Deployed: Enabling an IoT data ecosystem 23-42
23.3.2. Hyper-Deployed: Communications and network infrastructure 23-43
23.3.3. Hyper-Deployed: Advanced computing paradigms 23-49
23.3.4. Hyper-Deployed: Facilitating human centric IoT systems 23-52

© Strategy of Things, 2025. All rights reserved.

24. Appendix: Government Opportunity to Address Gaps 24-1
24.1. IoT considerations for policymakers 24-2
24.2. Framework for IoT policymaking 24-3
24.2.1. Technology development 24-4
24.2.2. Commercial enablement 24-5
24.2.3. Facilitate market adoption 24-8
24.2.4. Lead by example 24-11
24.2.5. Broaden economywide benefits 24-13
24.3. Prior IoT studies 24-15
24.3.1. USA studies 24-15
24.3.2. EU studies 24-17
24.4. Government opportunities to address key gaps 24-18
24.4.1. Government opportunities: Core gaps 24-19
24.4.2. Government opportunities: Intelligence gaps 24-29
24.4.3. Government opportunities: Hyper-Deployed gaps 24-35
25. Appendix: Economic Analysis and Data Integration 25-1
25.1. Economic benefits of IoT for the United States 25-1
25.2. Data integration by industry 25-5
25.2.1. Classification presentation 25-5
25.2.2. Data integration 25-7
25.2.3. Agriculture 25-11
25.2.4. Manufacturing 25-20
25.2.5. Construction 25-30
25.2.6. Insurance 25-39
25.2.7. Smart Cities 25-49
25.2.8. Transport 25-57
25.2.9. Healthcare 25-65
25.2.10. Retail 25-74
25.2.11. Renewable Energy 25-83
26. Appendix: Qualitative and economic rankings 26-1
26.1. Ranking of qualitative issues 26-1
26.2. Ranking by economics and technology 26-1
26.3. Sensitivity analysis 26-2
26.4. Impact of $10 million investment in public R&D 26-3

© Strategy of Things, 2025. All rights reserved.

26.4.1. R&D to revenue 26-4
26.4.2. Gross margins..... 26-6
26.4.3. Surplus estimates by single technology component..... 26-8
26.4.4. Surplus estimates by identified core and intelligence gaps..... 26-11
27. Appendix: Acronyms and Initialisms..... 27-1

© Strategy of Things, 2025. All rights reserved.

Table of Figures

Figure 1: Research Objective 1 Findings EX-4
Figure 2: Research Objective 2 Findings EX-4
Figure 3: Research Objective 3 Findings EX-5
Figure 4: Research Objective 4 Findings EX-5
Figure 5: Top Technology Challenges by Industry. EX-6
Figure 6: Top Non-Technology Challenges by Industry. EX-7
Figure 7: IoT Technology Infrastructure Gaps by Category and Evolution Stage EX-8
Figure 8: Brief Description of IoT Technology Infrastructure Core Gaps. EX-9
Figure 9: Intelligence Gaps EX-10
Figure 10: Hyper-Deployed Gaps EX-12
Figure 11: Economic Impact of Investments in Most Important Single Technology Components EX-13
Figure 12: Revenue & Surpluses from a $10 million Public Sector Investment in Core and Intelligence Gaps Across All Industries EX-13
Figure 13: Revenue & Surpluses from a $10 million Public Sector Investment in Interoperability EX-14
Figure 14: Indicative Allocations by Gap of a $10 million Public Sector Investment EX-14
Figure 15: Government Opportunity Framework EX-16
Figure 2-1: Infrastructure Gaps Research Approach 3
Figure 2-2: Technology Taxonomy: 6 Categories and 25 Single Technology Components 5
Figure 2-3: Ranking Technology Gaps Schematic 6
Figure 2-4: Interviews Notes (Detail) 7
Figure 2-5: Desk Research (Detail) 7
Figure 2-6: Survey Detail Showing 25 Single Technology Components 8
Figure 2-7: Integrating Survey, Interview and Desk Research Data 8
Figure 2-8: Weighting and then Ranking IoT Technology Subcategories 9
Figure 2-9: A Portfolio Approach 10
Figure 4-1: Typical IoT Solution Architecture Model 17
Figure 4-2: Six Categories for 25 Single Technology Components 17
Figure 4-3: IoT Technology Stack (Non-Industry Specific) 18
Figure 4-4: IoT Differentiator for Products and Services 19
Figure 4-5: IoT Value by Industry and Allocation ($US bn) 20
Figure 4-6: U.S. IoT Value Estimates by Selected Industry ($US bn) 21
Figure 4-7: IoT Evolution Model 23
Figure 4-8: IoT Accelerators 25
Figure 5-1: Top Technology Infrastructure Challenges by Industry. 35
Figure 5-2: Top Non-Technology Challenges by Industry. 41
Figure 5-3: Agriculture: IoT Use Cases 46
Figure 5-4: Agriculture: Industry Challenges 47
Figure 5-5: Manufacturing: IoT Use Cases 49
Figure 5-6: Manufacturing: Industry Challenges 50
Figure 5-7: Construction: IoT Use Cases 52
Figure 5-8: Construction: Industry Challenges 53
Figure 5-9: Insurance: IoT Use Cases 55
Figure 5-10: Insurance: Industry Challenges 56
Figure 5-11: Smart City IoT Use Cases 58
Figure 5-12: Smart Cities: Industry Challenges 59
Figure 5-13: Transportation and Logistics: IoT Use Cases 61

© Strategy of Things, 2025. All rights reserved.

Figure 5-14: Transportation and Logistics: Industry Challenges 63
Figure 5-15: Healthcare: IoT Use Cases 65
Figure 5-16: Healthcare: Industry Challenges 66
Figure 5-17: Retail: IoT Use Cases 68
Figure 5-18: Retail: Industry Challenges 69
Figure 5-19: Renewable Energy IoT Use Cases 72
Figure 5-20: Renewable Energy: Industry Challenges 73
Figure 6-1: Overview of Process used to Identify Key Gaps 75
Figure 6-2: IoT Technology Infrastructure Gap Categories and Criteria 76
Figure 6-3: Cross industry IoT Technology Infrastructure Gaps by Category. 77
Figure 7-1: Ranking Confidence for the Four Most Important Single Technology Components 113
Figure 7-2: Public Sector Investment to Surplus 113
Figure 7-3: Economic Impact of Single Technology Component Investments 114
Figure 7-4: Investment Return for Hardware H-1 115
Figure 7-5: Investment Return for Standards Interoperability T-4 115
Figure 7-6: Investment Return for Software Data Collection S-3 116
Figure 7-7: Investment Return for Systems Security Y-3 116
Figure 7-8: Investment Allocations by Industry and Technology ($m). 117
Figure 7-9: Revenue and Surpluses from Public Sector Investment in Core and Intelligence Gaps 119
Figure 7-10: Impact of Public Sector Investment in Core: Interoperability 121
Figure 7-11: Impact of Public Sector Investment in Core: Privacy 121
Figure 7-12: Impact of Public Sector Investment in Core: Security 122
Figure 7-13: Impact of Public Sector Investment in Core: Connectivity 122
Figure 7-14: Impact of Public Sector Investment in Intelligence: Data Management 122
Figure 7-15: Impact of Public Sector Investment in Intelligence: Artificial Intelligence 123
Figure 7-16: Impact of Public Sector Investment in Intelligence: Intelligent Devices 123
Figure 8-1: Technology Diffusion 124
Figure 8-2: Government Opportunity Framework 127
Figure 8-3: Four Stage IoT Evolution 129
Figure 8-4: Core Gaps: Government Opportunities 130
Figure 8-5: Intelligence Gaps: Government Opportunities 135
Figure 8-6: Hyper-Deployed Gaps: Government Opportunities 140
Figure 11-1: IoT Architecture Overview 11-2
Figure 11-2: IoT Example: Manufacturing Opportunities 11-3
Figure 11-3: IoT Technology Stack (Non-Industry Specific) 11-4
Figure 11-4: IoT Single Technical Component Taxonomy 11-7
Figure 13-1: Agriculture: Use Case Categories and Representative Use Cases 13-8
Figure 13-2: Agriculture: Use Case and Industry Challenges Alignment 13-9
Figure 13-3: Agriculture: Use Case Details 13-12
Figure 13-4: Agriculture: Importance of IoT 13-13
Figure 13-5: Agriculture: Use Case Category Impact 13-14
Figure 13-6: Agriculture: Confidence in Suppliers Delivering 13-15
Figure 13-7: Agriculture: Top 10 Most Important Single Technologies 13-15
Figure 14-1: Manufacturing: Use Cases and Selected Use Cases 14-7
Figure 14-2: Manufacturing: Use Case and Industry Challenges Fit 14-9
Figure 14-3: Manufacturing: Use Case Details 14-12
Figure 14-4: Manufacturing: Importance of IoT 14-13
Figure 14-5: Manufacturing: Use Case Category Impact 14-14

© Strategy of Things, 2025. All rights reserved.

Figure 14-6: Manufacturing: Top 10 Most Important Single Technologies 14-15
Figure 15-1: Construction: Use Case Categories and Selected Use Cases 15-7
Figure 15-2: Construction: Use Case and Industry Challenges Alignment 15-10
Figure 15-3: Construction: Use Case Details 15-12
Figure 15-4: Construction: Importance of IoT 15-13
Figure 15-5: Construction: Use Case Category Impact 15-14
Figure 15-6: Construction: Confidence in Delivering Use Case Categories 15-15
Figure 15-7: Construction: Top 10 Most Important Single Technologies 15-15
Figure 16-1: Insurance: Use Case Categories and Selected Use Cases 16-8
Figure 16-2: Insurance: Use Case and Industry Challenges Alignment 16-10
Figure 16-3: Insurance: Use Case Categories Details 16-11
Figure 16-4: Insurance: Importance of IoT 16-12
Figure 16-5: Insurance: Use Case Category Impact 16-13
Figure 16-6: Insurance: Confidence in Suppliers Delivering 16-14
Figure 16-7: Insurance: Top 10 Most Important Single Technologies 16-14
Figure 17-1: Smart Cities: Top 10 Mayoral Priorities (2015 to 2022) 17-4
Figure 17-2: Smart Cities: IoT Use Cases Categories and Selected Use Cases 17-19
Figure 17-3: Smart Cities: Use Case and Challenges Alignment 17-23
Figure 17-4: Smart Cities: Use Case Categories Details 17-27
Figure 17-5: Smart Cities: Importance of IoT 17-28
Figure 17-6: Smart Cities: Importance of IoT Use Case Technology 17-29
Figure 17-7: Smart Cities: Top 10 Most Important Single Technologies 17-30
Figure 18-1: Transport and Logistics: Global Supply Chain Vulnerability Index (2020) 18-4
Figure 18-2: Transport and Logistics: Diesel Prices from 1993 – 2023 18-13
Figure 18-3: Transport and Logistics: Gasoline Prices from 1993 - 2023 18-14
Figure 18-4: Transport and Logistics: Use Case Categories and Selected Use Cases 18-17
Figure 18-5: Transport and Logistics: Use Case and Industry Challenges Alignment 18-20
Figure 18-6: Transport and Logistics: Use Case Details 18-25
Figure 18-7: Transport and Logistics: Importance of IoT 18-26
Figure 18-8: Transport and Logistics: Use Case Category Impact 18-27
Figure 18-9: Transport and Logistics: Confidence in Suppliers Delivering 18-28
Figure 18-10: Transport and Logistics: Top 10 Most Important Single Technologies 18-29
Figure 19-1: Healthcare: Payment Flows 19-4
Figure 19-2: Healthcare: Current and Forecasted Costs 19-5
Figure 19-3: Healthcare: Physician Shortage 19-19
Figure 19-4: Healthcare: Use Case Categories and Selected Use Cases 19-23
Figure 19-5: Healthcare: Use Case and Industry Challenges Alignment 19-25
Figure 19-6: Healthcare: Use Case Details 19-28
Figure 19-7: Healthcare: Importance of IoT 19-29
Figure 19-8: Healthcare: Use Case Category Impact 19-30
Figure 19-9: Healthcare: Confidence in Suppliers Delivering 19-30
Figure 19-10: Healthcare: Top 10 Most Important Single Technologies 19-31
Figure 20-1: Retail: Use Case Categories and Selected Use Cases 20-12
Figure 20-2: Retail: Use Case Alignment with Industry Challenges 20-14
Figure 20-3: Retail: Use Case Details 20-16
Figure 20-4: Retail: Importance of IoT 20-17
Figure 20-5: Retail: Use Case Category Impact 20-18
Figure 20-6: Retail: Confidence in Suppliers Delivering 20-19

© Strategy of Things, 2025. All rights reserved.

Figure 20-7: Retail: Top 10 Most Important Single Technologies 20-20
Figure 21-1: Renewable Energy: Use Case Categories and Selected Use Cases 21-15
Figure 21-2: Renewable Energy: Use Case and Industry Challenges Alignment 21-17
Figure 21-3: Renewable Energy: Use Case Details 21-19
Figure 21-4: Renewable Energy: Importance of IoT 21-20
Figure 21-5: Renewable Energy: Top 10 Most Important Single Technologies 21-21
Figure 22-1: The IoT Journey: Operational Efficiency to Full Autonomy 22-1
Figure 22-2: IoT Accelerators 22-4
Figure 23-1: Overview of Process Used to Identify Key Gaps 23-1
Figure 23-2: IoT Technology Infrastructure Gap Categories and Criteria 23-3
Figure 23-3: Key Gaps by Category 23-4
Figure 24-1: Technology Diffusion 24-1
Figure 24-2: Government Assistance Areas 24-4
Figure 24-3: Technology Development Examples 24-5
Figure 24-4: Commercial Enablement Examples 24-8
Figure 24-5: Facilitate Market Adoption Examples 24-11
Figure 24-6: Lead by Example Examples 24-13
Figure 24-7: Accelerate Value Realization Examples 24-15
Figure 24-8: IoT Studies 24-17
Figure 24-9: IoT Technology Infrastructure Gaps Mapped Against Four Stages of IoT Evolution 24-19
Figure 24-10: Core Gaps: Government Opportunities 24-20
Figure 24-11: Intelligence Gaps: Government Opportunities 24-35
Figure 24-12: Hyper-Deployed Gaps: Government Opportunities 24-39
Figure 25-1: IoT Value by Industry and Allocation ($US bn) 25-3
Figure 25-2: U.S. Global IoT Value Share Estimates 25-4
Figure 25-3: U.S. IoT Value Estimates by Selected Industry ($US bn) 25-5
Figure 25-4: Single Technology Classification Example from Desk Research 25-6
Figure 25-5: Single Technology Classification Example from Interviews 25-7
Figure 25-6: Example Top 10 Single Technology Ranking 25-9
Figure 25-7: Data Integration Method 25-10
Figure 25-8: Agriculture: Use Cases: Single Technology Classifications 25-12
Figure 25-9: Agriculture: Other Desk Research: Single Technology Classifications 25-13
Figure 25-10: Agriculture: Other Desk Research: Single Technology Classifications 25-14
Figure 25-11: Agriculture: Stakeholder Interviews 25-15
Figure 25-12: Agriculture: Round Table Discussions 25-15
Figure 25-13: Agriculture: Stakeholder Interviews: Single Technology Classifications 25-17
Figure 25-14: Agriculture: Stakeholder Interviews: Single Technology Classifications 25-17
Figure 25-15: Agriculture: Interview, Desk Research and Survey Technical Results 25-18
Figure 25-16: Agriculture: Role of the Public Sector in R&D 25-19
Figure 25-17: Agriculture: Ranking and Single Technology Weightings 25-20
Figure 25-18: Manufacturing: Desk Research: Use Case Single Technology Classifications 25-21
Figure 25-19: Manufacturing: Other Industry Desk Research: Single Technology Classifications 25-23
Figure 25-20: Manufacturing: Other Desk Research: Single Technology Classifications 25-23
Figure 25-21: Manufacturing: Stakeholder Interviews 25-24
Figure 25-22: Manufacturing: Stakeholder Interviews: Qualitative Single Technologies 25-26
Figure 25-23: Manufacturing: Stakeholder Interviews: Qualitative Single Technologies Classifications 25-27
Figure 25-24: Manufacturing: Use Case, Interview, Desk Research, Survey Technical Results 25-28
Figure 25-25: Manufacturing: Role of the Public Sector in R&D 25-29

© Strategy of Things, 2025. All rights reserved.

Figure 25-26: Manufacturing: Ranking and Single Technology Weightings 25-30
Figure 25-27: Construction Use Case: Single Technology Classifications 25-31
Figure 25-28: Construction: Other Desk Research: Single Technology Classifications 25-32
Figure 25-29: Construction: Other Desk Research: Single Technology Classifications 25-33
Figure 25-30: Construction: Stakeholder Interviews 25-34
Figure 25-31: Construction: Stakeholder Interviews: Single Technology Classifications 25-35
Figure 25-32: Construction: Stakeholder Interviews: Single Technology Classifications 25-36
Figure 25-33: Construction: Use Case, Interview, Desk Research, Survey Technical Results 25-37
Figure 25-34: Construction: Role of the Public Sector 25-38
Figure 25-35: Construction: Ranking and Single Technology Weightings 25-39
Figure 25-36: Insurance: Use Case: Single Technology Classifications 25-41
Figure 25-37: Insurance: Use Cases: Single Technology Classifications 25-42
Figure 25-38: Insurance: Other Desk Research: Single Technology Classifications 25-43
Figure 25-39: Insurance: Other Desk Research: Single Technology Classifications 25-43
Figure 25-40: Insurance: Stakeholder Interviews 25-44
Figure 25-41: Insurance: Stakeholder Interviews: Single Technology Classifications 25-45
Figure 25-42: Insurance: Stakeholder Interviews: Single Technology Classifications 25-46
Figure 25-43: Insurance: Interview, Desk Research & Survey Integrated Results 25-47
Figure 25-44: Insurance: Role of the Public Sector in R&D 25-48
Figure 25-45: Insurance: Ranking and Single Technology Weightings 25-49
Figure 25-46: Smart Cities: Use Cases: Single Technology Classifications 25-50
Figure 25-47: Smart Cities: Other Desk Research: Single Technology Classifications 25-51
Figure 25-48: Smart Cities: Other Desk Research: Single Technology Classifications 25-52
Figure 25-49: Smart Cities: Stakeholder Interviews 25-52
Figure 25-50: Smart Cities: Stakeholder Interviews: Single Technology Classifications 25-53
Figure 25-51: Smart Cities: Stakeholder Interviews: Single Technology Classifications 25-54
Figure 25-52: Smart Cities: Interview, Desk Research & Survey Integrated Results 25-55
Figure 25-53: Smart Cities: Role of the Public Sector 25-56
Figure 25-54: Smart Cities: Ranking and Single Technology Weightings 25-57
Figure 25-55: Transport and Logistics: Use Cases: Single Technology Classifications 25-58
Figure 25-56: Transport and Logistics: Other Desk Research: Single Technology Classifications 25-59
Figure 25-57: Transport and Logistics: Other Desk Research: Single Technology Classifications 25-60
Figure 25-58: Transport and Logistics: Stakeholder Interviews 25-61
Figure 25-59: Transport and Logistics: Stakeholder Interviews: Single Technology Classifications 25-61
Figure 25-60: Transport and Logistics: Stakeholder Interviews: Single Technology Classifications 25-62
Figure 25-61: Transport and Logistics: Interview, Desk Research and Survey Technical Results 25-63
Figure 25-62: Transport and Logistics: Role of the Public Sector in R&D 25-64
Figure 25-63: Transport and Logistics: Ranking and Single Technology Weightings 25-65
Figure 25-64: Healthcare: Use Cases: Single Technology Classifications 25-66
Figure 25-65: Healthcare: Other Desk Research: Single Technology Classifications 25-68
Figure 25-66: Healthcare: Other Desk Research: Single Technology Classifications 25-68
Figure 25-67: Healthcare: Stakeholder Interviews 25-69
Figure 25-68: Healthcare: Stakeholder Interviews: Single Technology Classifications 25-70
Figure 25-69: Healthcare: Stakeholder Interviews: Single Technology Classifications 25-71
Figure 25-70: Healthcare: Interview, Desk Research and Survey Technical Results 25-72
Figure 25-71: Healthcare: Role of the Public Sector in R&D 25-73
Figure 25-72: Healthcare: Most Important Single Technology Weightings 25-74
Figure 25-73: Retail: Use Case: Single Technology Classifications 25-75

© Strategy of Things, 2025. All rights reserved.

Figure 25-74: Retail: Use Cases: Single Technology Classifications....25-76
Figure 25-75: Retail: Other Desk Research: Single Technology Classifications....25-77
Figure 25-76: Retail: Other Desk Research: Single Technology Classifications....25-78
Figure 25-77: Retail: Stakeholder Interviews....25-79
Figure 25-78: Retail: Stakeholder Interviews: Single Technology Classifications....25-79
Figure 25-79: Retail: Stakeholder Interviews: Single Technology Classifications....25-80
Figure 25-80: Retail: Interview, Desk Research and Survey Technical Results.... 81
Figure 25-81: Retail: Role of the Public Sector in R&D....25-82
Figure 25-82: Retail: Most Important Single Technology Weightings....25-83
Figure 25-83: Renewable Energy: Use Cases: Single Technology Classifications....25-84
Figure 25-84: Renewable Energy: Other Desk Research: Single Technology Classifications....25-85
Figure 25-85: Renewable Energy: Other Desk Research: Single Technology Classifications....25-86
Figure 25-86: Renewable Energy: Stakeholder Interviews....25-87
Figure 25-87: Renewable Energy: Stakeholder Interviews: Single Technology Classifications....25-87
Figure 25-88: Renewable Energy: Stakeholder Interviews: Single Technology Classifications....25-88
Figure 25-89: Renewable Energy: Interview, Desk Research and Survey Technical Results.... 89
Figure 25-90: Renewable Energy: Role of the Public Sector in R&D....25-90
Figure 25-91: Renewable Energy: Ranking and Single Technology Weightings....25-90
Figure 26-1: Qualitative Gap Importance by Industry....26-1
Figure 26-2: All Industries Single Technology Component Technical Rankings....26-2
Figure 26-3: Subcategory Weighting Probability Distributions....26-3
Figure 26-4: Detailed R&D to Revenue by Industry....26-5
Figure 26-5: High, Medium and Low R&D to Revenue Percentages....26-6
Figure 26-6: R&D to Revenue by Industry....26-6
Figure 26-7: Gross Margin by Industry....26-7
Figure 26-8: Economic Surplus from a Nominal $10 million Investment in H-1 Hardware: IoT Sensors....26-9
Figure 26-9: Economic Surplus from a Nominal $10 million Investment in T-4 Standards: Interoperability....26-9
Figure 26-10: Economic Surplus from a Nominal $10 million Investment in S-3 Software: Data collect....26-10
Figure 26-11: Economic Surplus from a Nominal $10 million Investment in Y-3 Systems: Security....26-11
Figure 26-12: Impact of a Nominal $10 million Public Sector Investment in Core: Interoperability....26-13
Figure 26-13: Impact of a Nominal $10 million Public Sector Investment in Core: Privacy....26-13
Figure 26-14: Impact of a Nominal $10 million Public Sector Investment in Core: Security....26-14
Figure 26-15: Impact of a Nominal $10 million Public Sector Investment in Core: Connectivity....26-14
Figure 26-16: Impact of a Nominal $10 million Public Sector Investment in Intelligence: Data Management....26-15
Figure 26-17: Impact of a Nominal $10 million Public Sector Investment in Intelligence: Artificial Intelligence26-15
Figure 26-18: Impact of a Nominal $10 million Public Sector Investment in Intelligence: Intelligent Devices....26-16

© Strategy of Things, 2025. All rights reserved.

Acknowledgements

This study was extensive and explored a broad range of industries and complex topics. Our work would not have been possible without the collaboration and support of many people who generously gave their time, expertise and resources.

We would like to thank our project advisor at NIST, Kathleen McTigue, who supported us extensively throughout all phases of the project in many ways. Her guidance has greatly enhanced and improved the quality of this study, and for that, we are grateful.

Other NIST staff supported our work. We thank Michael Walsh, Michael Hall and David Butry for reviewing our economic approach and providing perspectives that help shape the approach and thinking. We thank Chris Greer, our technical advisor, for providing the guidance that helped us define and shape our technical analysis and narrative. And we thank Barbara Cuthill who meticulously reviewed our report drafts and executive summaries and provided a valuable critique of our work.

We are also grateful to the many people who have graciously shared their knowledge and perspectives through interview, survey response, round table discussion and in conversation and email. These conversations added much to our understanding of the unique characteristics of the industries studied, as well as the challenges and opportunities faced by the Internet of Things. Their perspectives and insights were instrumental in informing our research.

One of the challenges we faced was devising an efficient outreach to industry. We thank Keith Kreisher, Executive Director of the IoT M2M Council and the IoT M2M Council, who provided the resources and the industry outreach with solution providers and adopters to drive awareness of our project, provide perspectives and increase survey response.

Finally, we would like to thank our peer reviewers who provided an industry perspective on our drafts. Their comments helped us to bring clarity and often proposed better framings. More importantly, they validated our approaches, assumptions and findings. They are listed below in alphabetical order. If we have forgotten anyone, we apologize for the omission.

The report represents the views of the authors. Errors or omissions remain their responsibility.

© Strategy of Things, 2025. All rights reserved.

Organizations

Association of Equipment Manufacturers (AEM)

IoT M2M Council (IMC)

Open Connectivity Foundation (OCF)

Individual Experts

Aaron Allsbrook, CTO, ClearBlade

Eric Bathras, Associate Vice President, AECOM

Alex Bazhinov, CEO, Lumin

Bret Beringer, Chief Engineer, Fybr

Johannes Biermann, President/COO, aicas

Brian Bishop, CEO, Data Performance Consultancy Limited

Adam Boucher, CEO, Molecule Systems

Kevin Bowers, Director, Field services Research, TSIA

Ryan Briggs, Vice President, Automotive and Mobility Solutions, Swiss Re

Tim Brosnihan - Executive Director, SEMI MSIG (MEMS and Sensor Industry Group)

Dennis Buckmaster, Professor, Agricultural and Biological Engineering, Dean's Fellow for Digital Agriculture, Purdue University

Bong Castillo, Wireless Technology and Network Transformation Consultant, Myamma LLC

Ray Chan, Co-Founder, Nightingale Labs

Andrew Chin, Consultant, Strategy of Things

John Corbin, Automated Vehicle Program Manager, US Department of Transportation

Barbara Cuthill, National Institute of Standards and Technology

Frédéric Desbiens, Senior Manager, Embedded and IoT, Eclipse Foundation

Tim Drake, Senior Vice President for Public Policy and Government Affairs, ITS America

David Duncan, Consultant, Strategy of Things

Stephen F Duffy Ph.D, PE, Director, Cleveland State University Transportation Center, Professor, Department of Civil and Environmental Engineering, Cleveland State University

Nicole DuPuis, Vice President, Innovative Mobility and Emerging Technology, ITS America

Farid Farahmand, Professor, Sonoma State University

Gordon Feller, Global Fellow, Smithsonian Institute Wilson Center

Lucian Fogoros, Co-Founder, IIoT World

Amlan Ganguly, Department Head, Depart of Computer Engineering, Rochester Institute of Technology

© Strategy of Things, 2025. All rights reserved.

Adam Gittings, General Manager, HTS Ag

Kathleen Glass, Vice President of Marketing, AquaSpy

Arathi Gopinath, Director, Data Science, Data Analytics and Performance Metrics, Enphase Energy

Kyle Hefner, CableLabs

Tom Herbst, Principal, Fú Consulting

Ron Hiller, Founder, BLX

Dr. James Hunt, Co-founder/CEO/CTO, aicas

Uche Ishionwu, IoT and OT Security Solution Architect, Avanade

Bill Jennings, CTO/Senior Vice President Engineering, FarmX

Amit Jindal, Consultant, Accenture

Bradly Johnson, NASA

Bruno Johnson, CEO, Cascoda

Peter Jones, Distinguished Engineer, Cisco

Steve Jones, Senior Director, Industry Insights Research, Dodge Data & Analytics

Dr. Calvin Kam, CEO, Strategic Building Innovation

Brian Kilcourse, Co-founder, RSR Research

Jill Klein, Head of Emerging Technologies, CDW

Keith Kreisher, Executive Director, IoT M2M Council

Mohan Kumar, Professor, Department of Computer Science, Rochester Institute of Technology

Dr. Kiju Lee, Associate Professor, Engineering Technology and Industrial Distribution and Mechanical Engineering, Texas A&M University

Chris Link, Senior Director, Business Development, KORE Wireless

Kenneth A. Loparo, Ph.D., Faculty Director, ISSACS: Institute for Smart, Secure and Connected Systems, Co-Academic Director, IoT Collaborative, Arthur L. Parker Professor, Department of Electrical, Computer and Systems Engineering, Case Western Reserve University

RJ Mahadev, President, AIOTA

Shaun B. Manchand, Principal, Barmacy LLC

Joseph Mariani, Senior Research Manager, Center for Government Insights, Deloitte Consulting

Francisco Maroto, IoT Advisor

Bobby McCurdy, Senior Director, Policy and Advocacy, ITS America

Kathleen McTigue, Economist, National Institute of Standards and Technology

Dustin Mulvaney, Professor, Department of Environmental Studies, San Jose State University

© Strategy of Things, 2025. All rights reserved.

Dr. Venkatesh Narayanamurti, Harvard University, Benjamin Peirce Professor of TEchnology and Public Policy, Kennedy School and Belfer Center for Science and INternational Affairs

Mary Jo Nye, Chief Engagement Officer, Bellebrite Energy

Julie Powers, NASA

Dr. Ajay Raghavan, Strategic Execution Director, Systems Science Lab, Xerox PARC

Kavita Ramcharan, Vice President of Inspection Operations and Client Services, HSB Canada

Richard Rasansky, Serial Entrepreneur, XCMR

Brad Rein, National Science Liason, National Institute of Food and Agriculture, USDA

Graham Richards, Former Mayor of Fort Wayne, IN, Former CEO of Advanced Energy Economy

Tony Rinella, Strategic Building Innovation

Steve Rowen, Managing Partner, RSR Research

Orlando Saenz, Founder/CEO, Aker Technologies

Doug Sandy, VP of Technology/CTO, PCI Industrial Computer Manufacturers Group (PICMG)

Stan Schneider, CEO, RTI

Ali Shakouri, Professor of Electrical and Computer Engineering, Associate Dean for Research and Innovation, Purdue University

Eric Simone, CEO ClearBlade

Dimitrios Spiliopoulos, IoT Global Strategist and GTM

David Smith, Vice President of IoT Solutions, GetWireless

Richard Soley, Executive Director, Industrial Internet Consortium

Rob Spiger, Principal Security Strategist, Global Cybersecurity Policy Team, Microsoft

Craig Stark, Director, Strategy of Things

David Steven Jacoby, Managing Director, Boston Strategies International

Ravi Subramaniam, Senior Director, IEEE

Dan Sweeney, Research Scientist, MIT D Lab

Robert Tse, Senior Policy Advisor, USDA

Dr. Garrick Villaume, CTO, Nuxsen

Joe Ward, Senior Director of Sales and Business Development North America (retired), e-peas S.A.

Tim Way, IoT Solutions Architect, Telit

Ken Wei, Managing Partner, Gartner

Jon Weiss, VP of IoT and Analytics, Software AG

Jeff Whitman, Director of Business Development, AECOM

© Strategy of Things, 2025. All rights reserved.

Peter Williams, Principal, Peter Williams Consulting

Joe Work, Senior Growth Advisor, Manufacturing Advocacy and Growth Network

Eva Yu, Associate, Manager of Education Programs, Strategic Building Innovation

© Strategy of Things, 2025. All rights reserved.

Executive Summary

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

© Strategy of Things, 2025. All rights reserved.

Executive Summary

At their simplest, Internet of Things (IoT) devices contain sensors and actuators to monitor and control the physical environment, an embedded system with a microprocessor and memory to process the data collected and a means of communication with the Internet. The data collected from the IoT devices may be analyzed on the device or a nearby local server ("edge"), on a server in a moving vehicle ("mobile edge"), or on a server in a remote data center ("cloud"). Examples of consumer IoT devices include smart phones and smart home thermostats. In a factory setting, connected vibration sensors monitor the mechanical vibration levels of manufacturing equipment and alert plant managers if a machine is behaving abnormally.

The Internet of Things is an evolving technology domain that is transforming our daily lives, affecting industry, academia and government, with significant economic, social and national security implications. This evolving technology has the potential to enhance U.S. global competitiveness, increase the resilience of our nation and contribute to increased economic security. Recognizing IoT's importance, the federal government has made IoT a key focus in its "Lab to Market" initiative, which aims to bridge research investments and technology transfer.

In 2019, the U.S. National Institute of Standards and Technology (NIST) awarded research and innovation advisory firm Strategy of Things a cooperative agreement (grant) for a study to assess the potential economic impact of federal research investments in developing the technological infrastructure necessary to support IoT.

During the time this study was conducted, the rising prominence of Artificial Intelligence (AI) has reinforced the importance and relevance of IoT. The Internet of Things provides AI with a data source to build and train algorithms and models. In turn, AI enables IoT systems to make sense of the monitored conditions and respond to these situations.

In Fiscal Year 2022, the U.S. federal government invested more than $195 billion[1] in basic and applied research and development across a range of disciplines from computer information to social sciences. Over $70 billion of this research is conducted at nearly 300 Government Owned, Government Operated (GOGO) and Government Owned, Contractor Operated (GOCO) laboratories across the country.[2] Approximately $106 billion of this investment was in extramural research and development at universities, non-profits, and small and large businesses across the country.[3]

This study provides a set of analyses that identify IoT infrastructure gaps that have the potential to be efficiently addressed with public sector investments across a range of technologies and industries.

Scope

The study aims to assess the current state of IoT technology infrastructure across nine industries and identify key cross industry technology gaps. The study includes an economic analysis of the impact of addressing these gaps where appropriate with a combination of federal policies,

[1] "Federal Funds for Research and Development: Fiscal Years 2022–23", National Center for Science and Engineering Statistics. NSF 24-321, April 3, 2024. Table 1. Link

[2] ibid. Table 12.

[3] ibid. Table 9.

© Strategy of Things, 2025. All rights reserved.

initiatives and investments. It will also recommend those areas for federal research investments to strengthen U.S. competitiveness and national security. While IoT offers a variety of societal benefits, the analysis of those was beyond the scope of this research.

The findings will be shared with federal agencies, academia and industry through various communication channels, including publications, presentations and digital platforms.

The objectives of the research study are:

- **Objective 1.** Assess the current state of the IoT technology covering research, development and adoption across nine industries. The industries examined include agriculture, manufacturing, construction, insurance, smart cities, retail, transportation and logistics, healthcare and renewable energy.
- **Objective 2.** Analyze these findings and identify technology infrastructure gaps. IoT technology infrastructure refers to hardware, software, networking, applications, systems and standards.
- **Objective 3.** Perform an economic analysis to understand the potential impact on the national economy of the government appropriately addressing those gaps
- **Objective 4.** Recommend potential areas for appropriate federal IoT-related research investments that will enhance U.S. competitiveness and national and economic security.
- **Objective 5.** Communicate these findings across the federal government, academia and industry.

Approach

The research looked at nine industries. Information was collected through 450 survey responses along with 50 targeted interviews and secondary research on government, scientific and industry publications, online blogs and other publicly available reports. From this, we identified the industry specific barriers ("challenges") hindering the development, adoption and broader use of IoT. We determined the most commonly cited and observed cross industry IoT technology research barriers ("gaps") by screening them with a set of criteria.

IoT is not one technology, but a collection of disparate individual technologies ("components") and systems. To conduct the economic analysis, we decomposed IoT into twenty-five single technology components that can be researched and quantified. Each IoT technology infrastructure gap is made up of a specific combination of these single technology components. The cross industry technology infrastructure gaps are quantified by summing the economic impacts of the individual technologies.

Given the complexity and breath of the study, we employed a portfolio management approach that considered and integrated three perspectives: technology, economics and government. This approach is well suited for innovation management and recognizes the diverse types and nature of the gaps across industries, prioritizes the gaps across the ongoing evolution of IoT, and considers the range of possible responses and resources needed to effectively address these gaps. The portfolio approach balances risk, resource allocation, capabilities, the maturity of the technology and the evolutionary stage of IoT to improve the likelihood of beneficial outcomes. We quantified the impact of federal research by estimating the revenues and profits (economic

© Strategy of Things, 2025. All rights reserved.

surplus) generated from a nominal $10 million research investment to address the challenges and the gaps.

Three frameworks and models were developed to facilitate the analysis and creation of results in this research.

- A framework was developed to identify and prioritize a cross industry technology infrastructure gaps portfolio that is aligned with the evolution of the Internet of Things.
- An economic model was developed to quantify the impact of addressing the identified technology infrastructure gaps. This model incorporates an investment portfolio approach to allocating investments across technology areas, infrastructure gaps and industries.
- An opportunities portfolio framework was developed to identify and classify the potential means and capabilities the federal government has to address the technology infrastructure gaps.

Overview

The research identified a portfolio of eleven IoT technology infrastructure gaps that the federal government should consider for research investment to advance the Internet of Things. These gaps were classified into three categories and span a range of technologies and capabilities that affect both the current state of IoT and the future state with billions of hyperconnected and autonomous IoT devices and IoT-enabled systems.

Economic analyses estimating the long term revenues and profits generated from a nominal $10 million research investment for some of the gaps were performed. The analyses quantified how each gap investment should be distributed across the nine industry sectors to maximize economic outcomes.

The gaps identified are well-suited for federal research investments to address. These federal investments complement existing industry efforts by addressing research topics that are not undertaken by private organizations. This includes undertaking research that is outside of industry's short to mid-term priorities. It also includes areas where industry participants lack the expertise or capabilities, and areas that may conflict with their own proprietary approaches.

Similarly, federal investments may be used to conduct groundwork research to enable future IoT technologies as well as address existing gaps in new and more novel ways. This research can be transferred to industry for further development and commercialization.

The gaps require specific treatments that vary by industry and stage of IoT evolution. The study recommended that government leaders and policymakers employ a portfolio "whole of government" approach to address the gaps. A portfolio approach optimizes the allocation of research investments across the nine industries for a particular risk and aligns it with the most appropriate federal capabilities to address the gaps efficiently.

Key Findings

The research suggests ten key findings. These highlight both technological and non-technological challenges in IoT development as well as opportunities for public sector investment to enhance U.S. competitiveness and drive economic growth. Figure 1 to Figure 4 below show these findings mapped to the first four objectives of the work.

© Strategy of Things, 2025. All rights reserved.

Objective	#	Finding
Objective 1. Assess the current state of IoT technology across industries	1	IoT is envisioned to evolve in four distinct stages, with each new stage delivering increased capability and benefits. The four stages are: Stage 1: Things become "smart", Stage 2: AI algorithms take action, Stage 3: Outcomes and Utilities, and Stage 4: Hyperconnected autonomy.
	2	AI offers the potential to deliver transformational value to IoT in several different ways, including the efficient analysis of large volumes of data, autonomous operations, and facilitates interoperability, cybersecurity and network operations.
	3	Non-technological challenges are slowing the adoption, operation and realization of the value IoT brings to the economy. These include change or adoption resistance/slow adoption, the digital skills gap, legacy infrastructure, data ownership, industry structure, regulatory and financial factors.

Figure 1: Research Objective 1 Findings

Objective	#	Finding
Objective 2. Identify technology infrastructure gaps	4	IoT is hindered by eight common technology challenges that vary by industry. These are interoperability, cybersecurity, AI, data management, privacy, edge computing, devices/hardware and connectivity.
	5	There are three types of IoT technology infrastructure gaps. Core gaps are foundational technological gaps that hinder the operation and scaling of the Internet of Things across all stages of the IoT evolution. Intelligence gaps hinder data processing and analytical capabilities to create an autonomous and intelligent IoT. Hyper-Deployed gaps hinder the development of a future infrastructure to support a massively connected (hyperconnected) and autonomous IoT ecosystem across the economy.
	6	Our research identified the following technology infrastructure gaps: • Core gaps: Interoperability, cybersecurity, privacy and connectivity • Intelligence gaps: Data management, trust in artificial intelligence and intelligent devices. • Hyper-Deployed gaps: IoT data ecosystem, communications and network infrastructure, advanced computing paradigms and human centric IoT systems
	7	IoT is made of a diverse set of underlying technologies. Our research identified four technologies that industry felt were the most important areas appropriate for public sector investment. The four public sector investment areas are: (1) Hardware: IoT Sensors, (2) Standards: Interoperability, (3) Systems: Security and (4) Software: Data Collection.

Figure 2: Research Objective 2 Findings

© Strategy of Things, 2025. All rights reserved.

Objective	#	Finding
Objective 3. Perform an economic analysis to understand the potential impact on the national economy of the government appropriately addressing those gaps	8	The economic model allocated a nominal public sector investment of $10 million distributed across the nine industries for each single technology component. The allocations were made to provide the maximum benefit to the economy based on the role of the public sector, the importance of the single technology component and the likely future value of IoT in that industry. The analysis considered a $10 million investment in each of the four single technology components specified in the 25 level IoT single technology taxonomy. The investments over the nine industries generated a long term cumulative revenue that ranges from $269 million for an investment in Software: Data Collection to $578 million for an investment in Systems: Security. These investments created a corresponding economic surplus, ranging from $72 million (Software: Data Collection) to $150 million (Systems: Security). A nominal public sector investment of $10 million in each one of the core and intelligence gaps is associated with a long-term cumulative revenue for each gap addressed. The long-term cumulative revenue generated varies by gap, from $548 million for Privacy to $889 million for Data Management. Similarly, these investments create a corresponding economic surplus for each gap, ranging from $149 million (Privacy) to $239 million (Data Management).
	9	The allocations based on the role of the public sector, the importance of the single technology component and the likely future value of IoT led to different allocations of the $10 million investment in each industry for each technology infrastructure gap. For example, the analysis estimated that 36.8% of the $10 million nominal research investment in interoperability be allocated to the healthcare industry while only 1.1% be allocated to the renewable energy industry. This is largely driven by the substantially higher economic value of IoT to the larger healthcare industry compared to the renewable energy industry.

Figure 3: Research Objective 3 Findings

Objective	#	Finding
Objective 4. Recommend potential areas for federal investments	10	Five broad areas were identified that provide opportunities for the federal government to consider addressing the Core, Intelligence and Hyper-Deployed gaps identified in Finding 6. These areas are technology development, commercial enablement, market adoption, lead-by-example and economy wide benefits. Each gap has a different combination of possible opportunities specific to the nature of the gap, its technological maturity and other factors.

Figure 4: Research Objective 4 Findings

© Strategy of Things, 2025. All rights reserved.

State of IoT in Industry: Technology and Non-Technology Challenges

Our research uncovered a variety of technological challenges hindering the adoption and advancement of IoT in industry. A combination of interviews, secondary research and surveys was conducted to identify and understand the opportunities and challenges to the development and adoption of IoT. Each research method approached the challenges from a different perspective.

For example, the survey targeted a large audience and asked specific questions that supported the economic analysis and around 450 responses were received. The interviews targeted a small number of people who provided deeper insight and context to supplement the information already collected. Finally, the desk research, consisting of a review of online news articles, published research reports, vendor and government white papers, blogs, webinars, videos and other content provided a broad overview of the use case applications of IoT in the industry.

Figure 5 shows the technology categories of challenges mapped against the industry. The individual top three or four technology challenges per industry have been aggregated into eight categories to have a broader cross industry perspective.

Technology Challenges	Agriculture	Manufacturing	Construction	Insurance	Smart Cities	Transportation & Logistics	Healthcare	Retail	Renewable Energy
Interoperability	✓	✓	✓		✓	✓	✓		✓
Cybersecurity		✓	✓	✓	✓	✓	✓	✓	✓
Artificial Intelligence				✓		✓	✓	✓	
Data Management/Integration			✓			✓			✓
Privacy				✓	✓		✓	✓	
Edge computing	✓	✓			✓				
Devices (cost, others)		✓						✓	
Connectivity	✓	✓			✓		✓		

Figure 5: Top Technology Challenges by Industry.

Our research uncovered a variety of non-technology[4] challenges hindering the further adoption and advancement of IoT in industry. The 25 individual industry non-technology challenges have been clustered into seven categories and discussed here from a broader cross industry perspective.

[4] Non-technology challenges include challenges that may be technical in nature but are not related directly to the Internet of Things.

© Strategy of Things, 2025. All rights reserved.

Figure 6 lists the non-technology categories of challenges mapped against each industry found in Section 5.2. These are briefly discussed below.

Non-technology Challenges	Agriculture	Manufacturing	Construction	Insurance	Smart Cities	Transportation and Logistics	Healthcare	Retail	Renewable Energy
Digital Skills	✓	✓	✓	✓	✓	✓		✓	✓
Adoption Barriers (resistance, trust, right to repair, awareness, etc.)	✓	✓	✓		✓	✓			
Legacy infrastructure and operations		✓		✓	✓	✓	✓	✓	
Data Ownership/Privacy	✓		✓			✓	✓	✓	
Industry structure: Fragmented industry structure, Utility company alignment			✓			✓			✓
Regulatory compliance, uncertain regulatory treatment				✓		✓	✓		✓
Financial (funding, ROI, capital)	✓	✓			✓			✓	

Figure 6: Top Non-Technology Challenges by Industry.

Cross industry IoT Technology Infrastructure Gaps

Cross industry IoT technology infrastructure gaps were identified by analyzing and aggregating the industry-specific technology challenges. Our research study identified eleven technology infrastructure gaps that hinder the development, adoption and operation of IoT in the U.S. economy and society. These gaps were identified using a framework developed to analyze and map to one of three gap categories (Core, Intelligence and Hyper-Deployed) which are aligned with the stages of IoT evolution to guide prioritization. Figure 7 below shows the gaps by category.

© Strategy of Things, 2025. All rights reserved.

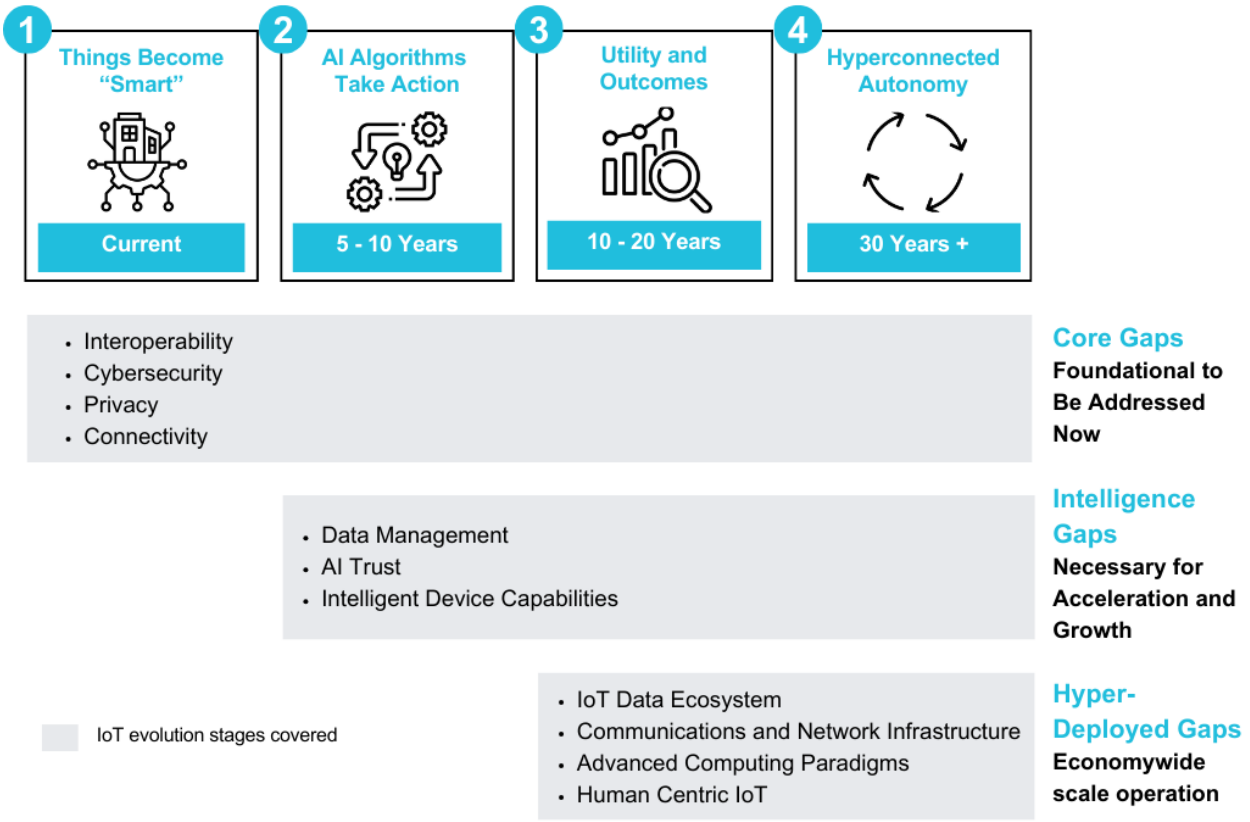


Figure 7: IoT Technology Infrastructure Gaps by Category and Evolution Stage

Core Gaps

Core gaps are foundational technological gaps that hinder the operation and scaling of the Internet of Things across all stages of the IoT evolution. The four IoT technology infrastructure core gaps are described briefly in Figure 8 below.

Core Gap	Gap Description
Interoperability	The lack of interoperability hinders different devices and systems from integrating, communicating and sharing information with each other. Barriers to achieving interoperability include limited focus of standards initiatives, resistance to open and industry consensus standards, regional standards and standards implementation errors and deviations. The government currently supports with pre-standards research and science, the development of frameworks and testbeds and convening stakeholders.
Cybersecurity	IoT devices expose new attack surfaces that can be exploited by criminals to enter the network, steal information and disrupt operations. It is difficult to fully eliminate cybersecurity risks. There is no "one size fits all" approach because IoT devices and systems are diverse and heterogeneous. Devices are resource constrained and have limited ability to implement robust measures. Threats are evolving. Government plays a critical role in

© Strategy of Things, 2025. All rights reserved.

Core Gap	Gap Description
	facilitating standards, developing frameworks, convening stakeholders, informing regulations and researching novel approaches.
Privacy	Privacy challenges include the unauthorized collection, storage and use of data as well as the unauthorized disclosure and sharing of private information. Businesses are incentivized to collect and use personal data. Privacy is hindered by a fragmented regulatory environment, inadequate cybersecurity measures, inadequate privacy consent mechanisms and deanonymization of private data. The government plays a key role in facilitating standards, developing frameworks, conducting research in privacy enhancing technologies, advanced computing paradigms to enhance privacy (i.e., context aware computing) and other approaches.
Connectivity	IoT enabled equipment requires connectivity to send data to edge servers and remote data centers in the cloud for processing and storage. Connectivity challenges are multi-dimensional in nature and challenging to solve due to various factors, including the need for substantial infrastructure investment, the lack of a "one size fits all" approach along with issues in market economics, funding and incentives, "last acre" coverage and spectrum. The government plays critical roles in facilitating infrastructure, spectrum and future connectivity (6G, etc.).

Figure 8: Brief Description of IoT Technology Infrastructure Core Gaps.

Intelligence Gaps

Intelligence gaps hinder data processing and analytical capabilities to create an autonomous and intelligent IoT. The three IoT technology infrastructure intelligence gaps are briefly described below.

Intelligence Gap	Intelligence Gap Description
Data management challenges	As IoT scales, so does data management complexity. The IoT data collected comes in a variety of types, formats and sizes. Some data are time-sensitive and must be processed immediately while others are stored for future actions. Data may be required to comply with industrial, state and national regulations. Robust data management is foundational for artificial intelligence systems. Data management challenges are complicated by exponential growth in data volume and velocity, privacy considerations, cybersecurity factors, interoperability concerns and regulatory compliance requirements. Government can support progress here through standards and research in novel and emerging approaches.

© Strategy of Things, 2025. All rights reserved.

Intelligence Gap	Intelligence Gap Description
Challenges affecting trusting AI	AI outcomes produced may not be explainable, nor fair or ethical, leading to a lack of trust. However, establishing trust in AI-enabled IoT systems is complex due to a variety of technical, human and societal factors. Some major complicating factors include human reluctance and resistance, unclear data ownership and management, uncertain accountability and liability, lack of standardized guidelines for AI development and deployment and ethical dilemmas from AI generated outcomes. Government can support progress here through standards, frameworks and research in explainable AI and novel and emerging methods.
Intelligent device capabilities	On-device and edge processing of data are increasingly common and are needed for applications that are autonomous, latency sensitive or operate in an area with unreliable service. Other edge applications include IoT device swarms and ambient IoT use cases that require contextual information from other nearby devices. Developing IoT devices capable of supporting AI is challenging due to the physical limitations of semiconductors and microprocessors, complex programming requirements and high upfront development costs. The government augments industry through standards and novel and emerging approaches.

Figure 9: Intelligence Gaps

Hyper-Deployed Gaps

The envisioned future "hyper-deployed IoT" economy and society require a technology infrastructure much different than the current infrastructure. This infrastructure must support billions of heterogeneous connected IoT devices and systems reliably and predictably. It must allow for the seamless exchange of data and information and do so such that it can be made available and acted upon in a timely manner. It must support an economy where intelligent autonomous systems and human AI collaborations are the norm. It must protect against a variety of known and yet to be discovered future cybersecurity threats and autonomously contain and mitigate the impact of these threats. The algorithms used to analyze and act on the collected data must do so in a way that is accurate, fair and explainable. Our research identified the four IoT technology infrastructure hyper-deployed gaps briefly described below.

© Strategy of Things, 2025. All rights reserved.

Hyper-Deployed Gap	Hyper-Deployed Gap Description
IoT data ecosystem	One of the foundations of the future digital economy and society is the massive volumes of data generated by billions of smart devices and IoT-enabled systems. The future IoT data ecosystem is envisioned to be a highly interconnected network where data generated by IoT devices and systems is seamlessly shared, monetized and utilized across various sectors. There are, however, a number of technical challenges to building such an IoT data ecosystem. These include data quality, interoperability, privacy and security, data sovereignty, scaling and standards for data management. Government supports progress through facilitating standards, interoperability, architectures and convening stakeholders among other things.
Communications and network infrastructure	Industry analysts estimate that there will be 55.9 billion IoT devices generating 79.4 zettabytes (ZB) of data by 2025.[5] Current communication networks and architectures are not designed to manage the needs of IoT at this scale. New processes and technologies for configuring, managing, operating and maintaining the hyperconnected network will be necessary. Representative areas of infrastructure innovation are needed to support real-time autonomy and complex IoT applications, be fault tolerant and resilient and defend and heal against threats. Government can support progress through standards, advanced research in concepts, and research in advanced and novel approaches.
Advanced computing paradigms	IoT operates in an expansive ecosystem of interconnected heterogenous devices collecting, processing and exchanging data in real-time across the economy and society. There is no "one size fits all" architecture and the requirements of the specific IoT applications will determine what architecture works best. The future IoT ecosystem integrates several computing paradigms, including distributed computing, context-aware computing and swarm intelligence, to create intelligent and adaptive systems. Open research challenges must be addressed to fully realize their potential. Government supports progress through standards, advanced research in concepts, and research in advanced and novel approaches.

[5] "How You Contribute to Today's Growing DataSphere and Its Enterprise Impact," D. Reinsel, IDC Blog, November 4, 2019. Link

© Strategy of Things, 2025. All rights reserved.

Hyper-Deployed Gap	Hyper-Deployed Gap Description
Human centric IoT systems	Although IoT connects "things" or machines with other "things" and machines, its value is felt and realized by people. Human centric IoT is necessary for the future hyperconnected and autonomous IoT to become reality. Open areas of interdisciplinary research and innovation needed include human-AI collaboration and interaction, generative AI for IoT and methods to facilitate improved trust, inclusion and accessibility. Government supports progress through standards, advanced research in concepts, and research in advanced and novel approaches.

Figure 10: Hyper-Deployed Gaps

Economic Impact of Addressing the IoT Technology Infrastructure Gaps

In quantifying the economic impact of addressing the IoT gaps, our study employed the perspective of federal government executives planning research investment decisions. These executives face several questions, including:

- "If I had to invest a limited amount of money for research, what gaps do I spend it on?"
- "How and where should I allocate that investment to maximize its impact?"
- "How can I minimize the overall risks to my investments?"

Our study employed a portfolio investment approach to address these questions. Our economic analysis provided a directional estimate of how public sector investments could be allocated to produce revenues and profits (economic surplus) from a nominal $10 million public sector investment. The analysis was conducted at three levels:

- At the 25 single technology component level.
- At the infrastructure gap level, which is made up of multiple single individual technology components.
- At the industry level for each infrastructure gap.

In arriving at the allocations, we used information from the surveys, interviews and desk research to provide ranked lists of the importance of the 25 single technology components. These weighting were then adjusted on an industry basis by the long term value of IoT and the current ratios between revenue and research and development expenditure.

This produced an estimate of the incremental long term revenue from the investment which was then adjusted by gross margins to produce an estimate of the surplus. [6]

Figure 11 below shows these results of a nominal $10 million public sector investment in each of the four top single technology components underlying the Internet of Things.

[6] As a formula: Surplus = ($ 10 million * Single Technology Weighting) / R&D to revenue ratio) * Gross Margin

© Strategy of Things, 2025. All rights reserved.

Single Technology Component	Investment ($m)	R&D to Revenue	Revenue from investment ($m)	Gross Margin	Surplus from Revenue ($m)
Hardware Sensors	$10	1.8%	$549	26%	$143
Standards Interoperability	$10	2.3%	$438	24%	$106
Software Data Collection	$10	3.7%	$269	27%	$72
Systems Security	$10	1.7%	$578	26%	$150

Figure 11: Economic Impact of Investments in Most Important Single Technology Components

IoT technology infrastructure gaps are comprised of multiple underlying single technology components. For example, the economic analysis for interoperability combines economic contributions from the single technology components of standards and middleware.

Figure 12 below shows the indicative revenues and surpluses of a nominal $10 million investment in each of the IoT technology infrastructure gaps corresponding to the Core and Intelligence gap categories. Our economic analysis shows that a nominal $10 million investment to address interoperability will yield a long-term cumulative return of $650 million and an economic surplus (profit) of $162 million.

Gap	Investment ($m)	R&D to Revenue	Revenue from investment ($m)	Gross Margin	Surplus from Revenue ($m)
Core: Interoperability	$10.0	1.5%	$650	25%	$162
Core: Privacy	$10.0	1.8%	$548	27%	$149
Core: Security	$10.0	1.8%	$566	27%	$150
Core: Connectivity	$10.0	1.2%	$822	23%	$189
Intelligence: Data Management	$10.0	1.1%	$889	27%	$239
Intelligence: Artificial Intelligence (Trust)	$10.0	1.5%	$670	25%	$167
Intelligence: Intelligent Devices	$10.0	1.6%	$626	25%	$158

Figure 12: Revenue & Surpluses from a $10 million Public Sector Investment in Core and Intelligence Gaps Across All Industries

For each of the IoT technology infrastructure gaps identified, an allocation of the $10 million research investment by industry was estimated using our economic model.

Figure 13 below shows the indicative results for the $10 million public sector investment in the core gap of interoperability, with the investment allocated across the nine industries based on percentages determined from our economic model. Similar results for the other core and

© Strategy of Things, 2025. All rights reserved.

intelligence gaps are included in the body of the report.

Industry	Investment ($m)	R&D to Revenue	Revenue ($m)	Gross Margin	Surplus from Revenue ($m)
Agriculture	$1.38	0.8%	$177	14%	$24
Construction	$0.85	0.8%	$109	23%	$25
Renewable Energy	$0.11	0.8%	$15	40%	$6
Insurance	$0.40	0.8%	$51	31%	$16
Healthcare	$3.68	8.3%	$44	52%	$23
Manufacturing	$1.30	2.3%	$56	35%	$20
Retail	$1.16	0.8%	$149	24%	$36
Smart Cities	$0.59	2.3%	$26	29%	$7
Transportation/Logistics	$0.53	2.3%	$23	21%	$5
Total	**$10.0**		**$650**		**$162**

Figure 13: Revenue & Surpluses from a $10 million Public Sector Investment in Interoperability

Figure 14 below shows the indicative allocations of the investment for the seven gaps.

Industry	Core: Interop.	Core: Privacy	Core: Security	Core: Connectivity	Intelligence: Data Management	Intelligence: AI	Intelligence: Devices
Agriculture	$1.38	$0.93	$1.06	$3.40	$0.00	$1.44	$1.34
Construction	$0.85	$0.31	$0.27	$0.00	$0.00	$1.08	$1.03
Renewable Energy	$0.11	$0.11	$0.13	$0.00	$0.00	$0.15	$0.15
Insurance	$0.40	$0.65	$0.55	$1.17	$0.00	$0.43	$0.29
Healthcare	$3.68	$4.27	$4.06	$0.00	$0.00	$3.29	$4.37
Manufacturing	$1.30	$1.26	$1.24	$5.43	$4.64	$1.54	$1.07
Retail	$1.16	$0.92	$1.05	$0.00	$5.36	$0.89	$1.06
Smart Cities	$0.59	$0.77	$0.80	$0.00	$0.00	$0.84	$0.41
Transportation/Logistics	$0.53	$0.80	$0.84	$0.00	$0.00	$0.34	$0.28
Total	**$10.00**	**$10.00**	**$10.00**	**$10.00**	**$10.00**	**$10.00**	**$10.00**

Figure 14: Indicative Allocations by Gap of a $10 million Public Sector Investment[7]

[7] Zero allocations occur when the underlying single technology components were not identified as an issue in either the survey or desk research.

© Strategy of Things, 2025. All rights reserved.

Areas of Opportunity for the Federal Government

In many cases, such as with core and intelligence gaps, there are significant existing industry efforts to address the gaps identified in each of the three categories. For example, there are numerous industry efforts supporting Standards Development Organizations to develop a variety of standards across many market sectors. In addition, industry participants are developing commercial solutions to address a variety of gaps. However, many of these gaps are too broad, complex and challenging for industry, academia or government to address on their own. Each stakeholder plays a vital and complementary role.

For instance, standards are a key requirement for interoperability. The federal government supports standards development by performing the pre-standards research and building on the foundational science needed for industry. Once done, industry then builds consensus standards based on this groundwork. At the same time, as IoT evolves the government conducts research to enable future IoT technologies so that they can be transferred or utilized by industry at some later point.

In other cases, technological advances emerge that offer the potential to address gaps in new and more novel ways. The federal government may invest in research to understand and develop these approaches which can then be transferred to industry to continue its development and commercialization.

Finally, industry participants may not address certain gaps because they are outside their short to mid-term priorities, may lack the expertise or capabilities or may conflict with their own proprietary approaches. Those situations represent “market failures” that the federal government has an opportunity to address.

Our research proposes a framework to examine government opportunities to address IoT technology infrastructure gaps identified in this research. The framework, shown below in Figure 15, focuses on five areas that the U.S. federal government may consider to facilitate the resolution of the IoT technology infrastructure gaps.

© Strategy of Things, 2025. All rights reserved.

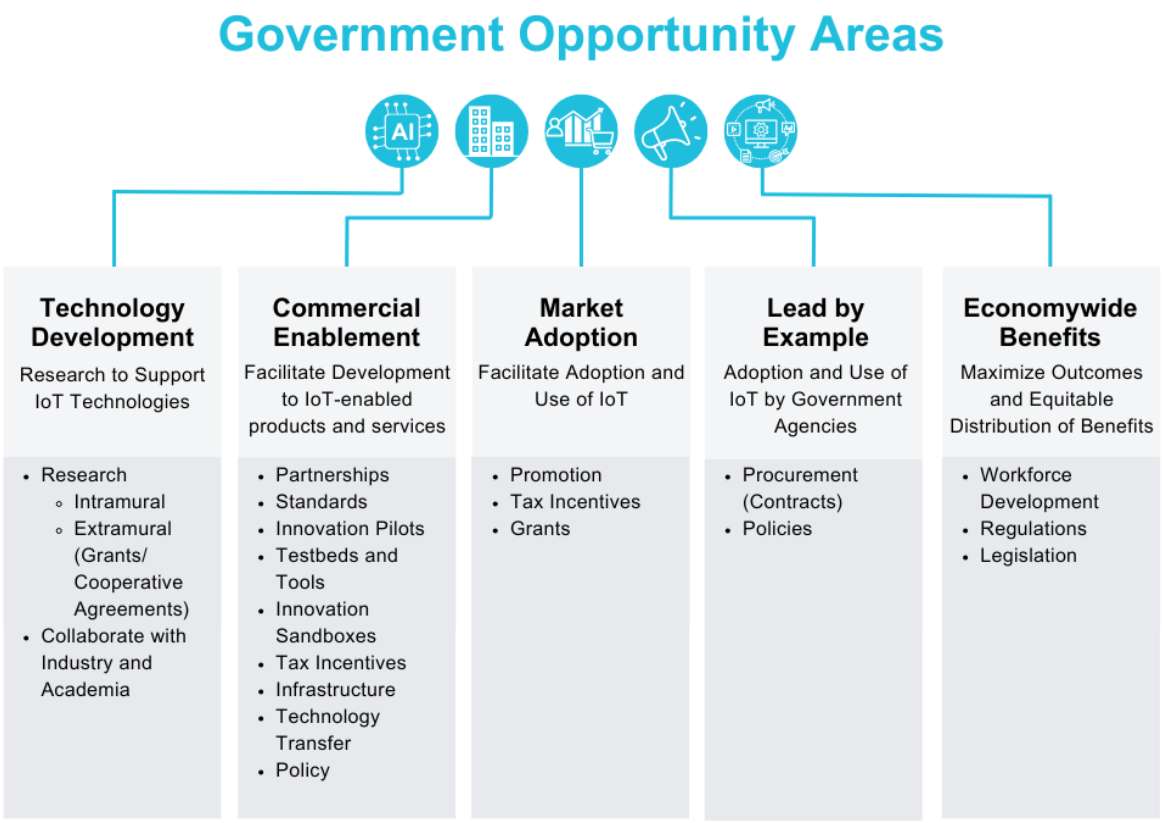


Figure 15: Government Opportunity Framework

Each of the five areas contains specific tools, capabilities and means that the federal government can employ to address these gaps. The list is representative rather than comprehensive. The specific gap, the industries it affects and the state of maturity of the technologies will determine the specific combination of these areas that are deployed to address the gap.

While these areas and capabilities are not new, government leaders and policy makers would do well to consider these capabilities as part of a broader portfolio of capabilities to provide a whole-of-government approach to more effectively address IoT technology infrastructure gaps. Some key reasons and support for such an approach include:

IoT faces a variety of technological and non-technological challenges. Both must be addressed to facilitate its continued development, adoption, operation and value realization.

IoT advancement faces a variety of technical and non-technical challenges. Some challenges, such as cybersecurity vulnerabilities and risks require technical responses. Other challenges, such as resistance to adoption and lack of a digital workforce, are major non-technical barriers hindering adoption and scaling. Another major area of non-technology challenges is regulations, including those at the federal, state and local levels, which impact what IoT can do, how it does it, and who may use and operate it.

Other challenges have both technical and non-technical aspects. For example, while the development of technical standards provides the foundation for interoperability, some users

© Strategy of Things, 2025. All rights reserved.

employ technologies with proprietary approaches because it "locks in" customers and yields higher profits.

Although the federal government has a variety of means to address different types of challenges, the government often applies them independently with limited coordination. For example, while the federal government participates in a variety of technical activities to support industry development of standards, it does not always leverage its significant buying power in procurements to specify the purchase of solutions that incorporate those standards. This can be a "disconnect" signal by the government that conveys a lack of market interest in standards, resulting in solution providers becoming reluctant to adopt the standards that can lead to interoperable systems.

Government leaders and policymakers addressing IoT challenges have the opportunity to consider a holistic approach that addresses both the technology and non-technology aspects. Initiatives that address only the technology challenges without simultaneously addressing the non-technology issues will not lead to the intended outcomes.

IoT technology infrastructure gaps fall into three categories. Different strategies and approaches are needed to address each category.

There is not a "one size fits all" approach to addressing IoT technology infrastructure gaps. IoT is in a continuous state of evolution, driven by a variety of technology, market and regulatory forces. This evolution creates gaps that fall into three distinct categories.

Each gap category addresses unique needs and requires specific approaches. Core gaps, concerned with the foundational capabilities that hinder the short and mid-term IoT development and adoption, are well-aligned for industry to address to support their commercial interests. In this category, the role of government is more strategic and targeted.

For example, while the federal government has traditionally conducted pre-standards research and science to enable industry to develop consensus standards, interoperability continues to be a major and long running core gap hindering IoT adoption and deployment.

In addition to continuing to support standards development efforts, the federal government is most effective augmenting industry efforts by addressing things industry cannot. One such opportunity is investigating emerging novel methods, such as the use of AI, to facilitate interoperability between incompatible devices. Furthermore, as IoT evolves, continued research is needed to address broader and more massive "systems to systems" interoperability gaps in support of the future hyperconnected economy.

In contrast, the federal government is well positioned to play a more substantial research role in addressing hyper-deployed gaps. This category of gaps hinders the future IoT-enabled economy and society, which will likely be teeming with billions of interconnected devices working autonomously and collaboratively. Industry, with its focus on short and mid-term priorities, does not have the interest nor the capabilities to address these gaps. Government investment is well-suited for addressing hyper-deployed gaps as it involves the development of transformational technologies and approaches that are forward looking and high-risk.

Government leaders and policymakers should consider the three categories of IoT technology infrastructure gaps as three portfolios of research opportunities diversified by industry and technology. For each gap category the government should have a unique research strategy and

© Strategy of Things, 2025. All rights reserved.

approach. Within each of the three categories, the approach to addressing an individual gap is tailored to meet the industry specific research objectives and outcomes.

The federal government has a comprehensive set of capabilities that is well suited to support a whole-of-government portfolio approach to addressing the technological gaps and non-technological challenges hindering IoT.

Our study has identified and categorized the federal government's capabilities to address IoT gaps into a framework with five broad areas. These capabilities, offered through various agencies, form a portfolio of capabilities. Each IoT technology infrastructure gap can be addressed by a specific combination of these capabilities within this portfolio.

Furthermore, each gap category has an approach that broadly determines what government portfolio capabilities should be utilized. For example, hyper-deployed gaps are forward-looking and are concerned with the later stages of IoT evolution. As a result, the most relevant identified government capabilities are focused on research and depending on the state of the technology, commercial enablement. In contrast, most current needs in the core gaps require the full range of government capabilities across the five broad areas.

Government leaders and policymakers would do well to consider taking a portfolio approach to addressing the IoT technology infrastructure gaps. The portfolio approach considered three perspectives: technology, economics and government. The technology perspective recognizes the diverse types and nature of the gaps, as well as the technology's maturity state along the IoT evolution cycle. The economic model provides information on the indicative allocations across the industries to address the gaps that will maximize outcomes for the broader economy. The actual uses of the funding allocations are informed by the specific federal capabilities available and needed to address the IoT gaps with those investment allocations.

This portfolio approach recognizes that multiple gaps need to be addressed simultaneously and the nature of those gaps varies depending on the evolutionary stage of IoT and its underlying technologies. In addition, some investments may be used to address gaps that may be more difficult to address than others and some gaps and industries may require more investments than others. Furthermore, the proposed set of actions undertaken by the federal government to address these gaps will vary depending on the nature of the gap, the roles of industry and academia, and the capabilities and resources available to address it.

The portfolio approach is more efficient, brings together a whole-of-government capabilities and expertise to the table to address both technology and non-technology gaps, reduces risks and offers the potential to maximize investment returns and economy wide benefits.

An investment portfolio approach informs IoT research funding priorities and offers the potential to maximize economic outcomes on an economy wide basis.

Technology infrastructure gaps hinder the continued development, adoption and operation of IoT in the industries studied. While the federal government has made research investments to address some aspects of these gaps, those investments are often made on an industry-by-industry basis without interagency coordination.

This study offers an economic analysis that determines the economic outcomes of a nominal $10 million investment in addressing specific IoT technology infrastructure gaps across nine industries. The quantification requires integrating qualitative data, the use of research and development to revenue ratios and gross margins for a particular industry and an estimate of the

© Strategy of Things, 2025. All rights reserved.

long term value of IoT. Each of these values has an associated variance which required assumptions, contributing to the decision to pursue a portfolio approach.

With these assumptions, the impact of a nominal $10 million federal investment in addressing the IoT technology infrastructure gaps was examined. Given the typical low ratio of research and development costs to revenue, a unit investment is associated with an indicative 55 to 89 times return in revenue and 12 to 128 times return in economic surplus.

The analysis also showed an optimum distribution, based solely on economic considerations, of that investment across the nine industries based on the findings from the integrated survey, interview and desk research data. For example, in the core gap of interoperability the research results led our economic model to allocate 36.8% of that investment to healthcare, followed by 14% to agriculture and 13% to manufacturing.

Government leaders and policymakers should consider taking a portfolio approach to address IoT technology infrastructure gaps. This approach takes into account the uncertainty of the quantitative analyses and the diverse nature of the technology infrastructure gaps in making informed allocations of limited research budgets.

This portfolio approach requires close coordination, collaboration, governance and management between federal agencies. With their agency specific missions and unique needs, coordination and management among agencies will be challenging. The potential central management and coordination of this portfolio may be done by an interagency group, such as the Networking and Information Technology Research and Development (NITRD) program or require a central and broader federal IoT organization[8] to be established.

Further study

The study developed an approach to address IoT technology infrastructure gaps that may be addressed by public sector investment. The approach could be extended to include other industries and strengthened to include more detailed economic and social impacts.

Managing the research portfolio across industries and the economy necessitates the ability to measure and monitor the economic benefits of these investments. A coordinating and collaboration structure and organization is required to design, implement and operationalize the proposed portfolio.

Finally, while the study examined nine industries and focused on IoT, the approach developed in this study has the potential to be replicated elsewhere to assess the economic benefits of public sector technology investments in other emerging technologies, such as AI.

[8] In 2024, a FACA, the IoT Advisory Board recommended the formation of a national IoT office. “Report of the Internet of Things (IoT) Advisory Board (IoTAB)”, October 2024. Link

© Strategy of Things, 2025. All rights reserved.

Recommendations

Based on a review of the gaps, the economic analysis and the portfolio of possible opportunities for the federal government to address these gaps, we make the following six recommendations to address the high level findings and infrastructure gaps identified in the research.

Recommendation 1. Consider research investments for the IoT technology infrastructure gaps informed by this study. These are:

- Core gaps: Interoperability, Cybersecurity, Privacy and Connectivity;
- Intelligence gaps: Data management, Trust in AI and Enablement of intelligent devices
- Hyper-Deployed gaps: IoT data ecosystem, Communications and network infrastructure, Advanced computing paradigms, and Human centric IoT systems.

Recommendation 2. Consider the findings and results in this report to inform federal IoT related research and development, investment, planning and policy considerations from a "whole-of-federal government" perspective. Furthermore, consider using a portfolio management approach to plan, guide and track the direction and implementation of investments and initiatives to address the gaps.

Recommendation 3. Consider building on this research by extending the study to additional industries, including those that are strategically important or emerging in importance. These may include mining and mineral processing, aerospace and defense and consumer packaged goods. This enables the portfolio approach to be broadened to additional economic sectors.

Recommendation 4. Refresh the economic analysis on a periodic basis to inform future federal research investments and initiatives as IoT evolves. Future refreshes of the research should consider technological advancements due to current federal investments, new emerging technologies and updated economic models based on the evolution of IoT. This provides the necessary information to assess the performance of the research portfolio.

Recommendation 5. Consider a future study to understand and quantify the economic and societal impact of the convergence of AI with IoT (AIoT), to create the AIoT-enabled economy.

Recommendation 6. Disseminate the findings of this report to industry and academia. Industry and academia should consider the findings, find opportunities and form strategic partnerships to collaborate with the federal government and agencies to address the gaps identified in this report.

© Strategy of Things, 2025. All rights reserved.

Conclusion

The Internet of Things (IoT) is an evolving technology infrastructure domain that has the potential to enhance U.S. global competitiveness, increase national resilience and increase national and economic security. The rising prominence of AI has further reinforced the importance and relevance of IoT.

Despite its strategic importance, advancement in IoT is hindered by a variety of technical gaps and non-technical challenges. These gaps are complex and broad, requiring active involvement from industry, academia and government to address. The federal government plays a critical role, bringing its "whole of government" capabilities and resources to complement efforts by existing efforts by industry and academia.

The study has identified a number of IoT technology infrastructure gaps that the federal government is well-suited to address. In addition, the study has quantified the impact on the national economy of addressing those gaps. The study further proposes a portfolio management approach to align gaps, research investments and federal capabilities and resources to efficiently address these gaps. It is the hope that the findings from this research will drive new collaboration models and partnerships between these groups to advance the research necessary to develop and build out the vision enabled by the Internet of Things.

In closing, the federal government is well-suited to address the gaps found. These gaps are too broad, complex and challenging for industry, academia or government to address solely. Each stakeholder plays a vital and complementary role. It is the hope of the authors that the findings from this research will also drive new collaboration models and partnerships between government, industry and academia to advance the research necessary to develop and build out the vision enabled by the Internet of Things.

© Strategy of Things, 2025. All rights reserved.

For more information contact:

Benson Chan
Email: benson@strategyofthings.io

Renil Paramel
Email: renil@strategyofthings.io

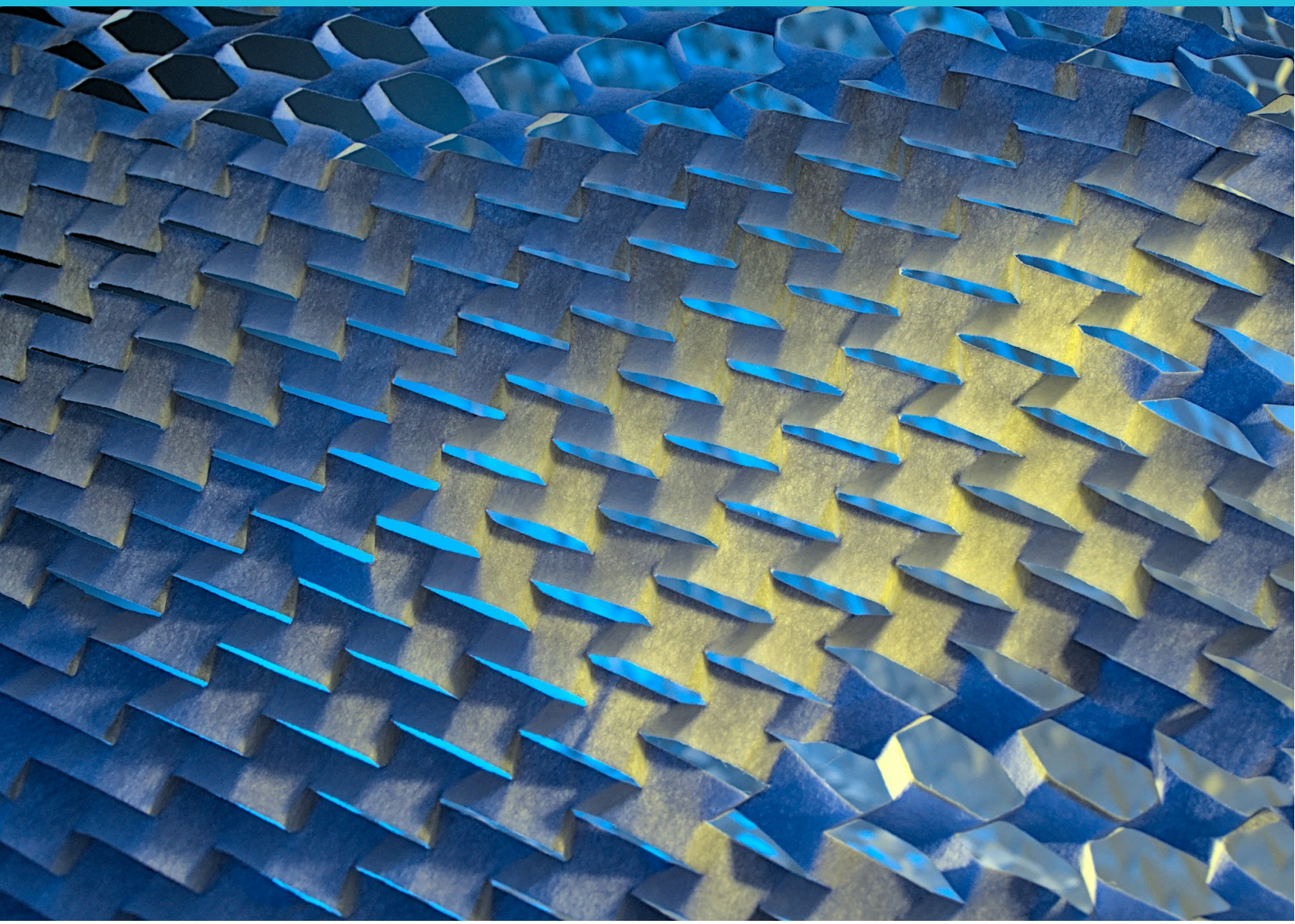
Christopher Reberger
Email: christopher@strategyofthings.io

Strategy of Things
www.strategyofthings.io

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the authors, except in the case of brief quotations embodied in research reports, industry articles and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Strategy of Things LLC
1305 Franklin Street, Suite 507
Oakland, CA 94612

marketing@strategyofthings.io



Main Report

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

© Strategy of Things, 2025

1. Introduction

The Internet of Things (IoT) is an evolving technology domain that is transforming our daily lives, impacting industry, academia and government, with significant economic, social and national security implications. IoT has the potential to enhance U.S. global competitiveness, increase the resilience of our nation and increase national and economic security. The rising prominence of artificial intelligence (AI) during the time period this study was conducted has reinforced the importance and relevance of IoT. The Internet of Things provides AI with one source of data to build and train algorithms and models. In turn, AI enables IoT systems to make sense of the monitored conditions and respond to these situations.

Recognizing its importance, IoT has been identified as an area of focus for the federal "Lab to Market" process[9], from research and development investments to technology transfer.

In September 2019, the U.S. National Institute of Standards and Technology (NIST) awarded research and innovation advisory firm Strategy of Things a cooperative agreement (grant) for an IoT study to assess the potential economic impacts, resulting from federal research investments, of meeting the Nation's need for technology infrastructure to support IoT.[10]

1.1. Purpose and overview

IoT is an evolving technology area with significant transformative benefits to U.S. global competitiveness, economic prosperity and national security. As with many early-stage technologies, however, it can take ten or more years to move an IoT related technology from incubation to market maturity.

The U.S. government invested more than $195 billion in research and development in Fiscal Year 2022.[11] Over $70 billion of this research is conducted at nearly 300 Government Owned, Government Operated (GOGO) and Government-Owned, Contractor Operated (GOCO) laboratories across the country.[12] Approximately $106 billion of this investment was in extramural research and development at universities, non-profits, and small and large businesses across the country.[13]

NIST seeks to understand the current state of IoT research efforts, the top technology infrastructure gaps and where future federal government research investments are appropriate to accelerate the adoption and deployment of IoT and to realize its economic benefits. While IoT offers a variety of societal benefits, the analysis of those was beyond the scope of this research.

Although there are significant existing industry efforts to address some of the gaps, many of these gaps are too broad, complex and challenging for industry, academia or government to

[9] "Lab-to-Market (L2M)", NIST Website. Link

[10] NOFO - 2019-NIST-TPO-IOT-01 ("Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)").

[11] "Federal Funds for Research and Development: Fiscal Years 2022–23", National Center for Science and Engineering Statistics. NSF 24-321, April 3, 2024. Table 1. Link

[12] ibid. Table 12.

[13] ibid. Table 9.

© Strategy of Things, 2025. All rights reserved.

address on their own. Opportunities exist for the federal government to play a vital and complementary role in addressing these gaps. For example, the federal government may well invest in research to understand and develop novel approaches to address gaps, which could then be transferred to industry to continue its development and commercialization. In other cases, government may be better suited to address gaps that are outside the short to mid-term priorities of industry participants, or where industry lacks the capabilities or where there are conflicts with industry proprietary approaches.

This study provides a set of analyses that identify IoT infrastructure gaps that have the potential to be efficiently addressed with public sector investments across a range of technologies and industries. Furthermore, the study quantifies the prospective benefits of those investments.

1.2. Research objectives

The objectives of the work are to:

- Objective 1. Assess the current state of the IoT technology covering research, development and adoption across nine industries. The industries examined include agriculture, manufacturing, construction, insurance, smart cities, retail, transportation and logistics, healthcare and renewable energy.
- Objective 2. Analyze these findings and identify technology infrastructure gaps. IoT technology infrastructure includes hardware, software, networking, applications, systems and standards.
- Objective 3. Perform an economic analysis to understand the potential impact on the national economy of the government appropriately addressing those gaps.
- Objective 4. Recommend potential areas for federal IoT-related research investments that will enhance U.S. competitiveness and national and economic security.
- Objective 5. Communicate these findings across the federal government, academia and industry through a variety of channels, including publications, speaking engagements, and journals as well as online and digital channels.

© Strategy of Things, 2025. All rights reserved.

2. Research Approach

Figure 2-1 shows an overview of our approach to identify the most important IoT technology infrastructure gaps for public sector investment along with the quantification method.

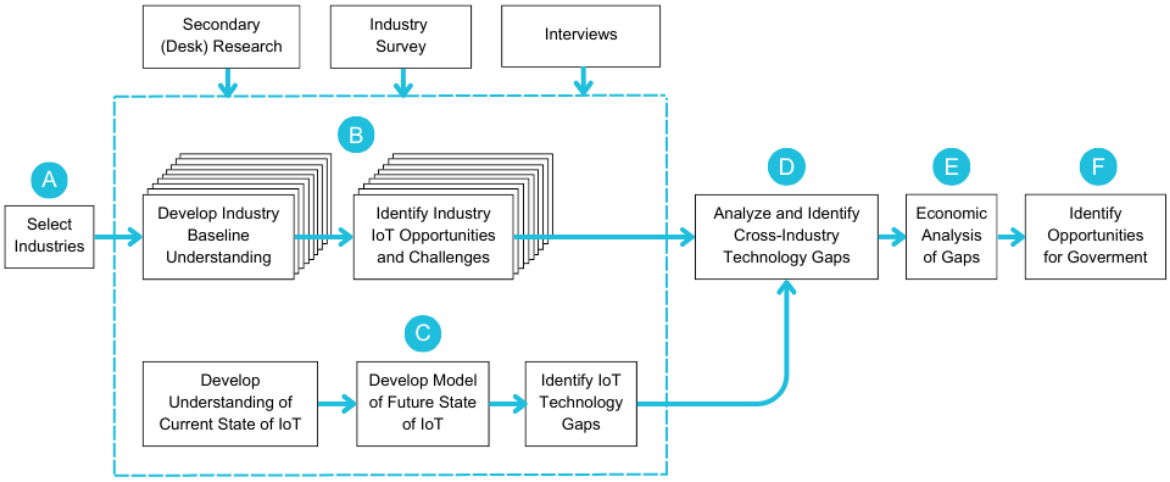


Figure 2-1: Infrastructure Gaps Research Approach

Step A. Industry selection was undertaken as the first step of the research approach. Some industries have an outsized impact on the U.S. economy and addressing gaps in those industries would likely have the most impact. Nine industries were selected based on considerations that included contribution to the national economy, strategic importance (including support of the CISA national critical functions[14]) and a subjective assessment of the "fit" of IoT with that industry.

Step B. The next step required developing a baseline background understanding of the selected industries. This included understanding how the industries "worked", the main industry activities and the value chain along with some of the top industry challenges.

This provided the context for identifying and understanding how and where IoT is used in the industry and the overall technical and non-technical barriers ("challenges"). The analysis focused on identifying technical challenges that aren't well addressed by industry and that could be an appropriate opportunity for the federal government to address.

Step C. In an independent research track, the work examined the current and future states of the development and evolution of IoT. This forward-looking understanding complements the industry-specific perspectives, which tend to be focused on the "here and now" and driven by market needs. The research work studied the drivers of IoT evolution and emerging trends.

The overall industry and technology research was conducted through secondary research, interviews and a survey. Secondary research consisted of literature reviews of government,

[14] National Critical Functions Set. Cybersecurity and Infrastructure Security Agency. Link

© Strategy of Things, 2025. All rights reserved.

scientific and industry publications, reports and online blogs. Interviews added context to some of the information collected from secondary research and the survey.

Interviews were selective and targeted a small number of people. The survey reached around 450 people and focused on a small set of specific questions.

Secondary research consisted of examining a variety of government, industry and academic sources, including blogs, white papers and published research papers.

Step D. To support the analysis stage of the research, the IoT technology challenges from each industry as well as the cross industry technology barriers ("gaps") from a future state of IoT were aggregated. From this, a cross industry technology infrastructure gaps list was developed.

The gaps selection process took into consideration the number of industries impacted, the strategic importance of the gap to IoT and its likely evolution and the opportunities for the government to participate in addressing a need that is not or could not be addressed adequately by industry. These gaps were then organized into three categories that aligned with the current and future states of IoT infrastructure development. An Internet of Things evolution model was developed to describe the current and future states of IoT.

Step E. An economic analysis was then performed looking at the possible economic surplus that could be achieved from a nominal public sector investment in the identified gaps.

Step F. Finally, a framework for possible government response was developed. This framework was used to examine previous examples of government actions and to identify areas of potential responses (including research investments) for the federal government. This covered both specific and representative federal government activities, programs and actions, along with more high level non-comprehensive opportunities to address the gaps.

2.1.1. 25 Technology gap collection framework

IoT is not one but rather a diverse set of technologies. To facilitate information collection for the underlying technologies that support and enable the operation of IoT[15] a six category framework of Hardware, Software, Applications, Networking, Systems and Standards was used for data collection and the gap analysis.

- Hardware. The physical components of an IoT solution.
- Software. Code and associated data intended to operate hardware within an IoT solution.
- Applications. Software that is designed to be used by people within an IoT solution.
- Networking. Collection of interconnected components and protocols that facilitate communication within an IoT solution and to other systems.
- Systems. Software providing services to other software within an IoT solution or to other systems.
- Standards. Rules, conditions or documentation established by consensus and approved by a recognized Standards Development Organization (SDO) body.

[15] "Economic Research and Analysis of the National Need for Technology Infrastructure to support the Internet of Things", Notice of Funding Opportunity 2019-NIST-TPO-IOT-01 Amendment 1, July 12, 2019. P. 9.

© Strategy of Things, 2025. All rights reserved.

Each of the six technological components was further assessed for comprehensiveness. Subcategories were introduced for each of the six technology areas to better capture the complexity and granularity of that area. This provided 25 single technology components. These are shown below in Figure 2-2.

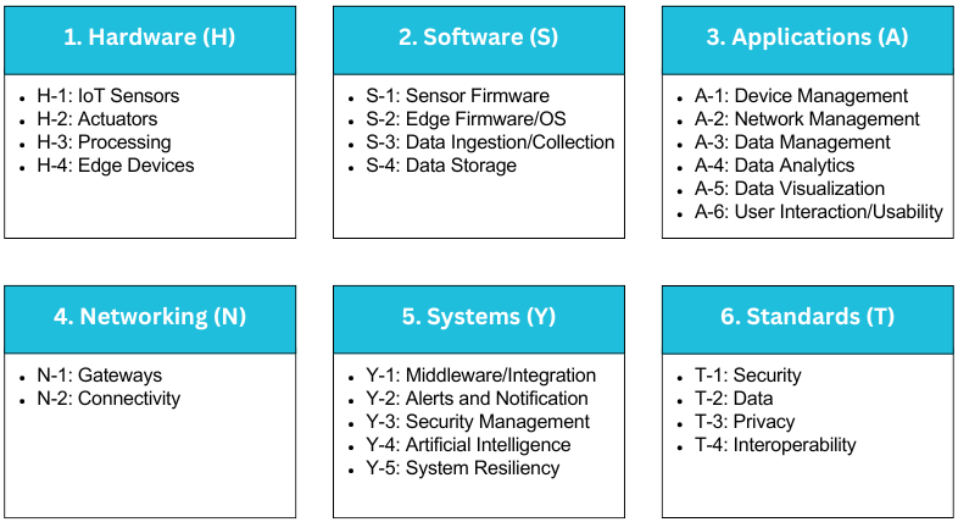


Figure 2-2: Technology Taxonomy: 6 Categories and 25 Single Technology Components

2.1.2. Economic modeling approach

The study's analysis provides a technological ranking of the 25 single technology components based on their economic impact adjusted by the role of the public sector. These rankings are then used to inform the decision on the most important IoT infrastructure gaps that have the potential to be remedied by public investment in the United States. The work used the following steps to produce a ratio ranked list.

- **Step A/B: Data integration for each industry.** The quantitative integration of all data collected from surveys, desk research and interviews adjusted by the role of the public sector.
- **Step B: Economic benefits of IoT to the United States.** We employed third party estimates of the long-term economic impact of IoT for each of the selected industries. This figure is used to adjust the rankings provided by the data analysis.
- **Step C: All industry technical weighting.** The integration of the quantitative and non-quantitative data provided weighted single technological component results for the nine industries. These results are adjusted by both economic impact and the role of the public sector.
- **Step D: Cross Industry Gaps.** Consider the cross industry gaps by developing combinations of investments in these single technology components.
- **Step E: Public sector investment.** An indicative estimate of the economic impact of a nominal public sector investment in the identified top single technologies and the core

© Strategy of Things, 2025. All rights reserved.

and intelligence gaps. A Monte Carlo analysis is performed on the cumulative single technology component results.

Figure 2-3 below shows a schematic of this approach.

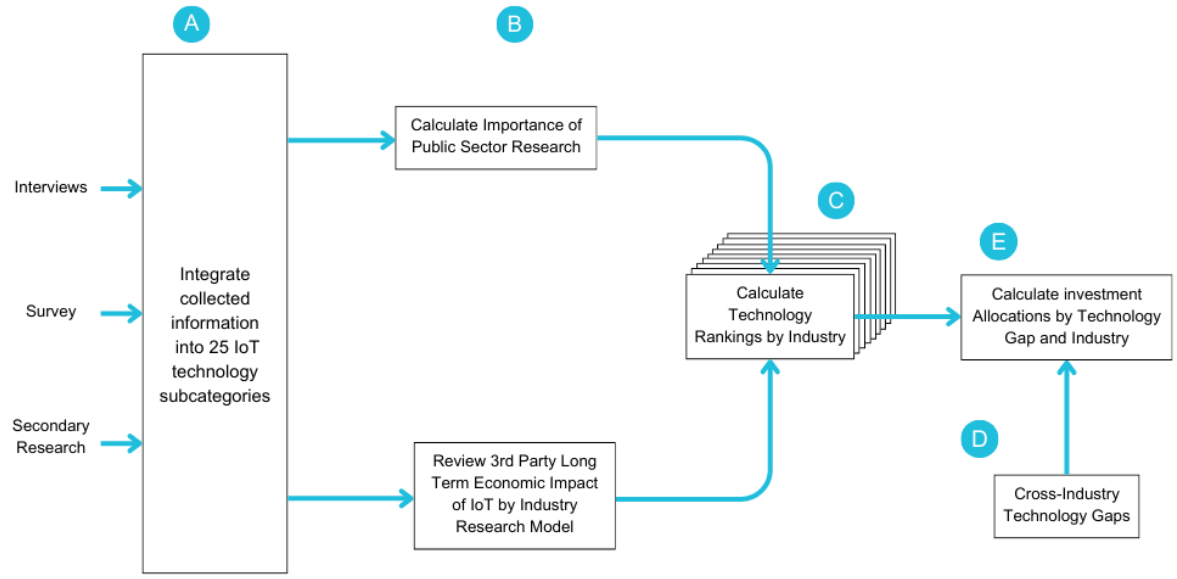


Figure 2-3: Ranking Technology Gaps Schematic

Economic model data collection

The economic model focused on what technology gap areas across industries deliver the greatest economic benefit from possible public sector investment or assistance. The model integrated data from desk research, surveys and interviews. The study analyzed around 450 survey responses, undertook approximately 50 personal interviews and performed desk research from both academic and industry sources. Detailed examples are shown below in Figure 2-5 to Figure 2-6.

© Strategy of Things, 2025. All rights reserved.

Different types of farming

- Row Crop farming
  - Crops are in a row, they can harvested and mowed over; cycle is repeated
  - Tractors are used here and many things are automated. Seed planting, fertilizer application, mowing, etc.
  - Relatively high tech – John Deere for example
- Permanent cropping
  - Vines, trees, etc. – plants that are fixed and certain things (fruits, nuts, etc.) are harvested. Plant remains. Can't process these with tractors
  - This type of farming is relatively low tech
  - Take irrigation for example. They use drip irrigation, but there are issues:
    - Underground rodents chew up the watering lines
    - Many are still triggered manually based on someone walking the field, dig into ground in a few places and look at soil moisture by hand (compacting dirt). This is relatively subjective process. Also, it is done during the day where evaporation is highest.
    - Irrigation is also problematic – lines are leaking and some areas of the field get a lot of water, while others are dry. Leaks create a lot of wasted water and drives up expenses.

Figure 2-4: Interviews Notes (Detail)

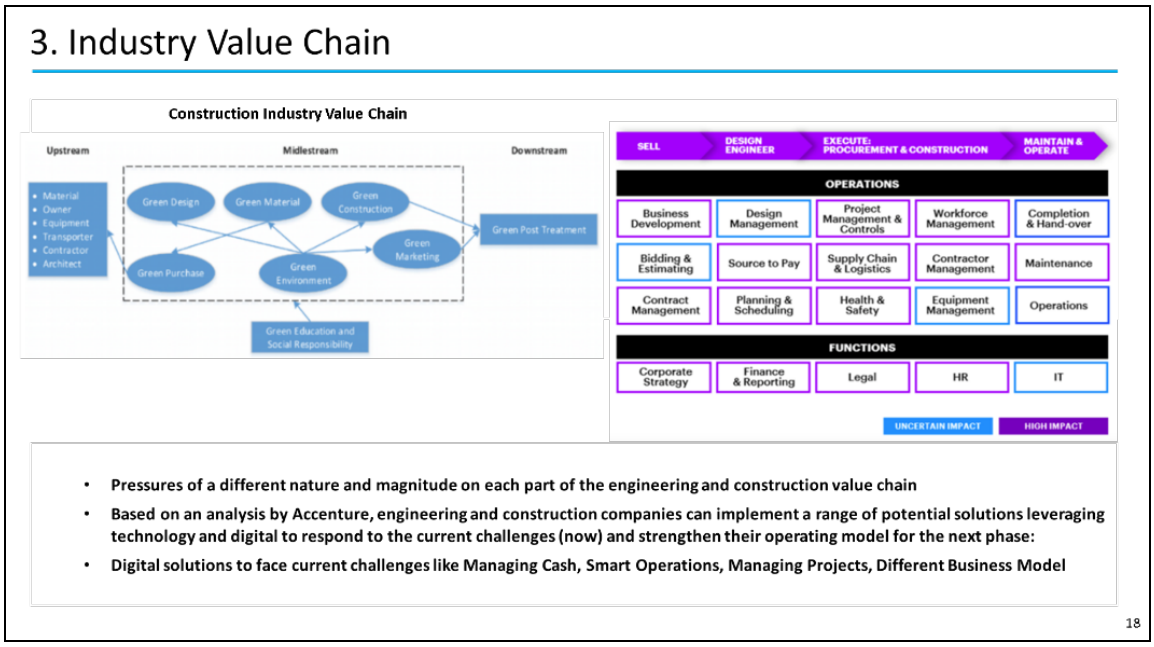


Figure 2-5: Desk Research (Detail)

© Strategy of Things, 2025. All rights reserved.

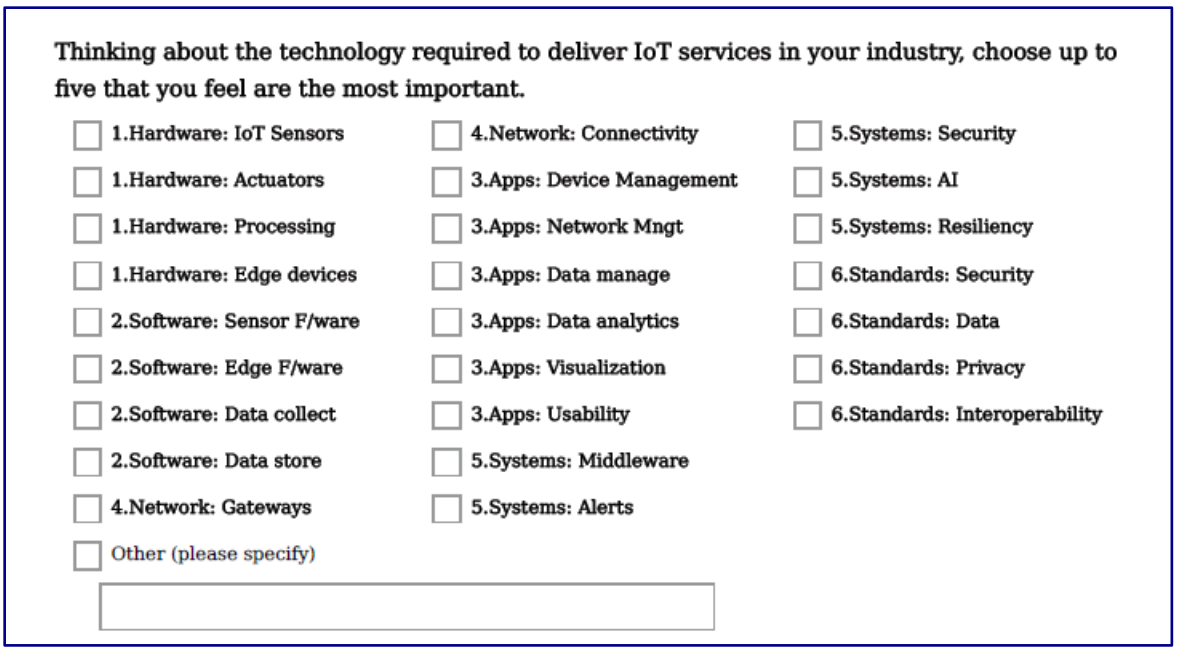


Figure 2-6: Survey Detail Showing 25 Single Technology Components

Economic model data integration

Figure 2-7 below describes how data from the surveys, desk research and interviews were integrated to rank the IoT technology areas for each industry. Details of the approach are available in Section 25.2.

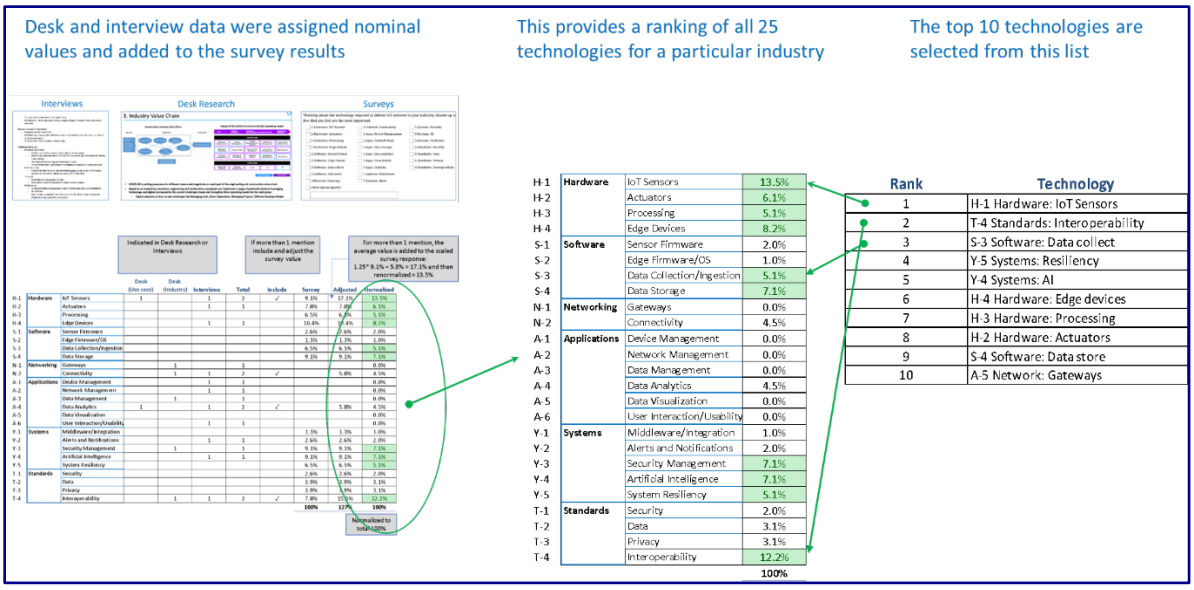


Figure 2-7: Integrating Survey, Interview and Desk Research Data

© Strategy of Things, 2025. All rights reserved.

Figure 2-8 below shows how the data from the surveys, desk research and interviews were weighted and ranked to provide an economy wide ranking of the technologies.

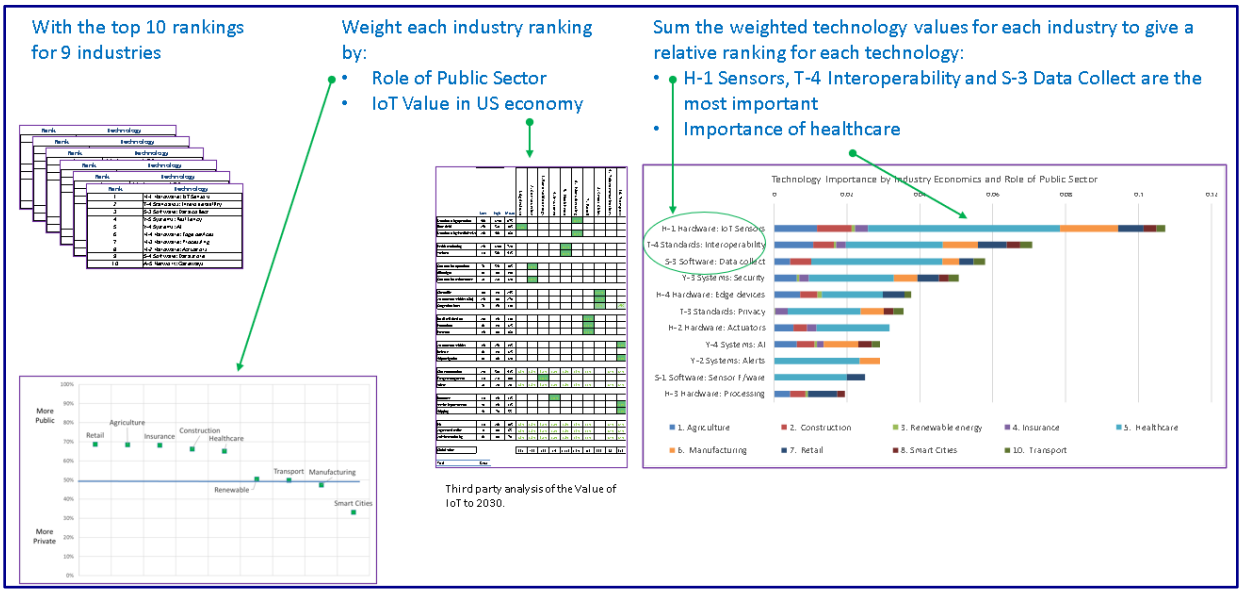


Figure 2-8: Weighting and then Ranking IoT Technology Subcategories

2.1.3. Portfolio Approach

Given the complexity and breath of the study, we employed a portfolio management approach that considered and integrated three perspectives: technology, economics and government. This approach is well suited for innovation management and recognizes the diverse types and nature of the gaps across industries, prioritizes the gaps across the ongoing evolution of IoT, and considers the range of possible responses and resources needed to effectively address these gaps.

This approach shown below in Figure 2-9 balances risk, resource allocation, capabilities, the maturity of the technology and the evolutionary stage of IoT to improve the likelihood of beneficial outcomes.

© Strategy of Things, 2025. All rights reserved.

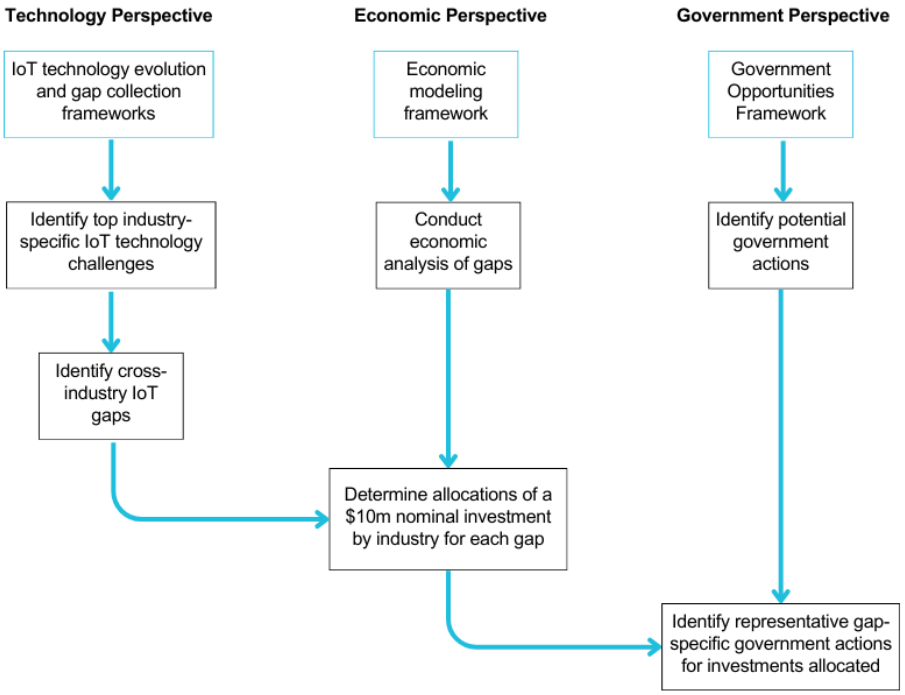


Figure 2-9: A Portfolio Approach

Three frameworks and models were developed to facilitate the analysis and creation of results in this research.

- A framework was developed to identify and prioritize a cross industry technology infrastructure gaps portfolio that is aligned with the evolution of the Internet of Things.
- An economic model was developed to quantify the prospective impact of addressing the identified technology infrastructure gaps. This model incorporates an investment portfolio approach to allocating investments across technology areas, infrastructure gaps and industries.
- An opportunities portfolio framework was developed to identify and classify the potential means and capabilities the federal government has to address the technology infrastructure gaps.

© Strategy of Things, 2025. All rights reserved.

3. High Level Findings Mapped to Objectives

The research uncovered ten key findings that map to the work's objectives. These highlight both technological and non-technological challenges in IoT development, as well as opportunities for public sector investment to enhance U.S. competitiveness and drive economic growth. These findings mapped to the objectives of the work are shown below.

Objective 1. Assess the current state of the IoT technology infrastructure covering research, development and adoption across nine industries.

- **Finding 1.** The benefits and economic value that IoT contributes to the economy are based upon the capabilities of IoT. These capabilities are evolving, driven by a variety of technological and non-technological forces. IoT technology and system infrastructure is expected to evolve in four distinct stages, each one building on the capabilities of the prior stage, with a corresponding escalation and scaling of benefits. This vision of the evolution of IoT is discussed in Section 4.2.1.

  The current state of IoT (Things become "smart"), involving the integration of sensors, embedded systems and a communications module onto a device to create "smart devices", represents the first stage. IoT devices collect and use data to create new capabilities, value and outcomes. AI and machine learning algorithms, tools and applications act on the collected data to create insights, enhance execution and optimize outcomes.

  The second stage (AI algorithms take action) is characterized by the convergence of IoT devices with artificial intelligence to support autonomous actions and operations of equipment, machinery, vehicles, and systems. The use of AI systems will shift from descriptive ("what happened?") and predictive ("what could happen?") activities to prescriptive ("what should be done?") and responsive ("act on it") activities. The emergence of edge computing servers and AI capable processors on IoT devices will enable low latency processing. When integrated with sensors and actuators, systems employing prescriptive and responsive AI algorithms can act autonomously in response to real time events.

  As devices add sensors and actuators, the ability to monitor, measure and control previously unavailable parameters creates consumption or outcome based "IoT as a Service" products from traditional products. IoT-enabled products offered as a service (IoT utility) represent the third stage (Utility and Outcomes) of IoT evolution. For a product to become a utility and be economically and technically viable, the outcomes it creates must be predictable, stable and reliable and consistent. AI algorithms play a key role in optimizing and enabling consistent outcomes.

  The fourth stage (Hyperconnected Autonomy) of evolution envisions a world that is massively connected with autonomous devices operating across the economy. As industries become integrated, automated and connected internally, they begin to integrate with other industries. As processes begin to integrate and interoperate across industries,

© Strategy of Things, 2025. All rights reserved.

so do relevant IoT systems. The automation of businesses that support multiple industries, such as transportation and logistics, becomes the glue that not only integrates automation between business value chains but also accelerates automation across multiple industries. Supporting the operation and maintenance of the autonomous economy will require convergence of digital and physical infrastructure, skillsets and resources.

- **Finding 2.** AI offers the potential to deliver transformational value to IoT in a number of different ways, including the efficient analysis of large volumes of data to create insights and outcomes.

  AI models implemented on IoT devices and edge servers could provide low latency processing to support the autonomous operation of devices and systems. In addition, there is an emerging use of AI to address interoperability challenges. AI could be used on a wide variety of devices to help detect and mitigate cybersecurity threats as well as optimize the operation of massively connected IoT device networks.

- **Finding 3.** Non-technological challenges are slowing the adoption, operation and realization of the value IoT brings to the economy. Our research identified seven common challenges.

  These include change or adoption resistance, a lack of digital skills, legacy infrastructure, data ownership, industry structure, regulatory and financial factors. Digital skills and change or adoption resistance/slow adoption are challenges that affect most of the industries studied.

  The specific challenges are discussed in Section 5.2.

Objective 2. Analyze these findings and identify technology infrastructure gaps.

- **Finding 4.** The development, adoption and operation of the Internet of Things is hindered by a variety of technological infrastructure challenges. While the specific nature and impact of the technological challenges differ by industry, they fall into one of eight common challenge categories.

  These challenges are:
  - Interoperability (inability of different IoT devices and systems to integrate, communicate and share information with each other).
  - Cybersecurity (vulnerabilities expose new attack surfaces that can be exploited to enter the network, steal information and disrupt operations).
  - Artificial intelligence (lack of trust as the produced outcomes may not be explainable, nor fair or ethical).
  - Data management (inability to fully manage the increasing volumes, velocity and growing complexities and requirements of the IoT data).

© Strategy of Things, 2025. All rights reserved.

- Privacy (unauthorized collection, storage and use of data and the unauthorized disclosure and sharing of private information).
- Edge computing (inability to process IoT data locally or in nearby servers outside of the cloud).
- Devices/hardware (inability of resource constrained devices to process and act on IoT data in real-time and protect against cyberattacks).
- Connectivity (inability for devices to connect to edge and cloud servers).

Of these, the three technological challenges that affect the most industries include interoperability, cybersecurity and AI. These challenges are discussed in Section 5.1. The specific industry challenges are discussed in Section 5.3.

- **Finding 5.** Our research identified a diverse mix of industry level technological challenges. To facilitate the mapping of challenges to gaps it was necessary to develop a framework that aligned the evolution of IoT with the challenge type. The resultant framework overlaid the three categories of gaps[16] with the four stages of the evolution of IoT.

  Core gaps represent foundational technological gaps that need to be addressed to support the operation and scaling of the Internet of Things across all stages of the IoT evolution.

  Intelligence gaps represent those technological challenges that need to be addressed to enable the data processing and analytical capabilities to create an autonomous and intelligent IoT.

  Hyper-Deployed gaps represent the future infrastructure that will support and scale a massively connected (hyperconnected) and autonomous IoT ecosystem across the economy.

  An explanation of the categories and their criteria is discussed in Section 6.

- **Finding 6.** The top core gaps are interoperability, cybersecurity, privacy and connectivity. The top intelligence gaps are data management, trust in artificial

[16] The terms "challenges" and "gaps" are both used to describe IoT technical deficiencies in this report. However, they are not interchangeable. We define IoT challenges as technical deficiencies found in the use of IoT in the specific industries.

For example, privacy protection is a technical deficiency or challenge identified in both cities and in retail, but the nature of those deficiencies differ. These challenges are aggregated and analyzed and a set of cross-industry technical deficiencies are identified. These cross-industry deficiencies are called "gaps."

Our research found privacy is a "challenge" at the industry level, and a technology infrastructure gap at the cross-industry level. However, at the cross-industry level, the privacy gap encompasses a broader set of deficiencies that is common across industries, whereas at a specific industry level, the nature of the technical deficiency for that privacy challenge is very specific to that industry.

© Strategy of Things, 2025. All rights reserved.

intelligence and intelligent devices. The top hyper-deployed gaps are the IoT data ecosystem, communications and network infrastructure, advanced computing paradigms and human centric IoT systems. The gaps are discussed in Section 6.

- **Finding 7.** The four most important single technological component investments for the public sector are: Hardware: IoT Sensors, Standards: Interoperability, Systems Security, Software: Data Collection. This result is presented in Section 26.2

Objective 3. Perform an economic analysis to understand the potential impact on the national economy of the government appropriately addressing those gaps s

- **Finding 8.** Using simple R&D to revenue ratios and gross industry margins, our analysis quantified the estimated economic impact of public sector investment in both the individual technologies and the core and intelligence gaps.

  A nominal public sector investment of $10 million in each of the single technology components[17] is associated with a long term cumulative revenue of between $269 million (Software: Data Collection) and $578 million (Systems: Security) and a corresponding economic surplus of between $72 million and $150 million.

  A nominal public sector investment of $10 million in each one of the core and intelligence gaps is associated with a long-term cumulative revenue for each gap addressed. The estimated long-term cumulative revenue generated varies by gap, ranging from $548 million for Privacy to $889 million for Data Management, and a corresponding economic surplus of between $149 million (Privacy) to $239 million (Data Management).

  A detailed discussion of the economic analysis is found in Section 7.

- **Finding 9.** The analysis quantified an optimal allocation of a nominal public sector investment of $10 million across the nine industries to provide the maximum benefit to the economy.

  These weightings were based on survey responses, desk research, interviews and the role of the public sector in that industry.

  For example, the most efficient public sector research investment of $10 million in IoT sensors would allocate 49% to the healthcare industry while 6% would go to retail.

  Results for the other three single technology components can be found in Section 7.1.2

[17] The 25-element taxonomy provides the set of single IoT technology components. The analysis looked at the impact of an investment in each of the top 4 single IoT technology components. Sets of single technology components were then chosen from the 25 and then combined to assess the impact of addressing the gaps at the core and intelligence levels.

© Strategy of Things, 2025. All rights reserved.

and in Section 7.1.3 for the core and intelligence gaps.

Objective 4. Recommend potential areas for federal IoT-related research investments that will enhance U.S. competitiveness and national and economic security.

- **Finding 10.** A framework was developed to categorize and identify potential government support actions to address the IoT technology infrastructure gaps found in this research.

  The framework identified five broad areas of activities for government support, many of which the federal government is familiar with and has employed with other novel technologies and innovations. These areas are technology development, commercial enablement, market adoption, lead-by-example, and economy wide benefits. However, in some areas, some specific examples of opportunities for addressing the IoT technology infrastructure gaps were identified. Additional details can be found in Section 8.3

© Strategy of Things, 2025. All rights reserved.

4. The Internet of Things (IoT)

At their simplest, IoT devices contain sensors and actuators to monitor and control the physical environment, an embedded system containing a microprocessor and memory to process the data collected and a means of communication with the Internet. The data collected from the IoT devices may be analyzed on the device or a nearby local server ("edge"), on a server in a moving vehicle ("mobile edge"), or on a server in a remote data center ("cloud").

An example of an IoT device is a connected vibration sensor in a factory that monitors the mechanical vibration levels of manufacturing equipment and alerts plant managers if a machine is behaving abnormally.

Another example of an IoT system is Light Detection and Ranging (LiDAR) sensors on autonomous vehicles that scan areas adjacent to a car and detect traffic and pedestrians. This information is sent to an onboard computer running driving algorithms, which then tells the car to act on the information to take any appropriate action or to avoid a collision.

Figure 4-1 below shows a typical IoT setup from data collection to use. [18] Data is routed from the IoT device to be processed through one of several wireless technologies such as Bluetooth, Wi-Fi, LoRaWAN, NB-IoT, 4G and 5G. The data are then aggregated by a local gateway router, transmission device or a remote cellular base station, where it is sent through a broadband infrastructure network to a remote cloud data center.

The data center collects the data, normalizes, stores, analyzes and acts according to algorithms or by user criteria. This information is then routed or made available to execution systems, such as Enterprise Resource Planning (ERP) systems or operations execution software applications for additional action.

Not all IoT applications route data to a cloud data center for storage and processing. For example, time sensitive IoT applications, such as sensors supporting autonomous driving, process data on the device, at a local gateway or at a local processing server.

[18] For our research, we elected to use a simplified but broader definition for IoT which included the device, the system and the broader enterprise IT environment it is connected and integrated into to capture the gaps more fully across the current and future states of IoT. We were informed by the various definitions for the IoT device, IoT component, IoT system and IoT environment as defined by NIST as specified in the IoT Definitions, January 2023 document. Link

© Strategy of Things, 2025. All rights reserved.

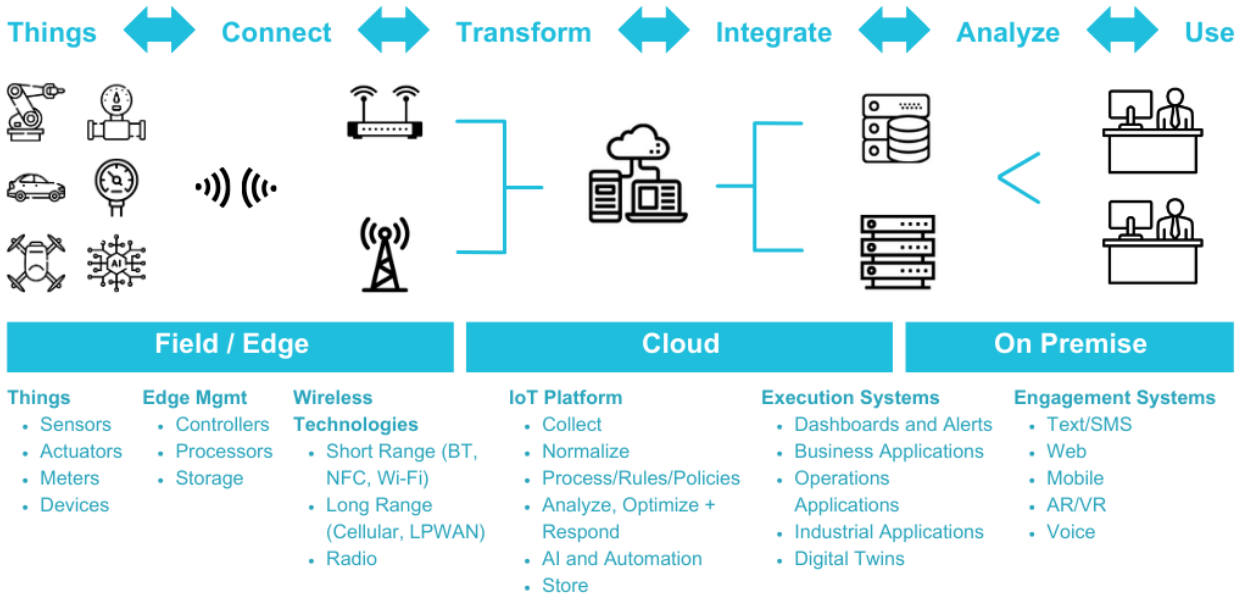


Figure 4-1: Typical IoT Solution Architecture Model

4.1.1. IoT technology stack

IoT is composed of diverse technologies which can be organized into six broad technology components as shown below in Figure 4-2. These component classifications are used in the survey, desk research and interviews to support the economic and infrastructure gap analyses.

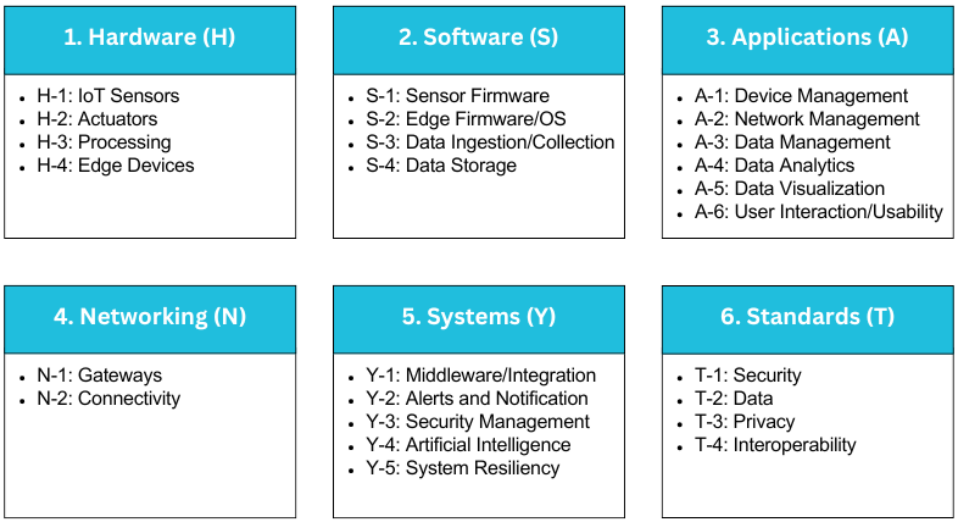


Figure 4-2: Six Categories for 25 Single Technology Components

© Strategy of Things, 2025. All rights reserved.

IoT technologies can also be organized collectively as a "stack" as shown in Figure 4-3 below. At the bottom of the stack are devices or "things" that sense and collect information or act. Information to and from the device is received and transmitted using one of several wireless methods.

The information is communicated to the cloud using one of several data protocols. Once ingested by the cloud platform, it is processed, stored and acted upon by various applications. The processed information is then presented to users through one of several possible methods. Each IoT use case or application uses a different combination of stack components.

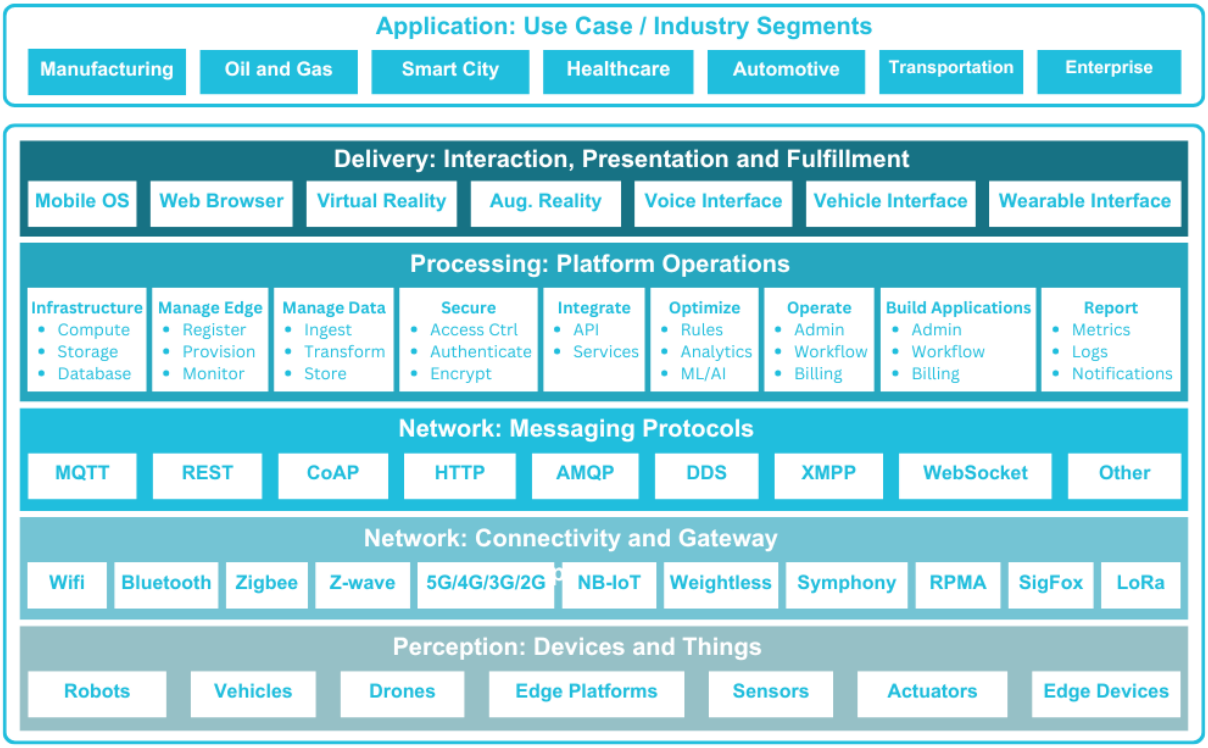


Figure 4-3: IoT Technology Stack (Non-Industry Specific)

4.1.2. Economic benefits of IoT

Adding sensors to the physical environment and collecting data yields value from doing old things in new ways and doing new things that were not previously possible. IoT drives value by creating opportunities for cost avoidance, increased efficiencies and productivity, reduced variability and waste as well as creating new classes of data enabled products and services. Figure 4-4 shows some representative new product, service and information offerings for an equipment manufacturer as an example.

© Strategy of Things, 2025. All rights reserved.

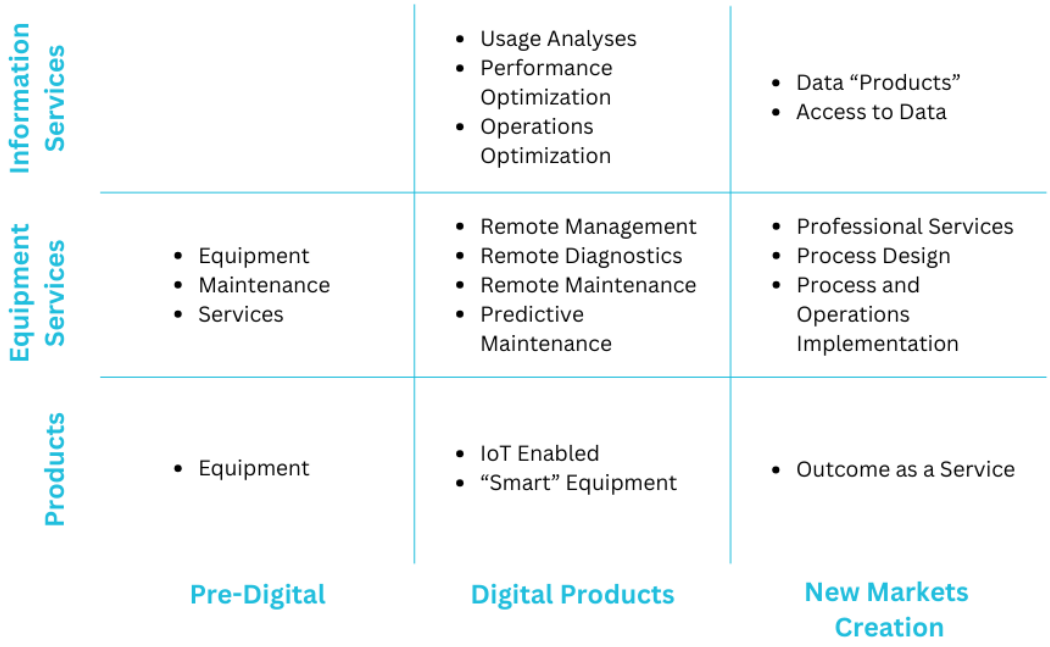


Figure 4-4: IoT Differentiator for Products and Services

Global consultancy McKinsey & Company estimated that IoT could enable $5.5 to $12.6 trillion of value globally between 2022 and 2030. Two-thirds, 62% to 65% of this value, is estimated to be captured by business to business (B2B) applications.[19]

Figure 4-5 below shows selected industry values in USD billions from the 2021 McKinsey study along with a mapping to the nine selected industries for this analysis. This provides a global estimate of $5,283bn for the selected industries which includes consumer surpluses.

[19] "IoT value set to accelerate through 2030: Where and how to capture it," M. Chiu, M. Collins and M. Patel. McKinsey Digital. November 9, 2021. Link

© Strategy of Things, 2025. All rights reserved.

	Low	High	Mean	1. Agriculture	2. Construction	3. Renewable energy	4. Insurance	5. Healthcare	6. Manufacturing	7. Retail	8. Smart Cities	9. Telecommunications	10. Transport
Manufacturing operations	460	1,290	875						100%				
Farm yield	250	520	385	100%									
Manufacturing: Predictive M	260	460	360						100%				
Health monitoring	240	1,200	720					100%					
Wellness	310	560	435					100%					
Construction operations	70	540	305		100%								
Oil and gas	80	300	190										
Construction maintenance	20	220	120		100%								
City traffic	100	390	245								100%		
Autonomous vehicles (City)	240	300	270								100%		
Congestion lanes	70	150	110								75%		25%
Retail self checkout	280	340	310							100%			
Promotions	60	190	125							100%			
Payments	140	180	160							100%			
Autonomous vehicles	140	250	195										100%
Defense	60	190	125										
Ship navigation	80	160	120										100%
Chore automation	290	580	435	0.2%	0.5%	2.0%	1.6%	1.3%	0.8%	1.0%		0.4%	0.4%
Energy management	130	230	180			100%							
Safety	20	20	20	0.2%	0.5%	2.0%	1.6%	1.3%	0.8%	1.0%		0.4%	0.4%
Insurance	130	140	135				100%						
Service improvements	90	140	115										100%
Shipping	40	70	55										100%
HR	110	260	185	0.2%	0.5%	2.0%	1.6%	1.3%	0.8%	1.0%		0.4%	0.4%
Augmented reality	30	100	65	0.2%	0.5%	2.0%	1.6%	1.3%	0.8%	1.0%		0.4%	0.4%
Activity monitoring	60	80	70	0.2%	0.5%	2.0%	1.6%	1.3%	0.8%	1.0%		0.4%	0.4%
Global value				386	429	195	148	1,165	1,241	603	598	3.3	515

Total	**5,283**

Figure 4-5: IoT Value by Industry and Allocation ($US bn)[20]

[20] Augmented reality, Activity monitoring and Safety percentages are allocated by percentage employment in the USA multiplied by U.S. share of world economy.

© Strategy of Things, 2025. All rights reserved.

These figures are then adjusted to estimate the value of IoT for the United States of $ 1,419 million as shown below in Figure 4-6. Further details are available in Section 25.1.

	1. Agriculture	2. Construction	3. Renewable energy	4. Insurance	5. Healthcare	6. Manufacturing	7. Retail	8. Smart Cities	9. Telecommunications	10. Transport
USA share of world	36%	25%	10%	31%	48%	18%	19%	23%	15%	14%
Value	139	106	20	46	557	223	116	137		74
% value	10%	8%	1%	3%	39%	16%	8%	10%		5%

Total	**1,419**

Figure 4-6: U.S. IoT Value Estimates by Selected Industry ($US bn)

4.2. State of IoT

The Internet of Things has seen significant growth and adoption across various sectors. Research firm IoT Analytics estimated that there were 16.6 billion connected IoT devices worldwide in 2023, up from 12.2 billion devices in 2021. This rapid expansion is projected to grow 2.5 times to reach 41.1 billion connected devices by 2030.[21] Research firm IDC estimated that by 2025, there will be 55.9 billion IoT devices generating 79.4 zettabytes (ZB) of data.[22] For comparison purposes, 1 ZB represents 30 billion 4K movies.[23]

This growth reflects the increasing recognition of IoT's potential to enhance operational efficiency and drive digital transformation. For example, the industrial sector has been a key driver of IoT adoption, with the share of IoT projects in manufacturing and industrial sectors increasing from 17% in 2018 to 22% in 2020. Other top sectors include transportation and mobility (15%), energy (14%), retail (12%) and cities (12%).[24] The top IoT applications are process automation (58% of the 2,089 IoT projects studied), quality control and management (55%), energy monitoring (55%), real-time inventory management (54%), supply chain track and

[21] "State of IoT 2024: Number of connected IoT devices growing 13% to 18.8 billion globally," S. Sinha, IoT Analytics, September 3, 2024. Link

[22] "How You Contribute to Today's Growing DataSphere and Its Enterprise Impact," D. Reinsel, IDC Blog, November 4, 2019. Link

23 "Seagate Is the First Company to Ship 3 Zettabytes of Hard Drive Storage," M. Humphries, PC Mag, April 8, 2021. Link

[24] "Enterprise IoT Statistics 2024 By Technology, Devices, Software," T. Pangarkar, market.us scoop, April 23, 2024 (updated). Link

© Strategy of Things, 2025. All rights reserved.

trace (54%), operations planning and scheduling, on-site facility track and trace (50%), asset performance optimization (48%), remote asset monitoring (48%) and location tracking (45%).[25]

Consumer applications are also fueling IoT growth. The global consumer IoT market is estimated to be $209.9 billion in 2024, of which $77 billion is in the United States. By 2029, the global market is projected to be $357.8 billion, growing at a compound annual growth rate (CAGR) of 11.3%.[26] Smart home devices, in particular, are gaining traction, with shipments forecast to reach 1.8 billion by 2025.

Despite the promising growth, IoT adoption and value realization still face a number of challenges. Global consultancy McKinsey & Company has cited change management as a challenge, with adopters treating IoT as a "technology project rather than an operating-model transformation." Other challenges include lack of interoperability, high installation costs, cybersecurity vulnerabilities and privacy concerns.[27] The IoT Advisory Board, a federally appointed advisory committee, cited in its 2024 report that industry adoption of IoT has been hindered by a number of challenges, including complexity and integration, cybersecurity, interoperability, data privacy and confidentiality, high implementation costs, lack of a skilled workforce, uncertainty about business value, change resistance and reliability and stability concerns.[28]

4.2.1. IoT evolution

The Internet of Things is evolving. IoT is composed of a set of diverse technologies at various stages of maturity and evolution. As these technologies evolve and mature, so will the functionality and capabilities of IoT. For example, the development of AI-capable microprocessors enables IoT devices to process and analyze data on the device immediately instead of sending it to a remote cloud data center for processing.

This section proposes a four-stage vision of how IoT will evolve. The analysis identifies the factors driving IoT evolution and ongoing trends that will facilitate the future state of IoT.

Figure 4-7 depicts our four-stage "IoT Evolution Model." It starts with our current state and proposes a future state that is informed by factors driving the IoT evolution, as well as emerging trends.

[25] "The top 10 IoT use cases," D. Paraskevopoulos, IoT Analytics, September 11, 2024. Link

[26] "Consumer IoT – Worldwide," Statista. Link

[27] "IoT value set to accelerate through 2030: Where and how to capture it," M. Chiu, M. Collins and M. Patel. McKinsey Digital. November 9, 2021. Link

[28] "Report of the Internet of Things (IoT) Advisory Board (IoTAB), B. Chan, D. Caprio, et al., September 20, 2024. Link

© Strategy of Things, 2025. All rights reserved.

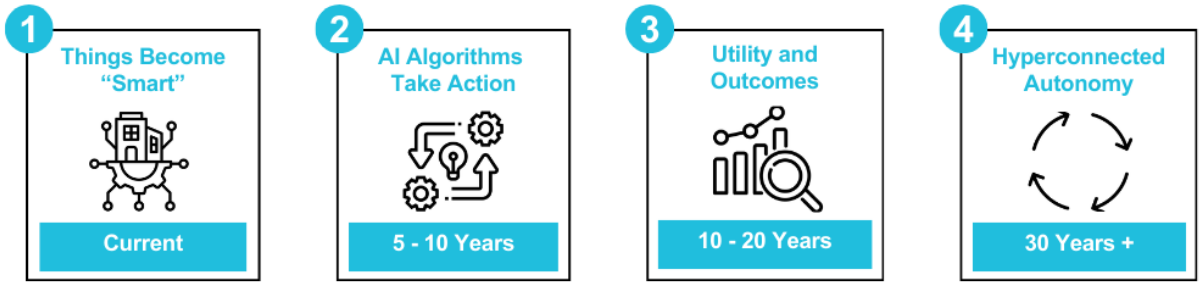


Figure 4-7: IoT Evolution Model

IoT Evolution stage 1: Things become "smart"

The addition of sensors and actuators and embedded systems to devices and machinery allows it and the environment around it to be monitored, managed and controlled in ways not possible before. For example, machinery can be monitored and operated remotely. Examples of "smart things" include our "smart phones", "smart thermostats" for homes and buildings, "smart watches", soil moisture sensors for agriculture, asset tracking sensors for inventory, vibration sensors on manufacturing equipment and so forth. The "smart" enablement of devices creates new economic opportunities for existing product manufacturers, as well as for new entrants in the marketplace. IoT devices collect and use data to create new capabilities, value and outcomes. AI and machine learning algorithms, tools and applications act on the collected data to create insights, enhance execution and optimize outcomes.

IoT Evolution stage 2: AI algorithms take action

Artificial intelligence (AI) is increasingly used to analyze large volumes of data to identify patterns, spot anomalies and create insights and understanding. Initial applications of AI augment human and manual activities. As the amount of collected data and data quality increases, along with rapid improvements in AI algorithms and hardware processing power, confidence in the outcomes produced from AI grows. The use of AI systems will shift from descriptive ("what happened?") and predictive ("what could happen?") activities to prescriptive ("what should be done?") and responsive ("act on it") activities. The emergence of edge computing servers and AI capable processors on IoT devices will enable low latency processing. When integrated with sensors and actuators, systems employing prescriptive and responsive AI algorithms can act autonomously in response to real time events. Examples of automated AI systems in use today include autonomous vehicles, resume screening, fraud detection and financial credit approvals.

IoT Evolution stage 3: Utility and outcomes

As devices add sensors and actuators, the ability to monitor, measure and control previously unavailable parameters creates consumption or outcome based "IoT as a Service" products from traditional products. Location sensors installed on cars allow users to car-share and pay by the mile. Heating, Ventilation and Air Conditioning (HVAC) systems equipped with high fidelity sensors and controllers will allow building owners to pay for the quality of the thermal comfort provided, instead of the heating and cooling systems. For a product to become a utility and be economically and technically viable, the results produced by actions from IoT must be

© Strategy of Things, 2025. All rights reserved.

predictable, stable, reliable and consistent. AI algorithms play a key role in optimizing and enabling consistent outcomes. The transition to a utility-based economy from a product-based economy brings significant disruptions but also yields significant benefits.

IoT Evolution stage 4: Hyperconnected autonomy

As industries become integrated, automated and connected internally, they begin to integrate with other industries. For example, the manufacturing ecosystem begins to integrate with the transportation and logistics industry, which integrates with the retail industry. As processes begin to integrate and interoperate across industries, so do relevant IoT systems. The automation of businesses that support multiple industries, such as transportation and logistics, becomes the glue that not only integrates automation between value chains, but accelerates automation across multiple industries. Supporting the operation and maintenance of the autonomous economy will require convergence of digital and physical infrastructure, skillsets and resources.

4.2.2. IoT evolution drivers and enablers

Industry analysts estimate that the number of connected IoT devices will grow from 11.3 billion in 2020 to 27 billion by 2025.[29] As the physical environment is equipped with additional sensors, the way those sensors and devices are used will evolve. Many of the IoT devices currently deployed operate in isolation or "islands." Driven by cross industry standards, use cases and middleware, these systems of connected devices integrate with other systems to form broader and bigger "systems of IoT systems."

Several interdependent factors will play influential roles in driving the evolution of IoT. The relationships between these factors are shown below in Figure 4-8.

[29] "State of IoT 2022: Number of Connected IoT Devices Growing 18% to 14.4 Billion Globally", M. Hasan, May 18, 2022. Link

© Strategy of Things, 2025. All rights reserved.

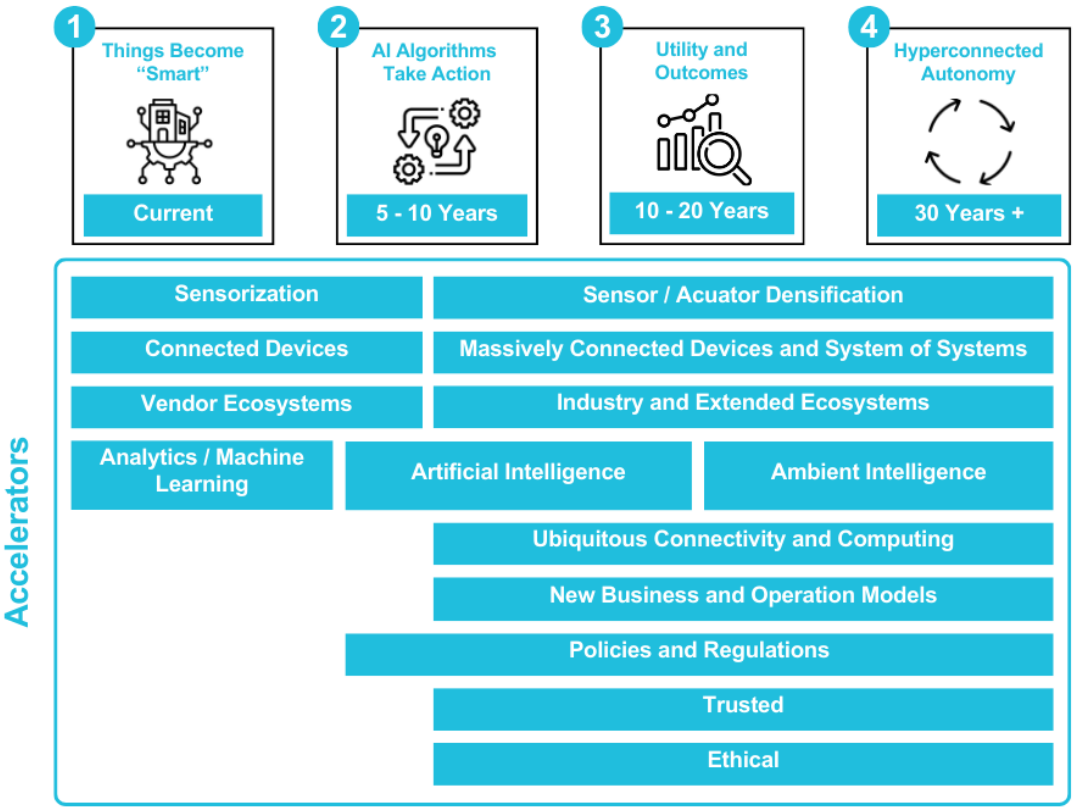


Figure 4-8: IoT Accelerators

The main factors that drive and enable IoT evolution are discussed below.

Interoperability and standards

Interoperability allows heterogeneous devices and systems to integrate, communicate and share information with each other. For example, information collected from one IoT device is used as input data by another device, or devices from different brands may communicate and work together in a system.

While interoperability is enabled by standards, it is difficult to achieve for a variety of reasons. In some areas, IoT technology is still new and rapidly evolving. There are many areas of IoT technology to be standardized and attaining agreement on a standard takes time. While open standards provide the potential for seamless interoperability, the current market is filled with products with proprietary protocols, "walled gardens"[30] device ecosystems and differing international standards and protocols. Some vendors believe their proprietary protocols are technically superior, some were first to market before standards developed, while others are concerned with commoditization of their offerings. For IoT to evolve, interoperability and open standards across devices and industries and countries are critical.

[30] A "walled garden" ecosystem is one in which a vendor or a group of vendors together form an ecosystem where their products are compatible with each other.

© Strategy of Things, 2025. All rights reserved.

Ubiquitous connectivity

The availability of connectivity service coverage supports IoT adoption. While urban areas have the infrastructure to offer different connectivity service options, rural areas and remote regions lack the same. Limited infrastructure, low population and population densities, terrain challenges and poor economic returns limit connectivity investments in these areas. Several government and private sector initiatives offer the potential to make connectivity ubiquitous. For example:

- A portion of the $65 billion in the federal Bipartisan Infrastructure Law will build infrastructure in underserved areas.[31]
- California is building a $6 billion middle mile fiber network to facilitate the creation of last mile services to underserved areas.[32] Middle mile networks connect the last mile with the broader Internet.
- The FCC is considering the use of the frequencies in the TV white space for connecting IoT devices over wide expanses of rural areas.[33]
- Several satellite operators are planning the launch of next generation Low Earth Orbit (LEO) broadband and IoT connectivity services to rural and underserved areas.[34]

These initiatives are supplemented by private enterprises establishing LTE and 5G private networks to connect campuses, factories and other facilities and augment commercial telecommunications services.

Ubiquitous computing

Analyzing data from IoT sensors and devices yields insights that optimize operations, boost efficiencies and create new value. While some of the data processing and analysis is performed in cloud data centers, other data are better suited to be processed at or near the point of use. This includes data from low latency applications and those in areas with unreliable connectivity. The development of AI capable microprocessors and microcontrollers, along with the emergence of efficient analytics (tinyML) algorithms optimized to run on resource constrained devices allow some data processing for certain types of applications to be processed on the device.

Telecommunications companies and other companies are building out mobile edge computing capabilities in cities. For example, one of the major telecommunications companies is building out a network of mobile edge computing centers across the country to support low latency, AI based applications. One U.S. startup company proposed placing servers in traffic cabinets in cities to support a variety of smart city applications. As IoT evolves, its myriad applications require the placement of computing infrastructure to support data processing to be located where it makes the most sense, whether that is in the cloud, at edge servers or on the device.

---

[31] "Fact Sheet: The Bipartisan Infrastructure Deal", White House Statement and Releases, November 6, 2021. Link

[32] State of California Middle-Mile Broadband Initiative. Link

[33] "FCC Expands TV White Space Use for Wireless Operations," M. Balderston, TV Tech, October 27, 2020. Link

[34] "Satellite IoT Connectivity: Three Key Developments to Drive the Market Size Beyond $1 Billion", E. Pasqua, IoT Analytics, August 25, 2022. Link

© Strategy of Things, 2025. All rights reserved.

Trustworthy IoT

IoT raises several cybersecurity and data privacy concerns. Cybersecurity is a priority for developers, adopters and privacy advocates. IoT devices expose new attack surfaces that can be exploited by criminals to enter the network, steal information and disrupt operations. Such data collected from IoT devices can be stolen, improperly accessed or used for purposes outside its initial design. In addition, algorithms can be biased to produce incorrect or unintended outcomes.

While interoperability, connectivity and processing provide the technical infrastructure for IoT to scale, a trust infrastructure is necessary for the IoT market adoption to scale. An example of a trust infrastructure is illustrated by the Strategy of Things' article on a trust model for a smart city.[35] In this model, data privacy and cybersecurity are only two of the elements that make up trust. The other elements include people and organizations, change and transformation management, governance, processes, algorithms, technology, user experience and strategic vision.

The article cites the air transportation industry as an example of a "trust" ecosystem "that ensures that flying is safe and reliable. A combination of rigorous engineering, regulations, policy, operational processes, stringent oversight and maintenance have made air transport safe. An ecosystem of partners, from government agencies, aircraft and component manufacturers, airlines, engineers and others worked together to ensure these outcomes."[36] For IoT to evolve and market adoption to scale, the focus on data privacy and cybersecurity must expand to build IoT trustworthiness.

Analytics and intelligence

Data collected from IoT devices are analyzed to create insights and drive positive outcomes. Some of these data are used to train machine learning (ML) and artificial intelligence algorithms to create those outcomes. As more sensors and devices are deployed, the quality of the data collected and used to train the algorithms improves, leading to more refined models, the extension of those models to more use cases and more accurate model outcomes. Continuing advances in algorithm development create new models that service more complex and computationally intensive applications, as well as enable more efficient processing on existing resource constrained microprocessors.

As connectivity and processing infrastructure expand, IoT will scale with new use cases that are ML/AI enabled. Continuing advances in interoperability and development of low-cost devices will eventually lead to an environment with ubiquitous intelligence. This state, called ambient intelligence, is reached when intelligence is embedded and integrated transparently into the physical environment.

This leads to a positive feedback cycle where developments in low-cost devices lead to more IoT devices, which increases the need for more connectivity service and coverage. As the number of devices scales, the amount of data collected grows. The need to process these data drives advances in computing infrastructure and algorithms to produce improved outcomes. These

[35] "Smart City Trust – Think Beyond Cybersecurity and Privacy", B. Chan, Strategy of Things blog, March 13, 2019. Link

[36] ibid.

© Strategy of Things, 2025. All rights reserved.

better outcomes increase the need for more devices to be integrated into the physical environment and the day-to-day interactions with people.

Convergence of IT, OT and enterprise systems

The Internet of Things is not a standalone technology. For IoT to scale into the economy and in daily use, there must be a convergence of Information Technology (IT), Operations Technology (OT), IoT and the cloud. While many uses of IoT today are in standalone applications or silos, for IoT value to be maximized, these different solutions across the spectrum must integrate and exchange information and data seamlessly.

There are millions of legacy and OT systems in use today, from manufacturing machinery to Programmable Logic Controllers (PLCs) and SCADA (Supervisory Control and Data Acquisition) systems. While some of these legacy and OT systems may offer data collection and control capabilities, they were not designed to connect to and communicate across the Internet.

It is neither feasible nor practical to replace all these legacy and OT systems with new connected "smart systems". Some of the legacy systems must be retrofitted with IoT technologies to enable them to connect, communicate and be interoperable with existing systems and modern smart systems. An ecosystem of solutions providers who build "bridging" solutions is required. In addition, as IoT evolves, the ability of users to maintain and sustain these legacy systems is critical. This integration is a journey that will occur over years, with progress mirroring advances in IoT capabilities.

Policies and regulations

These technological advances create new opportunities and challenges. For example:

- The integration of IoT into a manufacturing operation results in increased efficiencies which may reduce the size of the labor force and simultaneously require new skills.
- Facial recognition algorithms running on a city's network of video cameras help to deter and solve crimes but may lead to privacy violations when used outside of intended purposes or when inaccurate results are provided which may lead to false accusations, improper actions and other negative outcomes.
- Autonomous vehicles offer the potential of significant enhancements to traffic safety but may also incur significant and complex liabilities if an accident occurs.

From a historical perspective, technical advances often create both intended and unintended outcomes. Government policies and regulations help inform, facilitate and reduce the impact of unintended consequences while retaining the benefits of the intended consequences. While mature technologies are well suited for existing policies and regulations, new and emerging technologies often outpace the effectiveness of in place policies and result in unintended consequences.

For example, in San Francisco, the city enacted legislation that banned the use of facial recognition technology for cameras on city infrastructure and premises.[37] This legislation,

[37] "San Francisco Bans Police, Municipal Use of Facial Recognition Technology", M. O'Brien and J. Har, KQED, May 14, 2019. Link

© Strategy of Things, 2025. All rights reserved.

however, does not apply to merchants in a shopping district with cameras mounted on privately owned facilities.[38] Currently, San Francisco is running a 15 month pilot that will allow law enforcement to view video footage from private cameras.[39]

In addition, policies and regulations can be enacted by various government jurisdictions, such as cities, states, federal and international institutions. These well intended policies may conflict with one another, resulting in barriers to adoption, use, compliance and the value realized from IoT.

Innovative businesses and operating models

The application of IoT creates opportunities to extend and create new operating models and innovative businesses. Having the requisite technology infrastructure in place enables the creation of innovative business models and leads to market adoption of new business offerings.

For example, cellular connectivity and GPS-enabled tracking devices combined to enable ridesharing services. The success of the ridesharing businesses extended to the creation and adoption of shared micro-mobility services such as bike and scooter sharing. Besides transporting people, new businesses leveraged the existing infrastructure to deliver other goods such as meals and consumer products. Other examples of innovative models include “pay per mile” automobile insurance, predictive maintenance of equipment in factories and other industrial settings, and remote patient monitoring services in healthcare.

In areas without the technology infrastructure, however, these services are not offered. For example, remote patient monitoring services are not offered in areas with limited or no cellular connectivity. The availability of infrastructure enables businesses to create innovative applications for IoT, which drives new businesses and economic models. In a positive feedback loop, the success of these businesses drives the evolution of IoT, which then leads to new businesses development and emerging opportunities.

4.2.3. Emerging IoT trends driving IoT evolution

As IoT adoption continues to grow, IoT technology continues to mature. This study’s research identified ten current broad technology trends that are significant to the continued evolution and development of IoT. While these trends lead to the advancement of IoT, they also create new challenges and gaps to be addressed. These trends are discussed below.

Emergence of the edge

In a traditional IoT architecture, data is routed from the device to a remote cloud data center for processing and storage. Not all data collected needs to be or should be sent to the cloud for processing. In mission critical applications or in those where connectivity is intermittent or unreliable, processing is performed at the gateway or by the device itself. A 2022 survey of 910 IoT developers’, conducted by the Eclipse IoT Foundation, found that the top computing

[38] “San Francisco's Facial Recognition Ban Still Lets Corporations Spy on You”, N. Karlis, May 21, 2019. Salon. Link

[39] “Despite Privacy Concerns, San Francisco Supervisors Expand Police Access to Live Camera Feeds”, J. Har, KQED, September 21, 2022. Link

© Strategy of Things, 2025. All rights reserved.

workloads performed at the edge were artificial intelligence (38% of respondents), control logic (34%), data exchange across multiple nodes (22%) and data analytics (20%).[40]

Development of "low code" and "no code" software tools

Software tools which simplify coding for IoT adopters are emerging in the marketplace.[41] These 3rd party tools, integrated into popular IoT platforms, allow users with limited coding skills to create or update IoT applications. "No code" tools provide users with a graphical interface to "drag and drop" predefined "functions" in a logical sequence to create an application. "Low code" tools require limited skills, but instead of coding, the user is writing "scripts" to perform routine and non-routine actions, in a way similar to writing macros in Microsoft Excel. This "democratization" of integration and application development allows business users and consumers to create their own applications as needed without relying on a specialized IT department.

Increased open-source IoT ecosystem of users and developers

The use of open-source software is accelerating among business enterprises globally. According to a 2022 survey of 1296 global IT leaders, U.S. enterprise IT leaders reported their percentage of open-source software will grow from 53% today to 59% in two years.[42] The same report found that 73% of U.S. enterprise IT leaders are currently using edge computing and IoT and that 80% of them are planning to increase the use of open-source software for these technologies in the next two years.[43] There is a growing number of open-source development initiatives and projects in the IoT community. While this approach leads to lower development and ownership costs, continuous innovation, improved code functionality, performance and resilience and mitigation of vendor lock-in concerns associated with proprietary software, there are implications for long-term maintenance and cybersecurity updates. In addition to open-source software components, there are several open source IoT platforms and frameworks available to developers and users.

Developing cybersecurity standards and regulations for IoT

Cybersecurity is one of IoT's major concerns. Several high-profile events justify these concerns (i.e., the Mirai IoT botnet,[44] multiple security camera breaches, vulnerabilities found in open-source TCP/IP communication stacks used by millions of devices[45]). Industry has responded to these challenges through education and development of standards and certification programs (e.g., the Industry IoT Consortium has developed the Industrial Internet Security Framework,[46]

---

[40] "IoT and Edge Developer Survey Report", Eclipse Foundation survey, September 2022, Page. 12. Link.

[41] "Using Low-Code and No-Code in IoT App Development", L. Rosencrance, IoT World Today, May 17, 2021. Link

[42] "The State of Enterprise Open Source: A Red Hat report", P. Cormier, Red Hat report, February 22, 2022. Link

[43] See note 1446

[44] "Inside the Infamous Mirai IoT Botnet: A retrospective analysis", E. Bursztein, Dec 14, 2017. Link

[45] "AMNESIA:33 Vulnerabilities in TCP/IP Stacks Expose Millions of Devices to Attacks", I. Arghire, December 9, 2020, Security Week. Link

[46] "Industrial Internet Security Framework ", Industry IoT Consortium. Link

© Strategy of Things, 2025. All rights reserved.

the IoT Security Foundation has developed the IoT Security Assurance Framework,[47] the CTIA has developed a cybersecurity certification program for IoT devices[48]). In parallel with industry efforts to address cybersecurity concerns, governments have also acted (e.g., California SB-327: Information privacy: connected devices,[49] NIST Guidance for Manufacturers (NISTIR 8259)[50], European Norm EN303 645[51], FCC Cyber Trust Mark[52]).

Next generation satellite IoT connectivity services

Coverage is one of the most significant barriers to IoT adoption and operation. Many rural areas lack broadband service and cellular coverage. There are vast areas of the earth, such as oceans, forests, deserts and other areas that are remote, barren and unconnected. Driven by significant reductions in launch costs[53] and smaller, less expensive satellites, next generation space-based IoT connectivity services have emerged to provide coverage to the areas of the country where terrestrial based connectivity options are not economically feasible or physically possible. These privately owned and operated services complement terrestrial based connectivity services. Since 2018, 13 startups and 7 incumbent satellite operators have announced plans to offer satellite IoT services. These services come in two types – device to satellite connectivity and satellite backhaul (IoT gateway to satellite). Globally, there are around 5 million satellite IoT subscribers.[54] The number of satellite connected IoT devices is expected to reach 30.3 million by 2025.[55] Market revenues for connectivity services is expected to grow at CAGR of 14% from 2021 to 2026, reaching 1 billion USD by 2026.[56] Global revenues for satellite IoT device and connectivity services is expected to reach $5.9 billion USD by 2025.[57]

Rollout of 5G will accelerate and enable IoT

The fifth generation of cellular technology, also known as 5G, is in various stages of rollout across the United States. Compared to fourth generation technology (4G LTE, 4.5G), the performance improvements and capabilities offered by 5G are significant. [58] For example, 5G is up to 100 times faster, supports 1000 times more bandwidth capacity and can connect a

---

[47] "The Home of IoT Security Best Practice and Next Practice", IoT Security Foundation. Link

[48] "Internet of Things (IoT) Cybersecurity Certification", CTIA Certification. Link

[49] California SB-327. Link

[50] NIST Cybersecurity for IoT Program. Link

[51] "ETSI EN 303 645 Cybersecurity for Consumer IoT: what is it and why it's important", TUV. Link

[52] U.S. Cyber Trust Mark, FCC. Link

[53] "Space Launch to Low Earth Orbit: How Much Does It Cost?", T. Roberts, Aerospace Security, September 1, 2022. Link

[54] "Satellite IoT Connectivity: Three Key Developments to Drive the Market Size Beyond $1 Billion", E. Pasqua, IoT Analytics, August 25, 2022. Link

[55] "Satellite IoT: A Game Changer for the Industry?", H. Urlings, Satellite Markets and Research, September 3, 2019. Link

[56] See note 54

[57] See note 55

[58] "5G Technology and Networks (Speed, use cases, rollout)", January 5, 2022. Link

© Strategy of Things, 2025. All rights reserved.

minimum of million devices[59] in a square kilometer. One key 5G capability is its ability to support a broad range of use cases, including massive Machine Type Communication (eMTC) low bandwidth IoT applications, enhanced mobile broadband (eMBB) applications and ultra-reliable, low latency communication (URLLC) applications. Today, a variety of different connectivity options are used to support various use cases. The 5G's ability to slice the network to support these three use case categories, along with its high capacity and availability characteristics, will facilitate the development and deployment of IoT applications.

AI and machine learning capable IoT devices

The first generation of IoT devices contained simple microprocessors with limited processing and storage capabilities. Heavy computational tasks, such as analyzing data streams and running AI/ML algorithms, were offloaded to servers in the edge or to cloud data centers. Recent industry efforts have led to the development and introduction of more powerful and energy efficient AI capable processors for IoT devices.[60] The convergence of AI with IoT (AIoT) enables the ability to process data on the device itself, creates "smarter" IoT devices, yields faster device responses and allows the device to work without network connections. In addition to hardware enablement, other industry efforts like Tiny Machine Learning, or TinyML incorporate techniques and methods to run and operate algorithms specifically on resource constrained devices such as microcontrollers. [61]

Energy harvesting technologies deployed

Today, devices are powered through either electrical line power, solar power and both rechargeable and non-rechargeable batteries. There are, however, limitations to these power sources. Line power is only practical for a small subset of applications. Batteries have a limited lifetime and must be replaced or recharged. Energy harvesting solutions are emerging in the marketplace to partially address these power gaps and to power IoT applications. These technologies harness energy from the ambient environment and convert it to electricity. These energy harvesters include photovoltaic cells (light), piezoelectric transducers (vibration), RF (electromagnetic radio frequency) and thermoelectric generators (heat).[62] These harvesters currently produce small amounts of electricity and are only usable for select low power consumption applications. This includes powering low power IoT devices, as well as trickle charging batteries to extend their useful life. These energy harvesting solutions will augment rather than replace existing power systems. These systems, however, will allow many new IoT applications and devices to be created that would otherwise not be realizable with existing power systems. The importance of energy harvesting technologies to support IoT and other applications is significant. Researchers at EnABLES, a project studying the European infrastructure needed to power IoT, estimated that 78 million batteries that power IoT devices will be disposed every day by 2025 if battery life is not extended.[63] According to a 2021 article in industry publication Tech

[59] "5G and IoT: A failure to fly," D. Jones, EE Times, April 7, 2022. Link

[60] "Processors Roll for IoT and AI", G. Roos, March 23, 2020, Electronic Products. Link

[61] "What is Tiny ML and Why Does It Matter?", J. Riberio, December 22, 2020. Link

[62] "What is Energy Harvesting?", Versa Technology, August 24, 2021. Link

[63] "Up to 78 million batteries will be discarded daily by 2025, researchers warn," European Commission, July 23, 2021. Link.

© Strategy of Things, 2025. All rights reserved.

Briefs, a significant majority of the "trillion sensors that could be deployed within the next several years" will be of the ultra-low power wireless type and are ideal for integration with energy harvesting technologies.[64]

Multi-sensor data fusion becomes common place

Sensor fusion is the collection, joining, synthesizing and analysis of data from multiple and disparate sensors to create better insights for decision-making or acting than can be yielded by each sensor alone. For example, a car has a variety of different sensors, with each collecting information about its surroundings. When the separate data are integrated it provides a more complete context of the surroundings, so that the proper actions can be undertaken by the driver or the autonomous driving algorithms. In the future, the onboard car algorithms may supplement the car's on-board sensors with sensors from nearby cars and the roads to obtain additional context for decision-making and action. As the number and types of deployed sensors grows, the potential number of sensors that can potentially be fused will increase exponentially. An August 2021 Allied Market Research report projects that the global sensor fusion market will grow from $3.55 billion in 2020 to $19.8 billion by 2030, representing a CAGR of 19.7% from 2021 to 2030.[65]

Adoption of digital twin models

A digital twin is a virtual or digital model of a physical object, a group of objects, or a system. A machine, a factory, a building and even a city can be modeled as a digital twin. It acts and operates like the physical system. The digital twin is enabled by instrumented sensors and IoT, simulation and physics models and analytics algorithms. The sensors and IoT devices feed real time data into the digital twin, where simulation models and analytics algorithms act on it to replicate responses, actions and outcomes. A digital twin allows its operators to test new designs in a safe and controlled environment to see how the physical system may respond. Based on system responses, the physical design is updated and operational actions are undertaken. As the physical world is increasingly instrumented with IoT, more systems and operations can be modeled and the impact of digital twin models use will grow exponentially.

[64] "Energy Harvesting Can Enable 1 Trillion Battery-Free Sensors in the IoT," M. Hayes and B. Zahnstecher. Tech Briefs. October 1, 2021. Link.

[65] "Sensor Fusion Market", S. Wankhede and V. Kumar, August 2021. Link

© Strategy of Things, 2025. All rights reserved.

5. Technology and Non-Technology Challenges

This section provides details on the technical and non-technical challenges at the industry level.

5.1. Technology challenges

This research uncovered a variety of technological challenges hindering the adoption and advancement of IoT in each industry. While each industry faced a number of technology challenges, the study prioritized and included only the top three or four per industry. A combination of interviews, secondary research and surveys was conducted to identify and understand the most important and relevant opportunities and challenges to the development and adoption of IoT. Each research method approached the challenges from a different perspective.

For example, the survey targeted a large audience but asked specific questions that supported the economic analysis. The interviews targeted a small number of people who provided deeper insight and context to supplement the information already collected. Finally, the desk research, consisting of a review of online news articles, published research reports, vendor and government white papers, blogs, webinars, videos and other content provided a broad overview of the application of IoT in the industry.

The top challenges in each industry were selected from this broader perspective. As an example, while cybersecurity is a top three challenge in four industries, it was not a top three challenge in the other five industries. This does not mean that it was not an important challenge in those industries, but that there were other challenges that were of a higher priority. For instance, while cybersecurity is an important challenge for smart cities, our research found that privacy was rated a higher priority challenge hindering IoT adoption and operation.

Figure 5-1 shows the technology categories of challenges mapped against the industry. Each of these is discussed in detail below. Detailed discussions of the specific gaps by industry are documented in the corresponding industry appendices. The individual industry challenges have been aggregated into eight categories and discussed here from a broader cross industry perspective.

© Strategy of Things, 2025. All rights reserved.

Technology Challenges	Agriculture	Manufact.	Construct	Insurance	Cities	Tran & Log	Healthcare	Retail	Ren Energy
Interoperability	✓	✓	✓		✓	✓	✓		✓
Cybersecurity		✓	✓	✓	✓	✓	✓	✓	✓
Artificial Intelligence				✓		✓	✓	✓	
Data Management/Integration			✓			✓			✓
Privacy				✓	✓		✓	✓	
Edge computing	✓	✓			✓				
Devices (cost, others)		✓						✓	
Connectivity	✓	✓			✓		✓		

Figure 5-1: Top Technology Infrastructure Challenges by Industry.

Interoperability. Interoperability allows heterogeneous devices and systems to integrate, communicate and share information with each other. For example, information collected from one IoT device is used as input data by another device or devices from different brands may communicate and work together in a system.

The lack of interoperability is a major challenge due to the diverse range of equipment and systems that often use proprietary and incompatible protocols and limited adoption of standards. In agriculture, there is a mix of modern and legacy equipment not able to communicate with each other, making it difficult to integrate newer technologies with older machines. Similarly, manufacturing systems like MES, ERP, SCADA and DCS struggle with interoperability, which creates inefficiencies by limiting data sharing across these various systems. In construction, project teams bring disparate technologies to collaborate on a one-time basis, but these tools often lack the ability to communicate with each other, leading to manual data transfer and corresponding inefficiencies.

Other sectors like transportation, logistics and smart cities face similar issues. In transportation and logistics, the lack of universal standards for freight systems hampers data exchange, causing supply chain delays and increased costs. Smart cities, filled with IoT devices and systems owned by different entities, struggle with interoperability, locking cities into specific vendor solutions and preventing efficient data exchange between systems. Healthcare also suffers from fragmented, incompatible systems that make it difficult for medical devices to communicate, slowing down care and reducing operational efficiency. In renewable energy, interoperability is crucial for grid reliability, but inconsistent standards and policies hinder the integration of distributed energy resources (DERs) and energy management systems into the grid.

Ultimately, across these sectors, the lack of universally adopted standards and reliance on proprietary systems prevents seamless communication and data sharing, leading to inefficiencies, higher costs and reduced innovation. Without a concerted effort to adopt open standards and

© Strategy of Things, 2025. All rights reserved.

improve interoperability, these industries will continue to face challenges in maximizing the potential of their technologies.

Cybersecurity. IoT devices expose new attack surfaces that can be exploited by criminals to enter the network, steal information and disrupt operations. Such data collected from IoT devices can be stolen, improperly accessed or used for purposes outside its initial design. Cybersecurity challenges are increasingly significant in various sectors due to the growing integration of connected devices and the convergence of Information Technology (IT) and Operational Technology (OT)[66] systems. In manufacturing, formerly isolated OT systems are now accessible via the internet, exposing them to new cybersecurity threats. These environments were not originally designed with cybersecurity in mind, creating vulnerabilities as they become interconnected through IoT devices. Similarly, in the insurance industry, IoT devices, such as vehicle telematics and health monitors, introduce new attack surfaces and vulnerabilities, making insurance carriers attractive targets for cybercriminals due to their handling of sensitive data, including personally identifiable information (PII).

In the renewable energy sector, the integration of Distributed Energy Resources (DERs) like solar and wind systems into the grid introduces millions of potential cybersecurity vulnerabilities. These DERs, owned by independent producers using diverse IoT-enabled equipment with varying levels of security, pose significant risks to the integrity of the grid. The lack of standardized cybersecurity measures, coupled with the complexity of managing an automated environment with millions of devices, increase the potential for security breaches. Similarly, in healthcare, connected medical devices face significant cybersecurity risks, as many have long operational lives but are poorly supported by manufacturers. With limited computing resources, outdated software and the lack of basic protections like user authentication, these devices become vulnerable points in healthcare systems.

Across these sectors, the rapid adoption of IoT devices and the increasing interconnectivity of systems expose industries to heightened cybersecurity risks. Inadequate security measures, outdated equipment and varying levels of expertise among system operators contribute to these vulnerabilities, highlighting the need for robust IoT cybersecurity measures across industry.

Artificial intelligence. The use of AI in combination with IoT enables users to extract insights from volumes of data and take action based on that data. AI models running on IoT devices analyze data streams in real-time, identify patterns, predict outcomes, make intelligent decisions and may take autonomous action without human supervision. AI-driven analytics enable continuous learning and adaptation, allowing IoT systems to evolve and improve over time, leading to more accurate predictions and better resource utilization.

However, AI technology faces significant challenges across various industries due to issues with model accuracy, transparency, data quality and ethical concerns. In the insurance industry, AI can be used to analyze large volumes of data from IoT devices and other sources to support risk assessment and policy underwriting activities. But assessing risk is complex, often requiring

[66] According to cybersecurity company Otorio, Operations Technology systems are "hardware and software used in industrial control systems, such as supervisory control and data acquisition (SCADA) to monitor and manage physical processes. In contrast, IoT involves a network of interconnected devices and sensors that collect and exchange data over the internet. These two technologies work together to optimize industrial operations and enhance efficiency." Link

© Strategy of Things, 2025. All rights reserved.

years of data, expertise in understanding relationships and patterns and inferring correlations and outcomes. Furthermore, the lack of explainability in how AI models reach their conclusions can result in "proxy discrimination"[67] and other ethical concerns.

In transportation and logistics, AI offers transformative benefits such as optimizing routes and managing inventory, but its adoption is hindered by similar concerns. Limited access to high-quality data due to owners' reluctance to share data across the supply chains and lack of interoperability between systems, lack of transparency and bias in algorithms make businesses hesitant to rely on AI solutions. Similarly, healthcare is poised to benefit from AI, particularly with IoT-enabled medical devices that offer personalized care. However, challenges arise such as biased data, privacy issues that limit access to data to train models and explainable AI models hinder its use.

In the retail sector, privacy concerns limit data collection, which in turn affect AI algorithm development and training. Issues with AI model explainability raise concerns over biased or unfair outcomes.

These challenges across industries highlight the need for more explainable and trustworthy AI models, better data quality and solutions that address ethical concerns in AI decision-making.

Data management. Managing the volumes of data collected from IoT devices and systems is a major challenge. As IoT scales, so does data management complexity. The IoT data collected comes in a variety of types, formats and sizes. It resides and operates in a distributed environment, with data processed on the device, in moving vehicles, split among edge servers and the cloud. Some data are time-sensitive and must be processed immediately while others are stored for future actions. Data may be required to comply with industrial, state and national regulations.

Robust data management capabilities simplify these challenges and help unlock the value of IoT by enabling massive amounts of data to be collected, processed, stored, discovered, queried and analyzed. However, data management faces a variety of challenges. In the construction industry, the integration of IoT with Building Information Modeling (BIM) systems is challenged by siloed and fragmented data from various contractors, their reluctance to share data and a general lack of trust in a fragmented value chain.

In transportation and logistics, managing the vast data generated by IoT systems in the global supply chain is essential for smooth operations. With data flowing through multiple touchpoints such as manufacturing, transportation and warehousing, the challenge for supply chain and technology managers lies in handling decentralized and diverse data formats, while adhering to various regulatory standards. The exponentially growing volume of data requires businesses to have a scalable infrastructure capable of processing and storing information effectively.

---

[67] Institutions are barred from using prohibited traits, such as ethnicity and sex, from withholding or limiting services, setting prices, and so forth. Institutions instead use a neutral trait as a substitute for a prohibited trait to determine the level of services to be offered. For example, banks may use zip codes and profession, as one parameter of several to determine lending decisions. However, the use of zip codes may unintentionally lead to discrimination by proxy because some zip codes have a high proportion of certain demographics. The use of AI to analyze and predict patterns in data, including personal data, containing various proxy parameters may unintentionally lead to proxy discrimination.

© Strategy of Things, 2025. All rights reserved.

Similarly, in the renewable energy sector, managing IoT data is vital for grid operators and utilities to optimize the electric grid's performance. Data from wind turbines and solar panels needs to be processed and analyzed in real time to meet demand and improve grid operations. However, the diversity of data sources, varying data quality and regulatory complexities present significant challenges. Inadequate data management threatens the grid's automation, limits the use of AI and analytics for optimization and hampers regulatory compliance. Effective data management systems are critical for maintaining grid stability, fostering innovation and advancing toward a more autonomous energy grid.

Privacy. Privacy concerns surrounding IoT technologies are prevalent across various industries, affecting innovation and adoption. In the insurance industry, employed IoT devices collect significant amounts of personal data to improve products and services, but these technologies often lack robust privacy protections. Insurance regulators, sensitive to data privacy issues, impose strict limitations on data usage, which hinders the full potential of IoT implementation. State regulations, such as California's CCPA, add further requirements for transparency and control over personal data for the insurance industry, complicating the adoption of IoT solutions.

In smart cities, privacy is a major concern as IoT devices become integrated into urban infrastructure. Current privacy approaches for municipal entities, such as limiting data collection or banning facial recognition systems, are piecemeal and outdated. While these regulations aim to protect individual privacy, they also prevent cities from fully leveraging smart technologies to enhance urban living. As cities expand their use of IoT, relying on "device by device" privacy approaches are no longer sustainable or effective in managing the broader data privacy landscape.

In retail, IoT technologies offer retailers insights into customer behavior and enable personalized experiences. However, privacy regulations restrict the retailers' collection and use of customer data, slowing down IoT adoption in the sector. To balance the need for data with consumer privacy expectations, the development of privacy-enhancing technologies is becoming essential. These technologies could help retailers comply with regulations while still benefiting from the advantages that IoT offers, such as improved customer engagement and personalized services.

Edge computing. An increasing number of IoT applications employ edge computing to analyze and process the collected data. For example, applications that are latency sensitive or operate in an area with unreliable connectivity service may process data on the device or on a nearby edge server.

Edge computing presents significant challenges across several industries. In agriculture, future farms will rely heavily on sensors, drones, robotics and autonomous machines for operations, but much of the data needs to be processed locally due to limited broadband access, high cloud processing costs for data-intensive tasks like drone monitoring and the need for real-time responses in autonomous applications. The lack of enabling edge and cloud infrastructure in rural areas slows the development and adoption of agricultural IoT technologies, as current systems cannot efficiently handle the data processing needs on-site.

In manufacturing, factories are faced with a challenging wireless environment, where machinery, metallic surfaces and concrete structures interfere with signal propagation and create latency. Many manufacturing operations require real-time data monitoring, making on-device or local gateway processing essential. However, these operations often demand AI-capable microprocessors and advanced sensors, which are more expensive than traditional devices,

© Strategy of Things, 2025. All rights reserved.

leading to slower adoption. Additionally, many factories lack the necessary network infrastructure to support connected operations, further hindering their deployment of edge computing solutions.

For smart cities, edge computing is crucial for managing the growing number of IoT applications that demand real-time data analysis and processing at the device, gateway, or local server level. However, technical advances are needed in areas like scalable architectures, energy efficiency, interoperability and cybersecurity to fully realize the potential of smart city technologies. Without these improvements, cities will struggle to support the vast amount of data generated by IoT devices, limiting the effectiveness and expansion of smart urban environments.

Devices. The high cost of IoT devices presents a major barrier to their adoption across industries like manufacturing and retail. A large manufacturer may operate multiple factories containing thousands to hundreds of thousands of machines and production equipment of varying types. The cost to fit all production equipment in these factories with various devices can be cost prohibitive. The total IoT investment required is more than just devices, as hardware is usually around 30% of the initial implementation cost.[68] Additionally, the total cost of implementing IoT includes not just the devices, but also infrastructure upgrades, professional services and recurring costs for cloud services. Small and medium-sized manufacturers face even greater challenges due to limited capital and outdated infrastructure.

In retail, where profit margins are low, the cost of IoT devices is also a significant hurdle. Radio Frequency Identification (RFID) is the most commonly used IoT technology here, but while the tags themselves are affordable, the accompanying readers are expensive, with handheld readers costing up to $3,000 per unit and fixed readers as much as $20,000.[69] Although RFID is widely adopted for inventory tracking, other IoT technologies like beacons and condition sensors, which support additional applications such as remote monitoring services, are even more costly. Retailers are often unable to absorb these costs or pass them on to customers, making it difficult to justify large-scale IoT investments. To facilitate broader adoption, further research into lower-cost IoT technologies, such as non-silicon thin film sensors, is crucial.

Connectivity. Connectivity challenges significantly impact the effectiveness of IoT implementations in both agriculture and manufacturing. In agriculture, the ability to leverage IoT sensors and precision agriculture tools is constrained by connectivity issues. Many farms lack reliable broadband service, which prevents IoT devices from sending data to remote data centers for processing and storage. This connectivity gap hampers their ability to fully utilize advanced agricultural technologies and adapt to future needs.

In manufacturing, inadequate connectivity infrastructure further limits the potential of smart operations. Many factories, particularly those with outdated or insufficient network systems, struggle with poor wireless signal propagation due to extensive metal racking and machinery. This lack of modern network standards and infrastructure restricts the manufacturer's ability to deploy bandwidth-intensive applications, manage production equipment remotely, or track

[68] "How Much Will an IoT Device Cost Your Business?", Nabto blog, IDA HÜBSCHMANN, June 4, 2022. Link

[69] "Simple Cost Analysis for RFID Options – Choice Must Fit the Organization's Needs and Budget," T. Watson, April 28, 2015, IAITAM.org website. Link

© Strategy of Things, 2025. All rights reserved.

shipments in real-time. Rural factories, isolated from high-speed broadband, face even greater challenges, impacting their competitiveness and ability to adopt Industry 4.0 technologies.

Other sectors impacted by connectivity challenges include healthcare and rural communities. Access to healthcare is difficult for residents of rural communities. The federal government has designated 80% of rural areas in the United States as "medically underserved." These "medical deserts" are home to 20% of the U.S. population, but only 10% of the doctors. [70] The patient-to-primary care physician ratio is 39.8 per 100,000 in rural areas. In contrast, this ratio is 53.3 per 100,000 in urban areas.[71] Remote patient monitoring and telemedicine increases access to healthcare services for rural residents but is hindered by a lack of connectivity infrastructure. Similarly, the lack of connectivity hinders the adoption and operation of "smart city" IoT applications, such as infrastructure monitoring, for rural communities.

5.2. Non-Technology challenges

Our research uncovered a variety of non-technology challenges[72] hindering the adoption and advancement of IoT across industry. While each industry faced a number of non-technology challenges, the study included only the top three per industry. Detailed discussions of the specific challenges are documented in the corresponding industry appendices. The individual industry challenges have been aggregated into seven categories and discussed here from a broader cross industry perspective.

Figure 5-2 below lists the non-technology categories of challenges mapped against the industry it is found in. These are briefly discussed below.

[70] "'Out here, it's just me': In the medical desert of rural America, one doctor for 11,000 square miles," E. Saslow, Washington Post, September 28, 2019. Link

[71] "Top challenges impacting patient access to healthcare," S. Heath, Patient Engagement Hit, February 22, 2022. Link

[72] Non-technology challenges include challenges that may be technical in nature but are not related directly to the Internet of Things.

© Strategy of Things, 2025. All rights reserved.

Non-technology Challenges	Agriculture	Manufact.	Construct	Insurance	Cities	Tran & Log	Healthcare	Retail	Ren Energy
Digital Skills	✓	✓	✓	✓	✓	✓		✓	✓
Adoption Barriers (resistance, trust, right to repair, awareness, etc.)	✓	✓	✓		✓	✓			
Legacy infrastructure and operations		✓		✓	✓	✓	✓	✓	
Data Ownership/Privacy	✓		✓			✓	✓	✓	
Industry structure: Fragmented industry structure, Utility company alignment			✓			✓			✓
Regulatory compliance, uncertain regulatory treatment				✓		✓	✓		✓
Financial (funding, ROI, capital)	✓	✓			✓			✓	

Figure 5-2: Top Non-Technology Challenges by Industry.

Digital Skills. The workforce's lack of digital skills is a significant barrier to the adoption and scaling of IoT across various industries, hampering innovation and efficiency. In agriculture, modern farmers require expertise in data analysis, robotics, IoT and precision agriculture, but the workforce lacks these technical skills. The insurance sector faces similar challenges, as a shortage of digital talent, exacerbated by an aging workforce, limits the industry's ability to innovate and digitize operations. Smart cities, too, struggle with a shortage of skilled workers in software development, data science and systems integration, slowing down the implementation of IoT technologies. In transportation and logistics, the scarcity of IT professionals, combined with a perception of fewer career opportunities, is hindering IoT adoption, with many companies lacking in-house digital talent. The retail industry also faces a significant digital skills gap, particularly in integrating IoT with supply chain management and customer systems, preventing the scaling of emerging technologies. Similarly, the renewable energy sector requires digital skills in IoT, AI, data science and cybersecurity to optimize operations, but the workforce often lacks these essential capabilities, slowing the digitization of renewable energy infrastructure.

These widespread skills shortages are delaying the advancement of IoT and digital transformation across the economy, making it harder for industries to enhance productivity, innovate and meet evolving technological demands.

Adoption Barriers. Adoption resistance to IoT across various industries is significantly hindering its integration and growth in the economy. In agriculture, the "right to repair" issue creates a major barrier as modern equipment relies on IoT and cannot be easily fixed by farmers, leading to costly and delayed repairs that disrupt critical operations. Additionally, IoT adoption is slower among smaller farms due to connectivity challenges, wariness of new technology and reliance on personal experience. In the construction industry, a resistance to change, driven by a

© Strategy of Things, 2025. All rights reserved.

mindset of maintaining the status quo and risk aversion, further delays IoT adoption despite its potential to improve operations and compliance.

In sectors like smart cities and transportation, IoT integration faces challenges due to governance, lack of public trust and a culture resistant to change. Public concerns around privacy, cybersecurity and unauthorized data usage create trust issues, particularly in smart city projects, slowing the scaling of IoT. Similarly, in transportation and logistics, fears of job losses, transparency and performance issues result in slow adoption. Even in manufacturing, U.S. companies lag Europe and China in adopting Industry 4.0 technologies, which limits the broader economic benefits IoT could provide across industries.[73]

Legacy infrastructure and operations. Legacy infrastructure in various industries, such as transportation, logistics, retail, insurance and cities and municipalities, hinder the adoption of IoT and digital transformation. In transportation and logistics sectors, outdated software and hardware remain deeply embedded in operations, creating challenges like incompatibility, data silos, inflexible operations and limited scalability. These obstacles prevent companies from fully leveraging IoT technologies, modernizing processes and innovating their offerings. Similarly, in retail, legacy infrastructures are a significant barrier to digital transformation, with 38% of 104 retailers in a 2022 survey indicating their existing infrastructure could not support IoT.[74] This limitation affects retailers' abilities to meet evolving customer demands, personalize services and integrate IoT applications into operations.

The insurance industry faces similar challenges, where legacy systems and operations prevent insurers from innovating and transforming their business models to meet new customer needs. Traditional insurers struggle with outdated systems and processes that limit their ability to gain a comprehensive view of their customers, while digital-first "insurtech"[75] companies thrive. The high costs and risks of modernizing these legacy infrastructures make digital transformation a difficult endeavor for insurance firms. Additionally, in cities, legacy infrastructure drives up maintenance costs, hinders efficiency and increases cybersecurity risks, diverting resources away from innovation and making it harder to modernize public services. These pervasive issues with legacy infrastructure across industries are stalling IoT adoption and digital progress.

Data ownership and unauthorized usage and privacy. Data ownership, unauthorized usage and privacy concerns pose significant challenges to IoT adoption in industries like agriculture and healthcare. In agriculture, farmers are particularly protective of proprietary information, such as planting times, input mixes and livestock management practices. With IoT systems increasingly collecting this valuable data, 77% of 400 farmers surveyed by the American Farm Bureau Federation in 2016 expressed concern about who can access their data. Additionally, 67% indicated they would consider how third parties use and treat their data when choosing

[73] "Powering up the Connected Factory: The 2019 MPI Internet of Things Study", BDO USA LLP. Link

[74] "A Deep Dive into Retailers' Views About RFID and the Internet of Things", B, Kilcourse and S. Rowen, Retail Systems Research Benchmark Report, April 2022. Link

[75] Insurtech is a combination of the words insurance and technology. Insurtech companies use technology and innovation to create innovative offerings and services than those offered by traditional insurers.

© Strategy of Things, 2025. All rights reserved.

technology providers, highlighting the importance of transparency and control over data ownership in the agricultural sector.[76]

In healthcare, the growing use of consumer IoT devices like fitness trackers and wearable health monitors has enabled users to track vital health information, such as heart rates and sleep patterns. These devices can provide healthcare providers with valuable insights, leading to more accurate diagnoses and improved patient outcomes. For example, a smart watch may detect atrial fibrillation in a patient, allowing doctors to review the recorded data for a more comprehensive diagnosis. While the HIPAA Act of 1996 established strict regulations to protect patient data, ensuring that both clinical and non-clinical devices used for diagnosis and treatment comply with privacy standards, they do not apply to consumer health trackers.[77] As IoT technology continues to advance, balancing innovation with data privacy and ownership will be essential across industries.

Industry structure. The structure of certain industries poses significant barriers to the adoption of IoT technologies. In the renewable energy industry, the business model of Investor Owned Utilities (IOUs) creates a misalignment with the growth of renewable energy. These IOUs, which serve 71% of electricity customers in the United States,[78] are driven to maximize profits by selling more electricity. The increasing presence of residential and commercial rooftop solar systems, however, reduces the demand for electricity from IOUs, creating a conflict of interest. This dynamic can slow IoT adoption and the integration of renewable energy systems, as the utilities may resist changes that could affect their revenue streams.[79]

Similarly, the fragmented structure of the construction industry hampers IoT adoption. Construction projects typically involve a diverse range of contractors, subcontractors and specialists from various businesses, each with their own processes. This lack of shared collaboration across teams means that IoT solutions adopted by one party may not benefit the entire project. Each firm often focuses on optimizing their own processes, rather than collaborating for the broader project's benefit, which limits the full potential of IoT to improve efficiency and communication across the entire construction workflow.

Regulations and regulatory environment. The insurance industry faces challenges with IoT adoption due to its heavily regulated environment. The rapid advancement of IoT and related technologies like AI often outpaces regulatory developments, which can result in existing frameworks not adequately addressing these innovations. This mismatch can lead to regulatory actions that hinder IoT integration, stifling potential benefits and slowing adoption. Insurance regulators in California, sensitive to data privacy considerations, have imposed limits on what data can be used from vehicle telematics systems to support underwriting.

---

[76] "Farm Bureau Survey: Farmers Want to Control Their Own Data", Precision Farming Dealer, May 12, 2016. Link

[77] "Wearables: Where do they fall within the regulatory landscape?" G. Tomimbang, International Association of Privacy Professionals. Link

[78] "Investor-owned utilities served 72% of U.S. electricity customers in 2017," U.S. Energy Information Administration, August 15, 2019. Link

[79] "Policy Explainer: How Utility Reform Can Align Profits with Climate Goals," Climate Xchange, November 10, 2022. Link

© Strategy of Things, 2025. All rights reserved.

Similarly, in healthcare, the adoption of the Internet of Medical Things (IoMT) devices is complicated by stringent regulations. Devices that collect, transmit and store Protected Health Information (PHI) must comply with regulations such as HIPAA and FDA standards. These regulations aim to ensure safety and privacy but can be challenging for healthcare providers and IoMT manufacturers to navigate. Compliance involves safeguarding patient information, obtaining informed consent and establishing agreements with third-party vendors to meet privacy and security requirements.

As IoT devices proliferate across industries, ensuring that data collected and transmitted by these devices is protected against breaches and unauthorized access becomes crucial. Regulations like the GDPR in Europe and various national privacy laws, seek to address these concerns by imposing strict guidelines on data collection, storage and usage. Additionally, the lack of uniform standards for IoT devices can lead to inconsistencies in security and interoperability, posing risks to both users and businesses. Effective regulation is necessary to balance innovation with the protection of personal and sensitive data, while also fostering a secure and interoperable IoT ecosystem.

Financial considerations. The adoption of IoT technologies in various industries faces significant hurdles due to financial considerations around return on investment (ROI), funding limitations and the cost of technology. In the manufacturing sector, while IoT offers potential benefits such as enhanced efficiency and smarter operations, skepticism remains regarding its ROI promise. A 2021 survey revealed that 68% of 500 respondents felt their investments had not yet delivered positive returns and 65% believed the costs outweighed the benefits.[80] This skepticism is largely due to a lack of maturity and understanding of the long-term ROI and business case for IoT in manufacturing.

Similarly, smart cities struggle with funding challenges. While cities have limited internal funding sources and intermittent grants to do small scale pilot projects, they lack funding sources for scaling or maintaining smart city initiatives. Public-Private Partnerships (PPPs) offer larger funding opportunities but are complex to establish and manage.

In the retail sector, the low-profit margins create financial constraints that limit their ability to invest in advanced IoT technologies. Although RFID technology is inexpensive and is widely used in retail, it is not suitable for all applications. More advanced IoT solutions like beacons, condition sensors and robotics, support a variety of applications like remote monitoring of customer equipment and in-store customer tracking, but are significantly more expensive. This disparity in technology costs and low profitability margins makes it difficult for retailers to justify investment in more expensive IoT solutions despite their potential benefits.

5.3. Industry findings

This section shows the three most important IoT technology challenges for each of the nine industries. The following sections provide an industry overview with key facts and challenges, a set of use cases and the results of the synthesis of the collected data. In addition, details on each of the technology challenges are provided.

[80] "Accelerating the Adoption of Smarter Manufacturing", Lift industry survey, 2021. Link

© Strategy of Things, 2025. All rights reserved.

5.3.1. Agriculture

Agriculture plays an important role in the United States economy. In 2023, agriculture and related industries contributed $1.537 trillion, or 5.5% to national GDP.[81] Farm outputs generated $222.3 billion, or 0.8% of the national GDP.[82] In 2023, the industry generated commodity cash receipts of $521 billion for crops, animals and animal products.[83]

The agricultural and food sectors employed 22.1 million people, or 10.5% of the U.S. employment in 2022. Ranching and farming provided 2.6 million jobs, or 1.2% of all U.S. employment.[84] Another 1 million jobs, or 0.5% came from forestry, fishing and related activities.[85] Agriculture outputs, including food, beverage and tobacco manufacturing; food and beverage stores; food service, eating and drinking places; and textile, apparel and leather manufacturing lead to another 18.5 million positions, representing 8.8% of all U.S. jobs.[86]

The United States is the second largest agricultural exporter after the European Union. With U.S. agricultural output growing faster than domestic demand for many products, export markets have enabled farmers and ranchers to sustain prices and revenues. As a result, U.S. agricultural exports have grown steadily from $52 billion in 1994[87] to $174 billion in 2023.[88]

There were 2.05 million farms in 2017.[89] Small family farms, with a gross cash farm income (GCFI) of $350K, account for 90% of farms and 21% of production.[90] Large-scale family farms, with a GCFI of $1 million or more, accounted for 3% of farms and 46% of production.[91]

5.3.1.1. Agriculture: IoT opportunities

The Internet of Things (IoT) is a key driver of Agriculture 4.0, transforming agricultural operations by providing real-time data and insights through sensors and analytics. The use of IoT systems helps increase agricultural productivity, day-to-day operational efficiency, facilitate adaptation to climate changes and enhance overall competitiveness. IoT devices monitor equipment, machinery, livestock and soil conditions, offering data previously unavailable to farmers. For example, smart irrigation systems use soil moisture sensors to optimize water usage. Drones and livestock health sensors enhance plant and animal monitoring, reducing labor and

---

[81] "Ag and Food Sectors and the Economy", USDA. Economic Research Service, December 19, 2024. Link

[82] ibid.

[83] "Annual Cash Receipts by Commodity", USDA, Economic Research Service, December 3, 2024. Link

[84] See note 81

[85] ibid.

[86] ibid.

[87] "U.S. Agricultural Trade at a Glance", USDA, Economic Research Service, April 2023. Link

[88] "Agricultural Trade", USDA, Economic Research Service, February 16, 2024. Link

[89] "Farming and Farm Income", USDA, Economic Research Service, August 2023. Link

[90] ibid.

[91] ibid.

© Strategy of Things, 2025. All rights reserved.

improving efficiency. Overall, IoT addresses challenges like equipment downtime, inefficient operations and labor shortages, while improving productivity and economic outcomes.

Figure 5-3 below shows some representative IoT use cases for the agriculture industry.

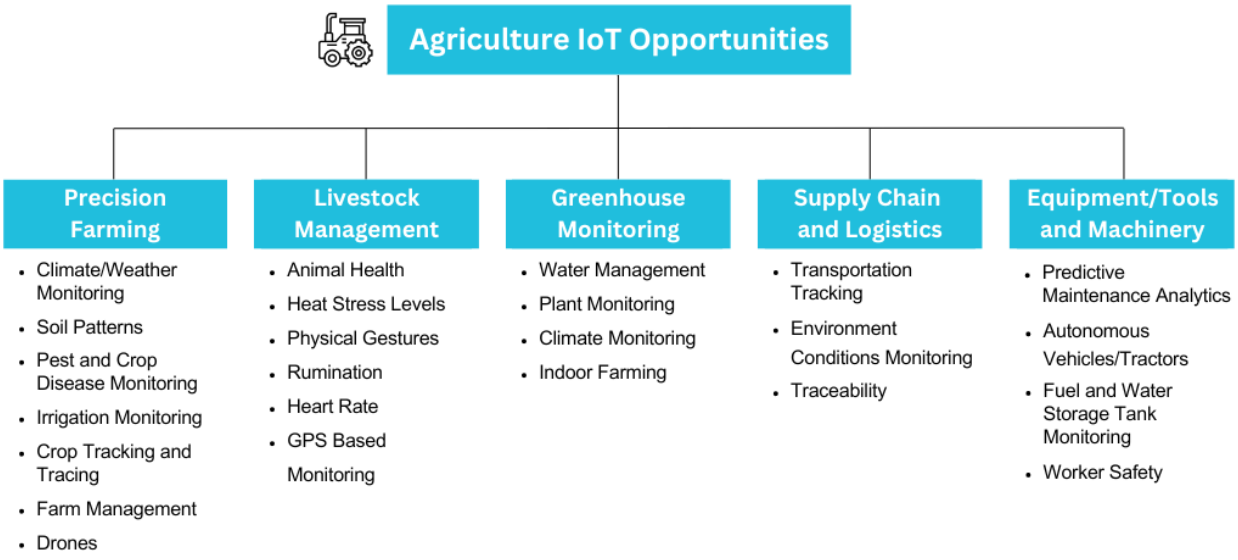


Figure 5-3: Agriculture: IoT Use Cases

Figure 5-4 below shows examples of IoT use cases aligned to key industry challenges.

Key Industry Challenges	IoT Opportunity See 13.2.1	Relevant IoT Solutions
Changing climate patterns decrease crop productivity, negatively affect livestock health, reduce output of animal products and increase input needs. See 13.1.2.1	Minimize the impact of droughts, heat waves, flooding and other conditions caused by changing climate patterns. Facilitate adaptation to changing climate patterns will lead to improved plant and animal health, resilience and production yields.	• Climate/weather monitoring • Soil moisture monitoring • Smart irrigation • Livestock health monitoring • Water management

© Strategy of Things, 2025. All rights reserved.

Key Industry Challenges	IoT Opportunity See 13.2.1	Relevant IoT Solutions
Persistent labor shortages hinder agricultural operations and production outputs. See 13.1.2.2	Optimize workforce productivity, efficiency and effectiveness through operations planning, task automation, resource optimization and data informed actions. IoT technology helps producers do more with fewer resources and to be more effective doing it.	• Autonomous tractors and machines • Drones • Worker safety • Predictive maintenance
Small family farms, representing 90% of all farms, face high financial risks and business viability. See 13.1.2.3	Small farms have limited resources and capabilities. IoT use helps optimize resources and capabilities, increase production yields and operational efficiencies, minimize operational costs. IoT helps small farmers become more resilient, competitive and profitable.	• Farm management • Soil moisture monitoring • Smart irrigation • Drones • Water management • Predictive maintenance
Ability to produce enough food to meet expected global food shortage. See 13.1.2.4	Increase production yields, reduce waste and spoilage to meet growing demand in domestic and international markets.	• Pest and crop disease monitoring • Animal health monitoring • Climate/weather monitoring • Soil patterns • Pesticide application • Fertilizer application

Figure 5-4: Agriculture: Industry Challenges

5.3.1.2. IoT technology challenges in agriculture

The technology challenges identified through research are discussed below.

Connectivity. Without connectivity, IoT sensors and other "precision agriculture" equipment are unable to send their data to remote data centers in the cloud for processing and storage. The connectivity challenges are manifested in several ways, including availability of broadband service to the farm, connecting to the field and evolving needs. See Section 13.3.1.1

Edge computing and processing. Farms of the near future will integrate sensors, drones, robotics and autonomous machines in many aspects of their daily operations. Much of this data must be processed on the farm due to lack of broadband services, high costs of cloud processing for data intensive applications (drones) and need for real-time processing (autonomous

© Strategy of Things, 2025. All rights reserved.

applications). The lack of enabling edge infrastructure technologies and cloud connectivity hinders agricultural IoT development and adoption. See Section 13.3.1.2

Interoperability. Farms have a variety of machines and equipment from the "latest and greatest" equipment with current technology to 30- to 40-year-old legacy equipment with limited technology and no connectivity. Interoperability challenges prevent old and new equipment from working together. Many of the machines employ a variety of proprietary and incompatible protocols that make sharing information with each other, as well as with farm operations software difficult or impossible. See Section 13.3.1.3

5.3.2. Manufacturing

Manufacturing is one of the largest industries in the United States. In 2020, U.S. manufacturing contributed $2.27 trillion to the American economy, representing 10.8% of the Gross Domestic Product (GDP).

When its indirect contributions are factored in, American manufacturing contributed 24.1% of the overall U.S. GDP.[92] The United States exported $1.17 trillion in manufactured goods in 2020.[93] The U.S. manufacturing industry is the nation's fifth largest employer.[94] U.S. manufacturers employed 12.8 million people in May 2022 with 57.9% of manufacturing workers employed at firms with 500 or more people.

In 2019 there were 243,687 manufacturing companies in the United States. Small businesses, employing 500 people or less, represent 98.3% of these manufacturers. And 87.7% of the firms employ less than 50 people with 74.3% having 20 employees or less.[95]

5.3.2.1. Manufacturing: IoT opportunities

IoT is a critical technology enabler of the manufacturing industry shift to "smart manufacturing." IoT technologies and applications help address many of the day-to-day manufacturing challenges such as unplanned downtime, inefficient operations, poor production quality, limited supply chain visibility and reactive field support.

Equally important, IoT helps manufacturers lessen the impact of labor shortages and declining labor productivity. For example, IoT in manufacturing monitors machine operations, utilization, production processes and product quality, helping optimize equipment use, reduce defects and minimize waste.

It also supports indirect activities like predictive maintenance, preventing unplanned downtime and maintaining production capacity. For machine builders and OEMs, remote monitoring of field equipment enables proactive customer support and efficient service management.

Figure 5-5 below shows some representative IoT use cases for the manufacturing.

---

[92] "NIST Advanced Manufacturing Series 100-42, 2021. Link

[93] "Facts About Manufacturing", National Association of Manufacturers. Link

[94] "Manufacturing in America: 2021", U.S. Census Bureau. Link

[95] ibid.

© Strategy of Things, 2025. All rights reserved.

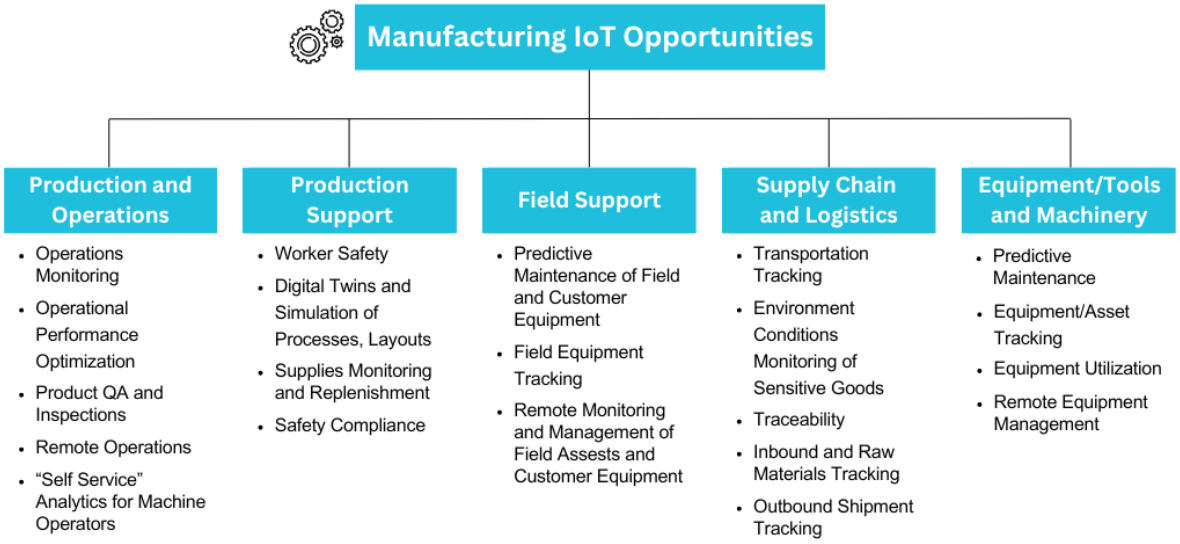


Figure 5-5: Manufacturing: IoT Use Cases

The table below shows examples of IoT use cases aligned to key industry challenges.

Key Industry Challenges	IoT Opportunity See 14.2.1	Relevant IoT Solutions
The U.S. supply chain is vulnerable, as experienced during the pandemic. Measures are needed to increase supply chain resilience. See 14.1.2.1	Track, monitor and optimize incoming parts and materials shipments needed for manufacturing. Track and monitor finished product shipments.	• Transportation tracking • Traceability • Inbound and raw materials tracking • Outbound shipment tracking • Supplies monitoring and replenishment
Declining labor productivity, leading to more people, or more labor hours, producing the same product. This increases the cost of the product and decreases the competitiveness of U.S. manufacturers. See 14.1.2.2	Increase productivity, efficiency and effectiveness through operations monitoring, improved resource utilization and optimization, automation, minimized unplanned downtime and waste and data informed targeted actions. IoT helps manufacturers be more resilient, competitive and profitable.	• Operations monitoring • Operational performance optimization • Product QA and inspections • Digital twin production simulations • Remote monitoring • Predictive maintenance

© Strategy of Things, 2025. All rights reserved.

Key Industry Challenges	IoT Opportunity See 14.2.1	Relevant IoT Solutions
Ongoing labor shortage in manufacturing. 89.4% of manufacturers have unfilled positions and are struggling to find qualified applicants to fill. See 14.1.2.3	Optimize workforce productivity, efficiency and effectiveness through operations planning, task automation, resource optimization and data informed actions. IoT technology helps manufacturers do more with fewer resources and to be more effective doing it.	• Remote operations • Worker safety and safety compliance • Remote equipment management • Remote monitoring and management of field assets and customer equipment • Process automation
Skills shortages will leave 2.4 million unfilled positions between 2018 and 2028, leading to a loss of $454 billion of manufacturing value in 2028. See Section 14.1.2.4	IoT reduces reliance on hard-to-find resources through intelligent algorithms and process automation.	• Self-service analytics • Robotics • Predictive maintenance • Process automation

Figure 5-6: Manufacturing: Industry Challenges

5.3.2.2. IoT technology challenges in manufacturing

The technology challenges identified through research are discussed below.

Interoperability. Factories have a variety of equipment, from new industrial equipment with current technology to legacy equipment with limited technology and connectivity. They employ a variety of proprietary and incompatible protocols that make sharing information from manufacturing execution systems (MES), enterprise resource planning (ERP) systems, supervisory control and data acquisition (SCADA) and distributed control systems (DCS) difficult or impossible. This creates operational inefficiencies. See Section 14.3.1.1

Cybersecurity. With the convergence of IT and Operational Technology (OT) systems, along with the integration of IoT devices, formerly “air gapped” (computer systems or networks that are physically isolated from other networks and the internet) OT systems are now accessible from the Internet. Most manufacturing environments were not designed to address cybersecurity issues. See Section 14.3.1.2

Sensors and devices. One challenge is the high cost of devices, which pose a barrier to adoption for manufacturers with multiple factories containing thousands to hundreds of thousands of machines and production equipment of varying types. A second challenge is the limited ability of current IoT devices to process and analyze data on the device to support real-time monitoring in a factory environment where wireless connectivity is challenging and limited. See Section 14.3.1.3

© Strategy of Things, 2025. All rights reserved.

Connectivity. Many manufacturers lack the appropriate connectivity infrastructure to support "smart operations" for tomorrow's factories. Some factories do not have an adequate network infrastructure because their previous production operations did not require connectivity. While some of their equipment may have collected data, there was no provision available to extract or analyze the data. Other factories are in buildings with extensive metal racking and machinery which hinders wireless signal propagation and results in poor coverage and performance. See Section 14.3.1.4

5.3.3. Construction

In Q1 of 2022, construction contributed $1.01 trillion USD[96] to the American economy, representing 4.13% of Gross Domestic Product (GDP).[97] The Architecture and Engineering industry is interdependent with the construction industry and contributed an additional $386 billion to GDP in 2019.[98] The construction industry had 753,000 employers and over 7.18 million employees in 2020.[99] The industry has a $458.9 billion annual payroll in 2020 and creates nearly $1.4 trillion worth of structures each year. The construction industry is dominated by small businesses. Two-thirds of the 753,000 establishments in the industry employ fewer than 5 people in 2020. Two-thirds of the 7.18 million employees work in businesses employing fewer than 100 people. There are 700 firms, or 0.1% of all construction firms, which employ more than 500 people.[100] In May 2022, the seasonally adjusted annual rate of construction spending was $1.76 trillion.[101] Of that, $932.9 billion (52.9%) was for residential construction, while the remaining $829.4 billion was for non-residential construction such as commercial buildings, highways and utilities.

5.3.3.1. Construction: IoT opportunities

The Internet of Things (IoT) offers numerous opportunities in construction, from enhancing worker and site safety to ensuring compliance with regulations. IoT-enabled imaging sensors and cameras can monitor progress, detect "as-designed-as-built" conflicts early and optimize schedules. Wearables track worker location, site conditions and health, while more advanced AR/VR tools support planning and modeling. IoT also improves modular construction by monitoring production quality, environmental conditions and materials and equipment tracking. Additionally, IoT integrates with AI and Building Information Modeling (BIM) for better project management, cost prediction and safety risk identification. Beyond construction, IoT enables equipment tracking, predictive maintenance and compliance monitoring, improving overall project efficiency and machinery management.

---

[96] "Interactive Access to Industry Economic Accounts Data." Link

[97] ibid.

[98] "New Study: Total Economic Contribution of Engineering an Architectural Services nearly $600 billion", ACEC Research Institute, Feb 2021. Link

[99] U.S. Census Bureau, 2000, CBP Tables 2020. Link

[100] ibid.

[101] "Monthly Construction Spending, August 2023 ", Census.gov. Link

© Strategy of Things, 2025. All rights reserved.

Figure 5-7 below shows some representative IoT use cases for the construction industry.

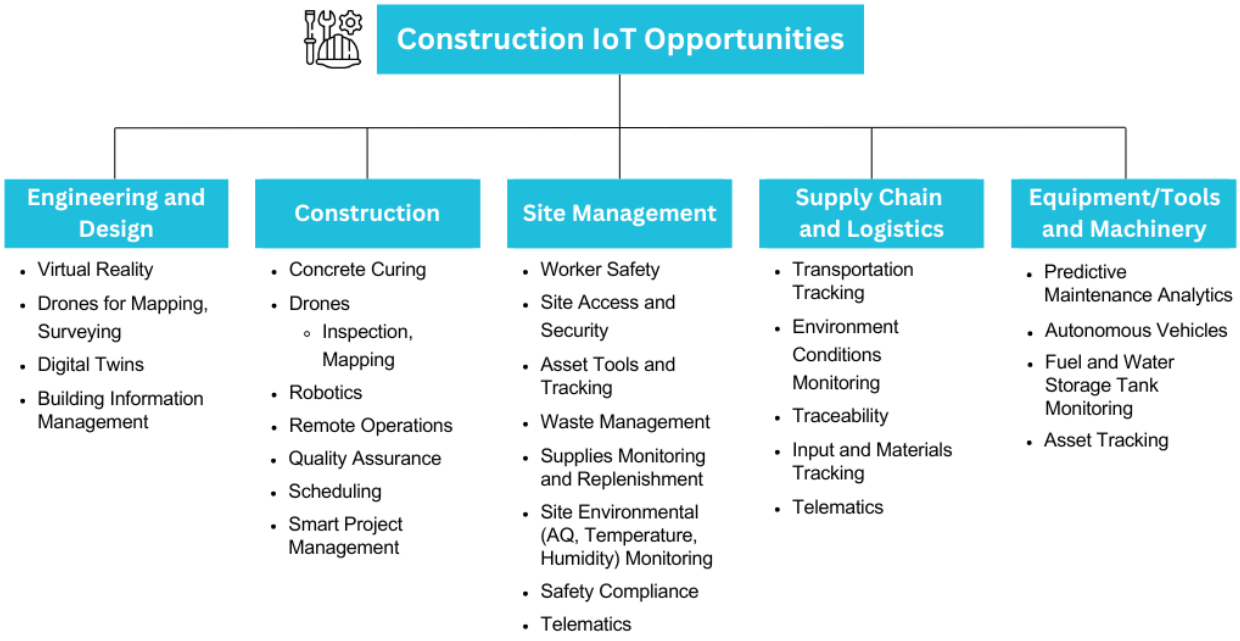


Figure 5-7: Construction: IoT Use Cases

The table below shows examples of IoT use cases aligned to key industry challenges.

Key Industry Challenges	IoT Opportunity See 15.2.1.1	Relevant IoT Solutions
Flat and stalled productivity for residential, multifamily residential, industrial buildings, highway, street and bridge construction. See 15.1.2.1	Boost productivity by enabling real-time tracking of equipment and materials, reducing downtime and waste.	• Input and materials tracking • Asset tracking • Telematics • Transportation tracking
Fragmented industry of general contractors and specialty subcontractors, hindering collaboration, communications and leading to suboptimal working relationships. See 15.1.2.2	Help integrate the industry by providing a unified platform for data sharing and collaboration among various stakeholders.	• Building Information Management • Digital twins

© Strategy of Things, 2025. All rights reserved.

Key Industry Challenges	IoT Opportunity See 15.2.1.1	Relevant IoT Solutions
Long running skilled labor shortage due to lack of new workers entering and wave of retirements. See 15.1.2.3	Mitigate labor shortages by automating routine tasks, such as equipment inspection and inventory management, freeing up workers for more complex tasks.	• Worker safety • Safety compliance • Storage tank monitoring • Remote monitoring and operations
Low adoption rate of digital technology, including digital tools and BIM. See 15.1.2.4	Drive digital transformation in the construction industry by demonstrating the tangible benefits of technology adoption such as cost savings and efficiency improvements.	• Robotics • Predictive maintenance analytics • Autonomous vehicles
Low profit margins due to rising materials costs, supply disruptions, labor shortages, errors, change orders and other factors. See 15.1.2.5	Improve construction quality and reduce rework and construction mistakes. Facilitate scheduling and project management to maximize utilization of general and specialized resources and timely delivery and availability of materials.	• Scheduling • Smart project management • Site access and security • Asset and tools tracking • Waste management • Supplies monitoring and replenishment • Traceability

Figure 5-8: Construction: Industry Challenges

5.3.3.2. IoT technology challenges in construction

The technology challenges are described below.

BIM-IoT data integration. Building Information Modeling (BIM) systems are a foundation for the digital transformation of the construction industry. The integration of IoT with BIM provides owners, builders and facility operators with real time physical "perception" information to augment static data throughout the asset lifecycle, from planning, design, construction and operations. For example, IoT sensors validate modeling assumptions during design, measure the progress and conflicts during construction and monitor and manage the constructed facility during its useful life. The BIM-IoT integration is pertinent in four areas, including construction operation and monitoring; health and safety management; construction logistics and management; and facility management. See Section 15.3.1.1

Data standards and interoperability. The lack of interoperability is a major barrier to smart or digital construction and operations of the constructed asset ("built environment"). Project teams in construction are assembled from many different businesses and come together to work in a "one-off" way." Each business brings their own technologies and software tools to the project. However, these tools often cannot communicate with each other. As a result, data is exchanged

© Strategy of Things, 2025. All rights reserved.

verbally, or through manual entry into disparate unconnected systems, or not at all. See Section 15.3.1.2

5.3.4. Insurance

The insurance industry sector facilitates the operation and resilience of the U.S. economy and its people. Property and casualty insurance helps people, businesses and communities recover and rebuild from natural and human-caused hazards and disasters by defraying the financial costs. Credit insurance allows merchants, manufacturers and banks to extend credit to their customers by protecting them from losses or damages resulting from the nonpayment of debts. The insurance industry created $695.2 B dollars of value in Q1 2022, representing 2.85% of the national GDP of $24.39 trillion.[102] It underwrote $1.351 trillion in premiums in 2021.[103] The industry employed 2.8 million Americans in 2021.[104] There were 181,309 insurance related business establishments in the United States in 2020. These businesses combined to pay $248.3 B in annual payroll.[105]

5.3.4.1. Insurance: IoT opportunities

IoT is expected to transform the insurance industry by providing new data sources that enhance risk assessment, create innovative product offerings and personalize customer experiences. The Internet of Things (IoT) allows insurers to gather real-time information that was previously unmeasurable, leading to more accurate underwriting and proactive risk management. In vehicles, IoT sensors enable Usage-Based Insurance (UBI) products, basing premiums on driving habits rather than assumptions, which incentivizes safer driving and reduces claims costs. IoT use also helps insurers to proactively manage risks, like using leak detection sensors to prevent major damage or drones to assess disaster-related claims efficiently. Additionally, IoT asset trackers aid in recovering stolen vehicles, while crash sensors expedite emergency responses. IoT strengthens the insurer-customer relationship through services like infrastructure monitoring, enabling early problem detection, reducing repair costs and fostering customer loyalty through ongoing engagement and improved claims processing. By creating personalized, IoT-driven policies, insurers can differentiate themselves, reduce losses and improve customer loyalty in a commoditized market.

Figure 5-9 below shows some representative IoT use cases for the insurance industry.

[102] "Insurance Carriers and Related Activities, Q1 2022, Value Added by Industry", Bureau of Economic Analysis. Link

[103] "Facts + Statistics: Industry Overview", Insurance Information Institute. 2022. Link

[104] ibid.

[105] U.S. Census Bureau, 2000, CBP Tables 2020. Link

© Strategy of Things, 2025. All rights reserved.

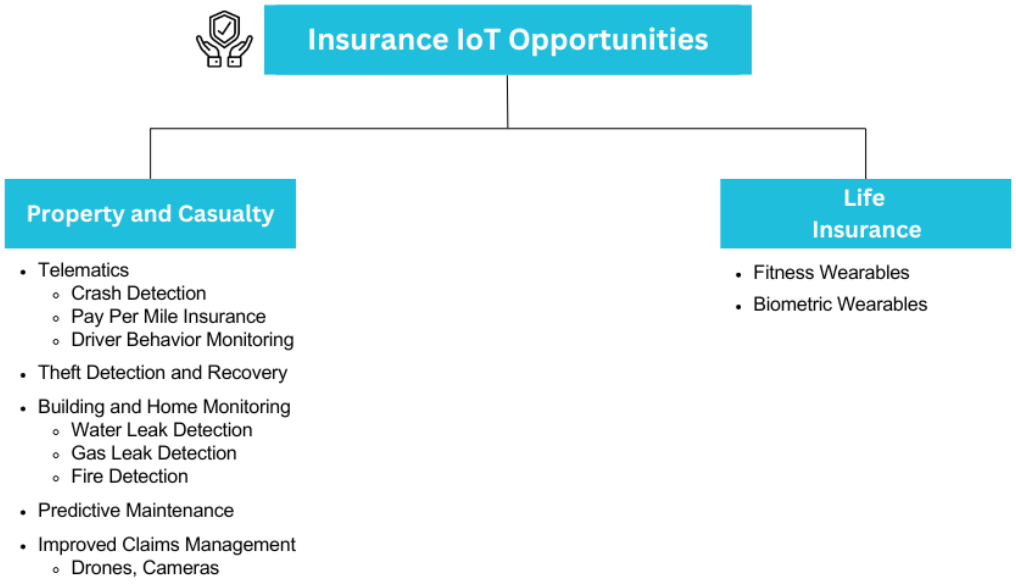


Figure 5-9: Insurance: IoT Use Cases

The table below shows examples of IoT use cases aligned to key industry challenges.

Key Industry Challenges	IoT Opportunity See 16.2.1	Relevant IoT Solutions
Customers expect personalized "instant gratification" engagements to learn, buy insurance and file claims. See 16.1.2.1	Enhance customer support and engagement, improve insurer proactiveness and responsiveness and increase loyalty and customer retention.	• Auto accident detection and automatic kickoff of claims process • AI-based camera systems and drones to determine accident and disaster damages to property
The increase in risk events and resulting payouts have led insurers to higher losses than expected, leading to lower profitability. See 16.1.2.2	Enable insurers to assess risks, create risk-tailored products and improve pricing decisions.	• Telematics and driver behavior monitoring • Theft detection and recovery • Remote equipment monitoring and notification
Insurance products are increasingly being commoditized. See 16.1.2.3	Facilitates insurer innovation and development of differentiated insurance offerings and responsive services.	• Mileage and usage-based auto insurance • Remote equipment monitoring and notification

© Strategy of Things, 2025. All rights reserved.

Key Industry Challenges	IoT Opportunity See 16.2.1	Relevant IoT Solutions
		• Predictive monitoring of home and business equipment • Health monitoring and wearables (life insurance)
Legacy infrastructure is hindering efforts to transform and become more efficient and to offer new products and services. See 16.1.2.4	Extend usefulness of legacy systems by adding real-time data and insights to complement existing static data on policyholders.	• Vehicle telematics for individual driver behavior determination • Wearables for health monitoring for life insurance

Figure 5-10: Insurance: Industry Challenges

5.3.4.2. IoT technology challenges in insurance

Each of these is discussed below.

AI model accuracy and explainability. IoT sensors and devices collect large volumes of data that are analyzed by machine learning and AI algorithms to predict outcomes, determine risks in underwriting policies and create new insurance products. However, results generated by AI may lead to "proxy discrimination" and "raise unique ethical implications." These AI generated results are not easily explainable in how they arrived at an outcome, leading to users' reluctance and guarded use of these AI models. See Section 16.3.1.1

Data privacy. The IoT technologies used in insurance products collect a large amount of personal data. However, data privacy concerns hinder IoT innovation and adoption in the insurance industry. Many IoT products are not designed with privacy in mind. Insurance regulators, often sensitive to data privacy considerations, have imposed limits on what data can be used. State regulations, such as California's CCPA, impose additional requirements for transparency and control of personal data. See Section 16.3.1.2

IoT cybersecurity. From telematics devices used in vehicles, to in-home sensors and human health monitors, IoT is increasingly used in new insurance products. The IoT devices represent new attack surfaces and introduce additional vulnerabilities into the connected networks. Insurance carriers are attractive targets for cybercriminals as they collect and make extensive use of data, including personally identifiable information (PII). See Section 16.3.1.3

© Strategy of Things, 2025. All rights reserved.

5.3.5. Smart Cities

As of January 1, 2022, the population of the United States stood at 332,403,650.[106] An estimated 286.5 million people live in one of 384 designated metropolitan statistical areas (MSA) in the United States as of July 1, 2021,[107] representing 86.2% of the total American population. There are 19,495 cities, towns or other incorporated places in the United States[108] and the majority of these are small. A significant portion of city populations live in a small number of large cities. There are 328 cities that have a population of 100,000 or more, housing a combined population of 96,558,086 or 29% of the U.S. population.

Despite occupying 2.7% of the country's land mass[109], American cities are economic engines. For example, the economies of the metropolitan areas accounted for 91.1% of the national GDP, 91.8% of all wage income and 88.1% of the jobs in 2018.[110] In 2020, the top ten U.S. metropolitan areas accounted for 37.3% of the total GDP of $18.8 trillion produced in the 384 U.S. metropolitan statistical areas. Cities generate income from several sources, including user charges and property taxes as well as property sales, net lottery earnings, sales taxes, individual and corporate income taxes, license fees, federal government and local sources.[111] A 2015 survey found that the 100 largest cities, with an average annual operating budget per city of $2.146 billion spent an average of $2,605 per citizen per year.[112] Common areas of city expenditures include public safety, social and health services, housing and urban development, public works and transportation, parks, recreation and cultural facilities, education, general government, debt service and other/miscellaneous.[113]

5.3.5.1. Smart Cities: IoT opportunities

"Smart cities" refers to cities that use IoT and other technologies to create outcomes supporting their community of residents, businesses and visitors. Those outcomes include operational efficiency and productivity, sustainability, health and wellness, mobility, economic vibrancy, public safety, quality of life and resilience.[114] IoT brings significant value to cities and municipalities by addressing various challenges, improving efficiency and enhancing public safety.

---

[106] "U.S. Population Estimated at 332,403,650 on Jan. 1, 2022", Derek Moore, Dec 30, 2021, U.S. Census Bureau. Link

[107] Metropolitan and Micropolitan Statistical Area Population by Characteristics: 2020-2021, U.S. Census Bureau. Link

[108] "Population and Housing Unit Estimates Tables, 2021", July 1, 2021, U.S. Census Bureau. Link

[109] "Land Use and Land Cover Estimates for the United States", Economic Research Service, USDA, April 27, 2022. Link

[110] "U.S. Cities Factsheet", University of Michigan Center for Sustainable Systems. Link

[111] "Local Government Revenue Sources – Cities", Government Finance Officers Association. Link

[112] "Analysis of Spending in America's Largest Cities", Ballotpedia. April 2015. Link

[113] "The Fiscal Landscape of Large U.S. Cities", Issue Brief, Pew Charitable Trusts, December 13, 2016. Link

[114] "Planning Sustainable Smart Cities With the Smart City Ecosystem Framework," B. Chan, Strategy of Things, January 24, 2018. Link

© Strategy of Things, 2025. All rights reserved.

For cities with limited budgets and resources, IoT solutions like smart streetlights and parking systems help increase staff productivity, reduce operational costs and improve service delivery. For example, connected streetlights can adjust illumination and detect outages, while smart parking systems ease congestion and enhance downtown accessibility. IoT systems also monitor infrastructure, such as bridges and waterways, enabling proactive maintenance and flood prevention. Public safety benefits from technologies like acoustic gunshot detection, Automated License Plate Recognition (ALPR) and facial recognition, which aid in crime prevention and response. Additionally, intelligent traffic monitoring systems optimize traffic flow, prioritize emergency vehicles and reduce accidents, making cities safer and more efficient.

Figure 5-11 below shows some representative IoT use cases for smart cities.

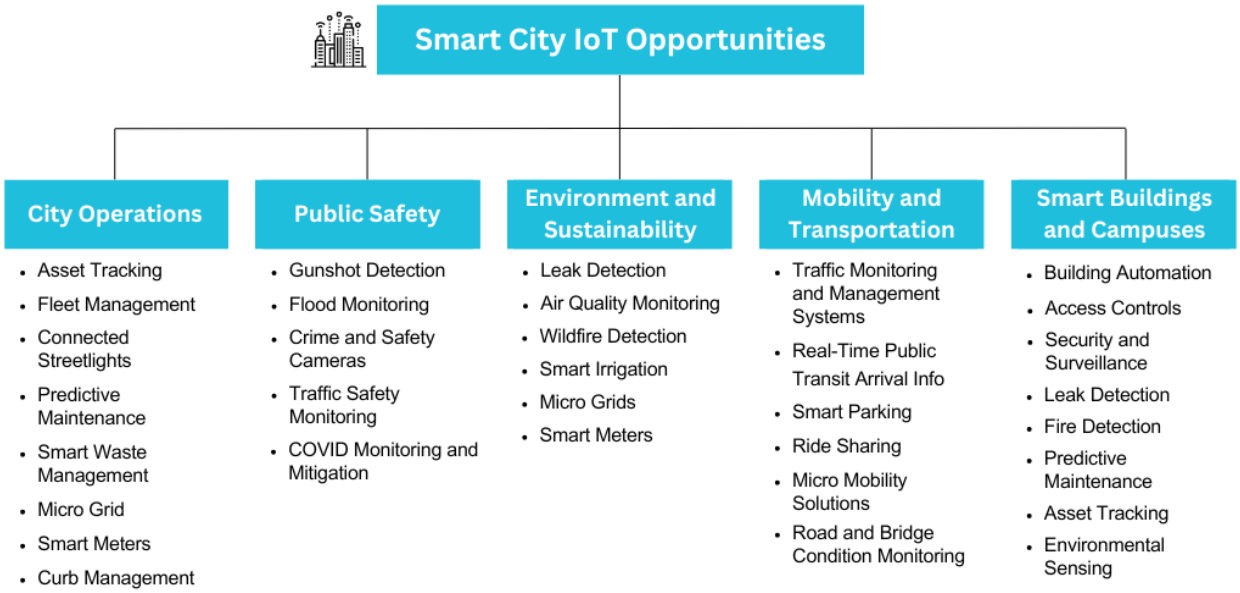


Figure 5-11: Smart City IoT Use Cases

The table below shows examples of IoT use cases aligned to key industry challenges.

Key Industry Challenges	IoT Opportunity See 17.2.1	Relevant IoT Solutions
Existing city infrastructure is old and in need of major repair and replacement. See 17.1.2.1	Monitor the condition of city infrastructure and improve responsiveness to service and repair of broken equipment and infrastructure. Increase proactiveness by predicting maintenance needs of assets and infrastructure.	• Infrastructures such as bridges, roads, water pipes, buildings, dams and levees and reservoir condition monitoring • Predictive maintenance of infrastructure facilities and equipment • Leak detection of pipes and irrigation systems

© Strategy of Things, 2025. All rights reserved.

Key Industry Challenges	IoT Opportunity See 17.2.1	Relevant IoT Solutions
Budgets are a source of ongoing challenge for municipal governments. These challenges were amplified by the COVID-19 pandemic and its lingering effects. See 17.1.2.2	Improve city staff and resource efficiency, effectiveness while creating cost savings and cost avoidance on assets and infrastructure.	• Smart waste management • City vehicle fleet management • Connected streetlights • Water leak detection • Building energy monitoring and management
Municipalities face a range of technological challenges to support modern municipal needs and digital government. See 17.1.2.3	Monitor physical assets, infrastructure and the environment and integrating into city operations and systems. Data gives managers and residents greater visibility and helps inform policies and decisions, as well as improves operational responsiveness.	• Asset tracking • Air quality monitoring • Traffic and traffic safety management and monitoring • Resource usage monitoring (water, electricity, gas)
Public safety is an ongoing and top of mind concern, including crime, homelessness, drugs, road safety and emergency response. See 17.1.2.4	Monitor conditions impacting public safety and the ability of first responders to address them, such as traffic, crime, fire, infrastructure conditions, river levels and scene situational awareness.	• Security and surveillance • Traffic monitoring and management systems • Gunshot detection • Connected streetlights • People location analytics and tracking inside buildings • River and stream water level monitoring • Drones for public safety and disaster response

Figure 5-12: Smart Cities: Industry Challenges

5.3.5.2. IoT technology challenges in smart cities

The technology challenges are discussed below.

Interoperability. Cities host a range of smart technologies, IoT devices and systems that are independently owned, operated and procured by different city organizations with little

© Strategy of Things, 2025. All rights reserved.

consideration for interaction and communication with each other. The lack of IoT interoperability prevents disparate systems from interconnecting, exchanging data and collaborating, locks the city to specific vendors and solutions and hinders the realization of interconnected urban environments. See Section 17.3.1.1

Privacy. Privacy is a top-of-mind concern for communities. Current approaches to smart city privacy are static, piecemeal and have limited effectiveness. For example, policies and regulations ban or limit the use of facial recognition systems, or systems are configured to disable certain functions or limit data collection. However, as IoT devices are increasingly integrated into city infrastructure and operations, "device by device" privacy approaches are no longer effective, sustainable or relevant. While these approaches achieve individual privacy goals, they also keep the city from realizing the full range of benefits from smart city technologies. 17.3.1.2

Edge infrastructure. Edge computing is an emerging paradigm to support increasing numbers of smart city applications that require data to be analyzed and processed on the device, gateway or local server. Advancements in a number of areas, such as scalable architectures, context aware computing, energy efficiency, interoperability and cybersecurity are needed. See Section 17.3.1.3

5.3.6. Transportation and Logistics

The transportation and warehouse industry created $721.3 billion[115] dollars of value in Q1 2022, representing 2.96% of the national GDP. In 2020, the transportation and logistics industry moved 2.29 billion tons of freight, equal to $3.67 trillion within the United States.[116] The top three modes of freight transportation are truck transportation (918.5 million tons), pipelines (444.9 million tons) and rail (392 million tons) in 2020.[117]

The industry employed 5.71 million people in 2020. The three sectors employing the most Americans in 2020 were truck transportation (1.624 million), warehousing and storage (1.141 million) and couriers and messengers (961.3 K).[118] The industry at that time created $292.4 B in total labor income, with $84.5 B (28.9%) coming from truck transportation, $52.8 B (18%) from warehousing and storage and $42.7 B (14.6%) from air transportation.[119] The industry is comprised mainly of small businesses, with 99.4% of the 257,785 businesses employing 499 people or less and 73.5%, employing less than 10 people.[120]

5.3.6.1. Transportation and Logistics: IoT opportunities

The transportation and logistics industry plays a critical role in maintaining the flow of materials, supplies and inventory across the global economy. The use of IoT facilitates better inventory

[115] Bureau of Economic Analysis. Link

[116] "Domestic Transportation Mode of Exports and Imports by Tonnage and Value", Bureau of Transportation Statistics, March 31, 2022. Link

[117] ibid, in 2017 dollars

[118] U.S. Census Bureau, 2000, CBP Tables 2020. Link

[119] ibid.

[120] ibid.

© Strategy of Things, 2025. All rights reserved.

management, demand forecasting and identification of potential supply chain disruptions for managers. IoT technologies, including telematics, GPS and fleet management software, are helping companies optimize routes, track weather and traffic conditions and improve Estimated Times of Delivery (ETD).

Additionally, IoT provides real-time visibility into inventory and goods across warehouses, enabling planners to minimize disruptions by drawing from the best locations. Beyond route optimization, IoT technologies monitor vehicle health, fuel consumption, driver performance and emissions, aiding in fleet management and enhancing safety and regulatory compliance.

Predictive analytics detect maintenance needs before breakdowns occur, reducing downtime and ensuring optimal vehicle performance. IoT technologies also ensure the safe transportation of sensitive goods like pharmaceuticals and food by monitoring environmental conditions such as temperature and humidity. In warehouses, IoT use enhances safety with tracking sensors, RFID and wearable devices that prevent collisions and accidents, while automation technologies like AGVs, robots and drones improve efficiency and reduce labor costs.

Figure 5-13 shows some representative IoT use cases for the transportation and logistics industry.

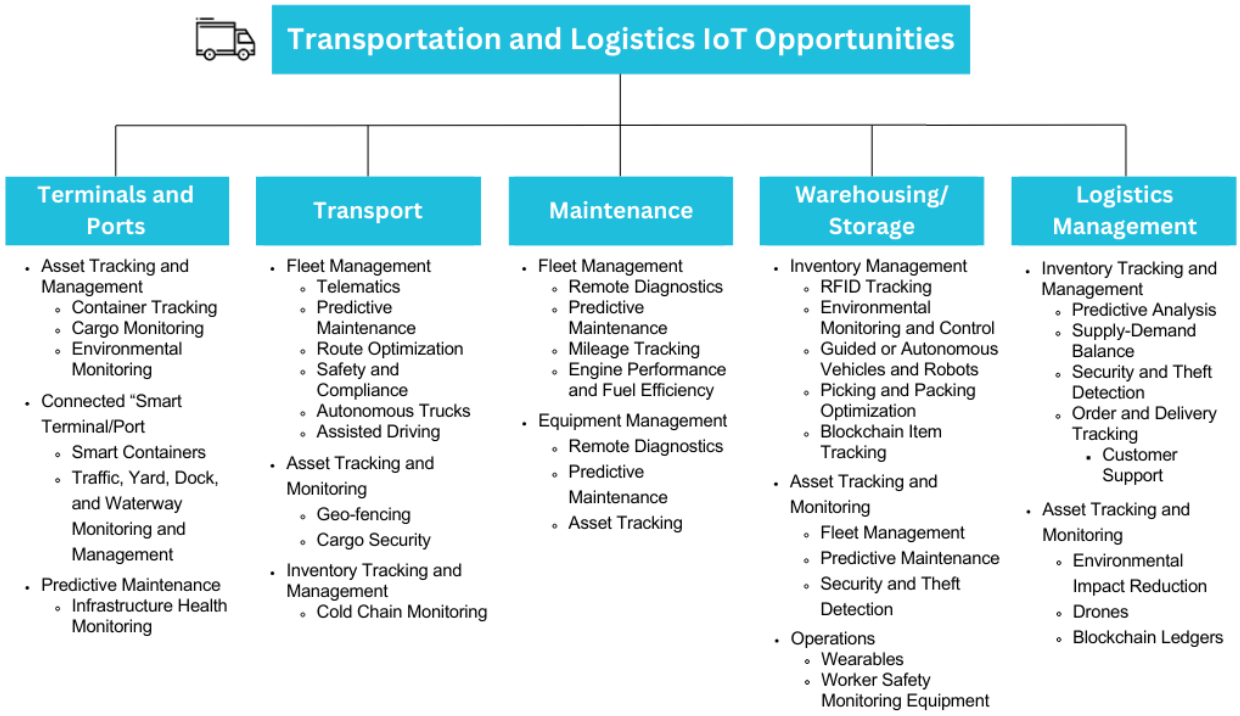


Figure 5-13: Transportation and Logistics: IoT Use Cases

Figure 5-14 below shows examples of IoT use cases aligned to key industry challenges.

© Strategy of Things, 2025. All rights reserved.

Key Industry Challenges	IoT Opportunity See 18.2.1	Relevant IoT Solutions
U.S. businesses are vulnerable to supply chain disruptions. See 18.1.2.1	Facilitate supply chain planning, from demand forecasting, inventory visibility and tracking, to supply replenishment and optimization of transport modes and routes.	• Inventory Tracking • Fleet management • Customer Order and Delivery Tracking • Predictive analytics
Poor state of U.S. infrastructure hinders the timely and safe transportation of freight and goods. See 18.1.2.2	Monitor and track freight shipments during transportation, including optimizing routes and modes to maintain on-time delivery and minimize impacts of delays, congestion and other factors due to poor condition of transportation infrastructure.	• Fleet management • Transportation safety • Predictive Analytics • Telematics
The transportation and logistics industry is subject to a variety of environmental and sustainability goals. See 18.1.2.3	Monitor and minimize emissions and energy consumption by vehicles and machinery during the transportation and handling of freight and inventory across the supply chain.	• Telematics • Monitoring Environmental Conditions • Engine Performance and Fuel Efficiency • Electric machinery and equipment monitoring • Predictive maintenance of vehicles and equipment
A driver shortage is hindering operations and impacting the economy. See 18.1.2.4	Optimize workforce productivity, efficiency and effectiveness through operations planning, task automation, resource optimization and data informed actions. IoT technology helps companies do more with fewer resources and to be more effective doing it.	• Workers' Safety • Robotics • Smart Inventory Management • Autonomous trucks • Robotics
Rising fuel costs are a major driver of increasing freight transportation costs. See 18.1.2.5	Monitor and minimize fuel consumption through data informed actions such as route optimization, load planning and coordination across the supply chain.	• Telematics • Traffic and route optimization management • Fleet management

© Strategy of Things, 2025. All rights reserved.

Figure 5-14: Transportation and Logistics: Industry Challenges

5.3.6.2. IoT technology challenges in transportation and logistics industry

The technology challenges of interoperability, data management and AI are discussed below.

Interoperability. Freight in the supply chain moves through a vast network of carriers, warehouses and terminal operators. Each party in the network has their own systems, software, technologies and processes. The lack of interoperability between these different technologies hinders the exchange of information, resulting in supply chain inefficiencies, increased costs, delays and a lack of real-time visibility and traceability. The reduced interoperability is due to a lack of universally adopted standards and the use of legacy and proprietary systems by the involved parties. See Section 18.3.1.1

Data Management. Information is essential to the operation of the digitalized global supply chain. IoT systems generate terabytes of supply chain information daily. A key requirement for the digital supply chain is the participant's capability to manage the data that are collected, stored and shared. The data may flow through multiple touchpoints, including manufacturing, transportation and warehousing. In addition, the data come from decentralized sources across the supply chain, maybe in different formats and standards and comply with a variety of regulations. Managing the exponentially growing volume of data requires a scalable, robust and advanced "beyond big data" management technologies and infrastructure. See Section 18.3.1.2

Artificial intelligence. Artificial Intelligence (AI) brings transformative benefits to the transportation and logistics industry. AI-powered algorithms are well-suited to analyze vast amounts of data to optimize transportation routes, minimize fuel consumption and ensure timely deliveries. AI-driven inventory management enhances supply chain efficiency by optimizing inventory levels and reducing stockouts. While AI offers significant benefits, it faces a variety of challenges to adoption in the transportation and logistics industry. Some of these include lack of trust in AI, limited access to high quality data, lack of transparency and explainability, biased data and algorithms, high costs and fear of job losses. See Section 18.3.1.3

5.3.7. Healthcare

Healthcare is one of the largest areas of consumer and government spending in the United States. National healthcare expenditures in the United States totaled $4.3 trillion in 2021, or $12,914 per person, representing a growth of 2.7% over 2020.[121] This figure is 18.3% of GDP. Personal healthcare spending represented 83.5% of the total 2021 healthcare expenditures. In 2021, the top areas of personal healthcare expenditures were hospital care ($1.32 trillion, 31.1% of total), physician services ($633.4 billion, 14.9%), clinical services ($231.2 billion, 5.4%) and prescription drugs ($378 billion, 8.9%).[122]

[121] "NHE Fact Sheet, 2021", Centers for Medicare & Medicaid Services. Link

[122] "National Health Expenditures, 2021: Decline in Pandemic-Related government spending results in 9-percentage point decrease in total spending growth", Apoorva Rama, AMA Policy Perspective, 2023. Link

© Strategy of Things, 2025. All rights reserved.

The U.S. healthcare industry is the largest employer of Americans employing 21.2 million people in 2020.[123] Employment in healthcare occupations is projected to grow 16% from 2020 to 2030, adding 2.6 million new jobs.[124] This growth is attributed to the U.S. aging population, creating more demand for healthcare services. There were 928,174 healthcare and social assistance businesses in the United States in 2020.[125] Ambulatory health care comprised the majority, 642,970 or 69.3%, of the businesses, followed by social assistance (184,970 or 20%), nursing and residential care (93,113 or 10%) and hospitals (7,121 or 7.8%).

5.3.7.1. Healthcare: IoT opportunities

The Internet of Things (IoT) is revolutionizing healthcare by enhancing how medical services are delivered, monitored and managed, leading to improved patient outcomes. Healthcare IoT devices, ranging from consumer fitness trackers to hospital equipment like remote monitoring tools and infusion pumps, are transforming the industry by addressing key challenges such as rising costs and access issues. The Internet of Medical Things (IoMT) devices enhance care delivery by enabling early diagnosis, remote patient monitoring and decentralized clinical trials, which reduce hospital visits and treatment costs. Wearable devices, like smartwatches, allow individuals to track vital signs and chronic conditions, enabling early detection, timely interventions and preventive care. The data collected by these IoT devices can be integrated with AI to provide physicians with personalized insights, tailoring treatments to patients' unique needs.

IoT technology use addresses major healthcare challenges, including rising costs, by enabling remote patient monitoring and decentralized clinical trials, reducing hospital visits and improving diagnoses. It facilitates access to healthcare for people in rural areas, those with disabilities and patients with chronic conditions by allowing doctors to remotely monitor patients and intervene when necessary. It also enhances the management of chronic diseases through continuous monitoring and medication adherence tracking. In the face of healthcare workforce shortages, IoT helps healthcare organizations become more efficient by integrating IoT and AI for data-driven insights and treatments, improving patient care while reducing the strain on medical staff.

Figure 5-15 below shows representative IoT use cases for the healthcare industry.

[123] U.S. Census Bureau, 2000, CBP Tables 2020. Link

[124] "Occupational Outlook Handbook - Healthcare Occupations", U.S. Bureau of Labor Statistics. Link

[125] U.S. Census Bureau, 2000, CBP Tables 2020. Link

© Strategy of Things, 2025. All rights reserved.

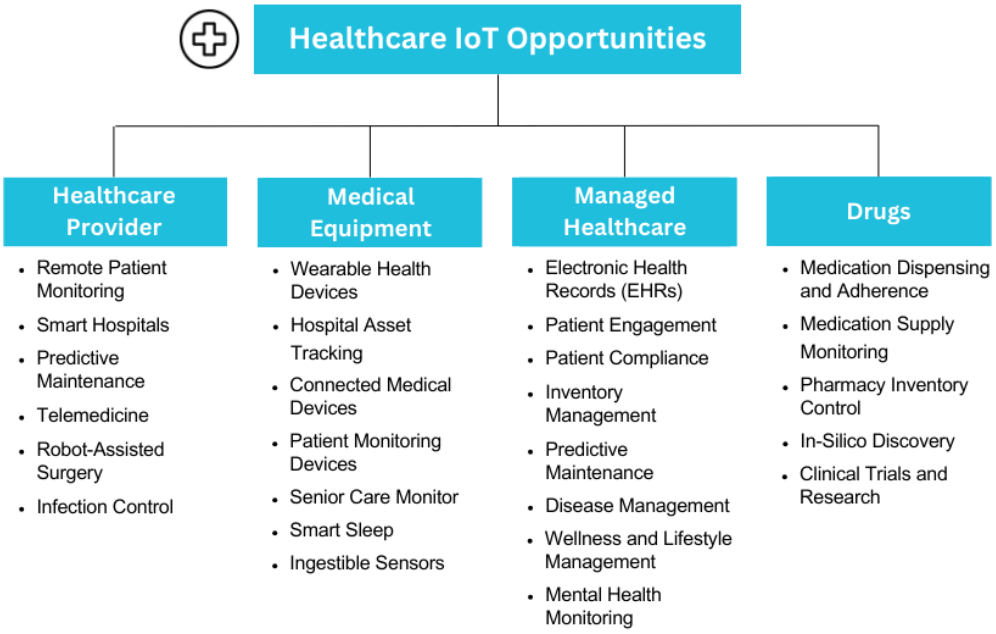


Figure 5-15: Healthcare: IoT Use Cases

The table below shows examples of IoT use cases aligned to key industry challenges.

Key Industry Challenges	IoT Opportunity See 19.2.1	Relevant IoT Solutions
Rising healthcare costs. See 19.1.2.1	Help control rising healthcare costs by enabling remote patient monitoring and telemedicine, reducing the need for hospital visits and stays.	• Predictive maintenance • Hospital asset tracking • Inventory management • Predictive maintenance • Pharmacy inventory control • Medication supply monitoring • Electronic Health Records (EHRs)
Access to healthcare. See 19.1.2.2	Improve access to healthcare by enabling remote consultations and treatments, making healthcare services accessible to people in remote areas or those with mobility issues.	• Telemedicine • Connected medical devices • Patient engagement • Wellness and lifestyle management • Patient compliance • Patient monitoring devices

© Strategy of Things, 2025. All rights reserved.

Key Industry Challenges	IoT Opportunity See 19.2.1	Relevant IoT Solutions
		• Senior care monitor • Wearable health devices
Chronic disease management. See 19.1.2.3	Wearable health monitors can provide continuous data on a patient's health, enabling better management of chronic diseases through timely interventions.	• Remote patient monitoring • Infection control • Smart sleep • Ingestible sensors • Disease management • Mental health monitoring • Medication dispensing and adherence
Healthcare workforce shortage. See 19.1.2.4	Address workforce shortages in healthcare by automating routine tasks, such as patient monitoring and data collection, freeing up healthcare professionals to focus on more complex tasks.	• Smart hospitals • Robot-assisted surgery • In-silico discovery • Clinical trials and research

Figure 5-16: Healthcare: Industry Challenges

5.3.7.2. IoT technology challenges in healthcare

The technology challenges are discussed below.

Cybersecurity. Cybersecurity is a major concern for connected healthcare devices and IoMT. The average medical device has 6.2 vulnerabilities.[126] Medical devices have long operational lives ranging from 10 to 30 years,[127] but more than 40% of medical devices are near end-of-life[128] and poorly or unsupported by the device manufacturer. Software update cycles vary from months to years. Many devices are built on embedded system platforms that have been customized by the manufacturers, are built on platforms with limited computing resources and are memory limited such that a quick patch in reaction to a cybersecurity vulnerability is not realistic. Many medical devices were not designed with cybersecurity protections, such as user authentication or credentials. See Section 19.3.1.1

Interoperability. The ability of healthcare IoT devices to communicate and exchange information with each other and medical systems will lead to timely and responsive care, automation of manual processes and improved quality, safety and operational efficiency while

[126] "Total Cost of Ownership Analysis on IoMT Cybersecurity Risk", August 2023. "Link

[127] Ken Fuchs, IEEE 11073 Standards Committee Chair, IHE DEV Domain Co-Chair.

[128] See note 126

© Strategy of Things, 2025. All rights reserved.

reducing human errors. Attaining interoperability is challenging as patient data are often stored in silos, with different systems using incompatible formats. In addition, healthcare and medical devices come from a variety of manufacturers and employ different and proprietary data formats and communication protocols. The adoption of open interoperability standards at the device level is hindered by the continued use of legacy devices, a lack of a business case for device manufacturers to move away from proprietary solutions and a lack of healthcare providers asking for open interoperable interfaces. See Section 19.3.1.2

Artificial intelligence. The use of artificial intelligence with medical devices by healthcare professionals can transform healthcare and create significant improvements in patient outcomes. For example, an AI-enabled glucose monitoring device allows physicians to create personalized care plans for patients, resulting in markedly improved healthcare outcomes. While use of AI offers significant opportunities for advances in healthcare through the Internet of Medical Things (IoMT), it is hindered by several challenges. These include limited access to high quality data, biased data, lack of transparent and explainable models, data privacy, inability of IoT devices to run AI models and limited ability to scale into clinical practices. See Section 19.3.1.3

5.3.8. Retail

The retail industry is a significant sector of the U.S. economy, playing a crucial role in driving consumer spending, employment and overall economic growth. Retail sales in the United States totaled $5.57 trillion in 2020.[129] Online sales have been rising since 2000, rising from 0.6% of all retail sales in Q4 2000 to a high of 16.4% in Q2 2020.[130] When its indirect and induced contributions are factored in, the total impact of American retail was $3.9 trillion or 18.7%[131] of the overall U.S. GDP.

The U.S. retail industry is the second largest employer of Americans after healthcare, employing 32.1 million people in 2018 with 21.1 million (65.8%) of retail workers employed at firms with 50 or more people.[132] The retail industry created an additional 19.8 million jobs indirectly.[133] Retailers created $1.04 trillion in total labor income, with $680.6 million (65.4%) coming from businesses employing 50 people or more.[134] Small businesses employing 50 people or less represented 98.5% of all retailers in 2018.[135]

---

[129] Annual Retail Trade Survey: 2020. Link

[130] E-Commerce Retail Sales as a Percent of Total Sales, FRED economic research. Link

[131] Table 5, "The Economic Impact of the U.S. Retail Industry", PWC and National Retail Federation report, May 2020. Link

[132] Table E-4, "The Economic Impact of the U.S. Retail Industry", PWC and National Retail Federation report, May 2020. Link

[133] ibid, Page 13

[134] ibid, Table 7

[135] Table E-4, "The Economic Impact of the U.S. Retail Industry", PWC and National Retail Federation report, May 2020. Link

© Strategy of Things, 2025. All rights reserved.

5.3.8.1. Retail: IoT opportunities

The retail industry is undergoing a technology-driven evolution, transitioning from e-commerce (Retail 3.0) to omni-channel retail (Retail 4.0), where physical and digital shopping experiences seamlessly integrate. The COVID-19 pandemic accelerated this transition. IoT is set to significantly transform the retail industry by enabling the collection of new data that addresses key challenges and enhances operations. Technologies like RFID and asset tracking devices enable real-time inventory management, reducing shrinkage in stores and warehouses, and improving stock distribution.

For the retailer, Bluetooth beacons provide insights into shopper movement patterns, allowing for optimized store layouts and personalized marketing to increase sales. Smart shelves detect when products need restocking, preventing lost sales, while embedded sensors in high-value items discourage theft. Additionally, self-checkout kiosks help alleviate labor shortages by allowing customers to process purchases independently, freeing up staff for more complex tasks.

Figure 5-17 below shows some representative IoT use cases for the retail industry.

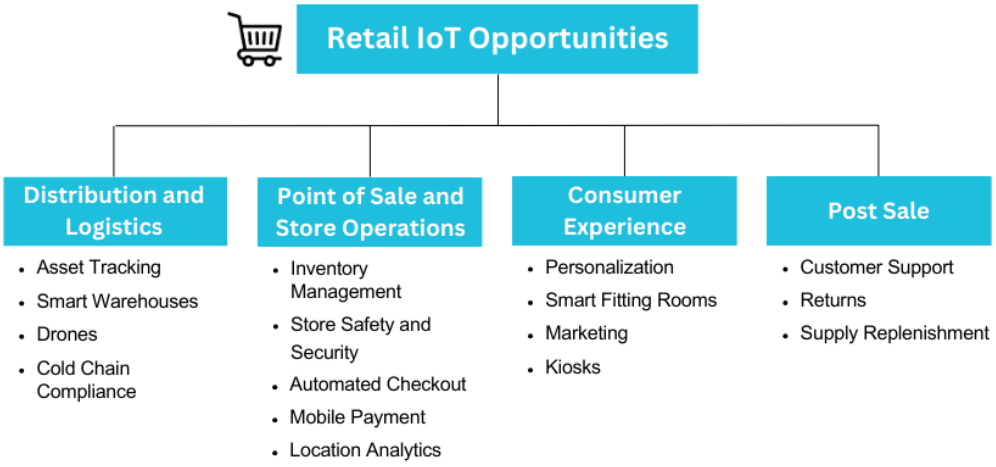


Figure 5-17: Retail: IoT Use Cases

The table below shows examples of IoT use cases aligned to key industry challenges.

Key Industry Challenges	IoT Opportunity See 20.2.1	Relevant IoT Solutions
Labor Shortage See 20.1.2.1	Mitigate labor shortages by automating routine tasks such as inventory tracking and checkout processes.	• Drones (in warehouses) • Store safety and security • Automated checkout • Smart fitting rooms and mirrors • Kiosks

© Strategy of Things, 2025. All rights reserved.

Key Industry Challenges	IoT Opportunity See 20.2.1	Relevant IoT Solutions
Inventory management See 20.1.2.2	Provide real-time inventory tracking, reducing overstock and out-of-stock situations.	• Asset tracking • Smart warehouses • Drones • Cold chain compliance • Inventory management • Store safety and security • Returns tracking and management • Supply replenishment
Shrinkage. See 20.1.2.3	Reduce shrinkage by providing real-time tracking of goods and alerting staff to potential thefts. Smart shelves and RFID tags can help identify when items go missing.	• Asset tracking • Inventory management • Store safety and security
Profitability. See 20.1.2.4	Improve inventory management, reducing shrinkage and automating routine tasks. Additionally, IoT can provide customer data that can be used to improve marketing and sales strategies.	• Asset tracking • Inventory management • Automated checkout • Mobile payment • Location analytics • Personalization • Smart fitting rooms and mirrors • Marketing • Kiosks • Customer support • Supply replenishment
Retailer resilience. See Section 20.1.2.5	Enhance resilience by providing real-time data that can be used to quickly respond to changing market conditions.	• Asset tracking • Inventory management

Figure 5-18: Retail: Industry Challenges

5.3.8.2. IoT technology challenges in retail

The technology challenges are discussed below.

© Strategy of Things, 2025. All rights reserved.

Low-cost sensors. Retail is a low margin business, with retailers having limited "free cash" available to invest in IoT and other initiatives. Low-cost IoT systems are a necessity in retail where applications requiring extremely large numbers of sensors are common. While RFIDs are low cost and the most popular IoT technology in retail, they are well suited mainly for a small number of applications like inventory management. Other IoT technologies, such as beacons, condition sensors and cameras and robotics support use cases not possible with RFID. These devices, however, are significantly more expensive than RFIDs and face financial barriers to adoption by retailers. New low cost IoT technologies are needed to facilitate adoption in the retail industry. See Section 20.3.1.1

Privacy enhancing technologies. The use of IoT technologies and the data it collects enable retailers to understand their customers better and offer personalized services and experiences not previously possible. However, privacy issues hinder the use of IoT technologies in retail. Regulations limit what data can be collected and how it is used. Retailers and the IoT solutions they use must balance the need for collecting and using data with the customers' expectations for privacy. The development and advancement of technical approaches, such as privacy enhancing technologies, are a necessary facilitator for retail IoT adoption. See Section 20.3.1.2

Artificial intelligence. As IoT adoption grows in the retail industry, it is expected to generate a "tsunami of data" that retailers are not prepared to handle. Artificial Intelligence (AI) technologies are poised to help retailers make sense of data, create insights and act on those insights in both real time and autonomously. However, the AI models may not be accurate, explainable and trustworthy. Privacy concerns limit what data can be collected and how it is managed and used. This in turn impacts algorithm development and model training. The decision process used by the AI model to create outcomes is not visible, transparent or easily explainable to decision-makers. AI may lead to potential outcomes and decisions that are "biased, discriminatory, exclusionary or otherwise unfair. See Section 20.3.1.3

5.3.9. Renewable Energy

Spurred by ongoing environmental sustainability initiatives and more recently, the Inflation Reduction Act of 2022,[136] the renewable energy industry is one of the fastest growing industries in the United States. Investments in renewable energy assets rose from just over $30 billion in 2014 to $47 billion in 2021.[137] The U.S. renewable energy capacity grew from 185 gigawatts (GW) to 353 GW over this period. Electric power generation grew from 550 terawatt hours (TWh) to 858 TWh over the same period.[138]

The percentage of power consumed in the United States that comes from primary renewable sources (wind, solar, geothermal, hydroelectric and biomass) has risen steadily from 6.2% in

[136] "H.R. 5376 – Inflation Reduction Act of 2022", Congress.gov. Link

[137] "Sustainable Energy in America: 2022 Factbook", p. 35, Bloomberg NEF, 2022. Link

[138] "Sustainable Energy in America: 2022 Factbook", p. 22, Bloomberg NEF, 2022. Link

© Strategy of Things, 2025. All rights reserved.

2000 to 12.5% in 2021.[139] In April 2022, renewable energy sources were 28% of total energy consumed.[140] By 2030, that percentage will reach 30%.[141]

The U.S. renewable industry directly and indirectly employed 620,000 people in 2020.[142] Of this, 517,000 worked in renewable electric power generation, 103,000 worked in the renewable fuels sector. These include jobs that indirectly support renewable energy generation. For example, of the 317,000 jobs in solar, 165,000 were in construction, 49,700 in professional services and 41,900 in solar equipment manufacturing.[143]

5.3.9.1. Renewable Energy: IoT opportunities

IoT plays a critical role in the operation and maintenance of renewable energy systems. IoT technology helps address key challenges in integrating renewable energy sources into the grid by optimizing electricity generation. For example, sensors adjust solar panels and wind turbines to maximize power output, reducing reliance on fossil-fuel "peaker plants"[144] to meet peaks in demand. IoT technology also improves the management of distributed energy resources (DERs) like solar and battery systems by allowing energy storage and strategic discharge to the grid during periods of high demand, further reducing fossil fuel use.

Additionally, IoT technology enhances grid stability and resilience through smart inverters that maintain grid reliability by autonomously adjusting to voltage and frequency changes. Maintenance of renewable energy systems is also streamlined with IoT, as sensors monitor equipment health, optimizing battery performance and reducing unplanned downtime. This remote monitoring increases operational efficiency and supports a more productive workforce, particularly in light of labor shortages in the renewable energy industry.

Figure 5-19 below shows some representative IoT use cases for the renewable energy industry.

[139] "July 2022 Monthly Energy Review", U.S. Energy Information Administration. Link

[140] Table 1.1. Net Generation by Energy Source: Total (All Sectors), 2012-May 2022, Electric Power Monthly. Link

[141] "Renewables on Track to Provide 33-50% of U.S. 2030 Electricity, Biden's 80% Goal Still Possible", K. Bossong, July 22, 2021. Link

[142] United States Energy & Employment Report 2021, U.S. Department of Energy. Link

[143] ibid.

[144] A peaker plant is a specialized type of power plant designed to generate electricity during periods of high electricity demand. These plants are typically activated during peak load times, such as hot summer days or cold winter evenings when energy consumption is at its highest.

© Strategy of Things, 2025. All rights reserved.

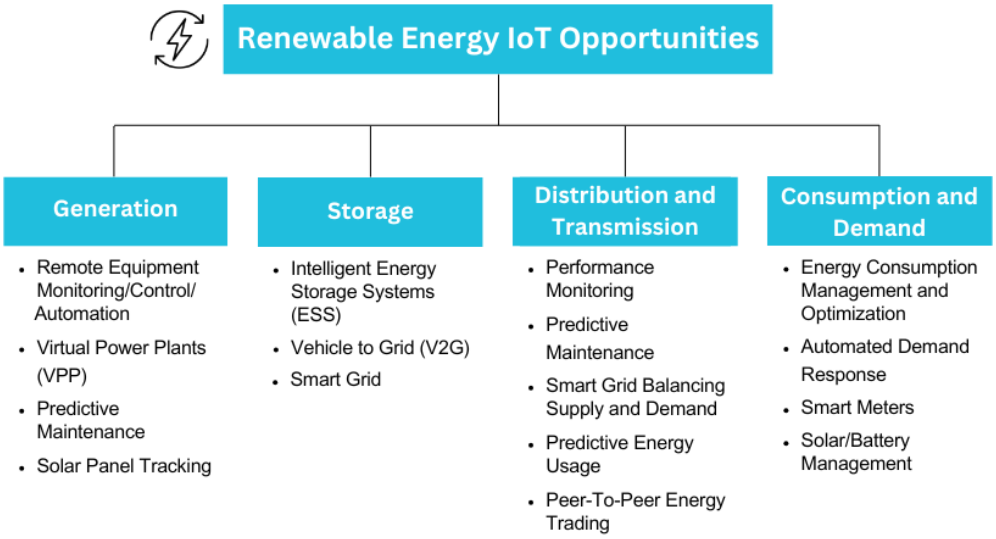


Figure 5-19: Renewable Energy IoT Use Cases

Figure 5-20 below shows examples of IoT use cases aligned to key industry challenges.

Key Industry Challenges	IoT Opportunity See 21.2.1	Relevant IoT Solutions
Integration of renewable sources into grid infrastructure. See 21.1.2.1	Facilitate the integration of renewable energy sources into the grid by providing real-time data on energy production and consumption. Balances supply and demand and ensures the stability of the grid.	• Intelligent Energy Storage Systems (ESS) • Performance monitoring • Vehicle to grid (V2G) • Automated demand response
Aging and outdated electric grid infrastructure. See 21.1.2.2	Monitor the condition of the grid infrastructure, enabling predictive maintenance and timely upgrades. Helps extend the lifespan of the infrastructure and improves its ability to manage the variable nature of renewable energy.	• Virtual Power Plants (VPP) • Predictive maintenance • Solar panel tracking • Predictive energy usage • Smart grid balancing
Workforce labor shortage. See 21.1.2.3	Address labor shortages by automating routine tasks, such as monitoring and maintenance.	• Predictive maintenance • Smart Grid • Energy consumption management and optimization • Smart Meters

© Strategy of Things, 2025. All rights reserved.

Key Industry Challenges	IoT Opportunity See 21.2.1	Relevant IoT Solutions
Permitting and planning obstacles See 21.1.2.4	Streamline the permitting and planning process by providing accurate data on potential renewable energy sites, such as wind speed and solar irradiance. Helps identify the most suitable locations for renewable energy installations.	• Peer-to-peer energy trading • Solar/battery management • Supply and demand

Figure 5-20: Renewable Energy: Industry Challenges

5.3.9.2. IoT technology challenges in renewable energy

The technology challenges identified are discussed below.

DER cybersecurity. The growing integration of Distributed Energy Resources (DERs), such as solar, wind and energy storage systems, into the electric grid supports the transition to clean energy. However, DERs represent millions of cybersecurity vulnerability points. Each DER is owned by an independent power producer using IoT enabled equipment from many different vendors with varying levels of cybersecurity measures, hardware configurations, software updates and configurations. DER owners, integrators, operators and aggregators may not have the skills and knowledge, tools and resources to address the cybersecurity vulnerabilities of their systems. Finally, in an automated environment with millions of DERs, the implied trust model which allows different systems and devices in the grid to communicate with each other "unchallenged" increases risk to the integrity of the grid and its ability to monitor, manage and deliver electricity to its users. See Section 21.3.1.1

Interoperability. Interoperability is a major challenge in the renewable energy industry. The ability of the various energy management devices and systems to communicate and interoperate with each other is essential to distributing electricity to meet demand and the reliable operation of the grid. Some examples of a lack of interoperability include equipment (batteries, inverters) that may not work together or with legacy devices, inverters and/or batteries that lack a standardized set of capabilities (e.g. black start, back-up power), legacy devices that lack the capability to connect to the Internet, or communicate with energy aggregators, Building Energy Management Systems that cannot communicate with automated demand response systems, DER system components and the grid. Reasons for the lack of interoperability include a lack of standards, varying government regulations and policies across states and regions, piecemeal approaches to DER integration into the grid and reluctance to move away from proprietary protocols. See Section 21.3.1.2

Data management. Information is essential to the operation of the modern electric grid. The IoT data produced from measuring the real time health, performance and energy production of wind turbines and solar panels supports actions that optimize grid performance and better meet demand needs. The management of these data, however, is a major challenge for several reasons. The data comes from a variety of diverse and siloed sources in varying levels of syntactic and semantic interoperability, quality and accuracy. The IoT data takes shape as large continuous streams that must be stored, processed and analyzed in real time. The data is subject to a variety

© Strategy of Things, 2025. All rights reserved.

of existing and evolving regulatory and compliance requirements. This inability to manage the growing amounts of data threatens the operation and automation of the grid, lessens the use of analytics and AI to plan and optimize grid operations, reduces regulatory compliance and limits innovation and the evolution of a potentially autonomous grid. See Section 21.3.1.3

© Strategy of Things, 2025. All rights reserved.

6. IoT Technology Infrastructure Gaps

One of the objectives of this research study is to identify the technology infrastructure gaps hindering the development, adoption and operation of IoT into the U.S. economy and civil society. These gaps are identified using the process shown in Figure 6-1 and are described below:

- Identify industry level IoT technology infrastructure challenges. For each industry studied, an initial set of IoT technology challenges was identified through secondary research, surveys and interviews. The specific challenges by industry are discussed in Section 5.3. These challenges are discussed in detail in Sections 0 to 21.
- Aggregate and analyze industry challenges. Individual technology challenges from each industry are reviewed and aggregated into a broader industry challenge. For example, a number of industries cited specific privacy-related challenges. These specific challenges are aggregated to create a broader privacy challenge. The IoT technology challenges are aggregated and summarized in Section 5.1.
- Identify the cross industry IoT technology infrastructure gaps. The cross industry IoT technology infrastructure gaps were identified by mapping them to one of three gap categories. Figure 6-1 below shows how these categories are aligned to the IoT stages of evolution and provides a context on prioritization.

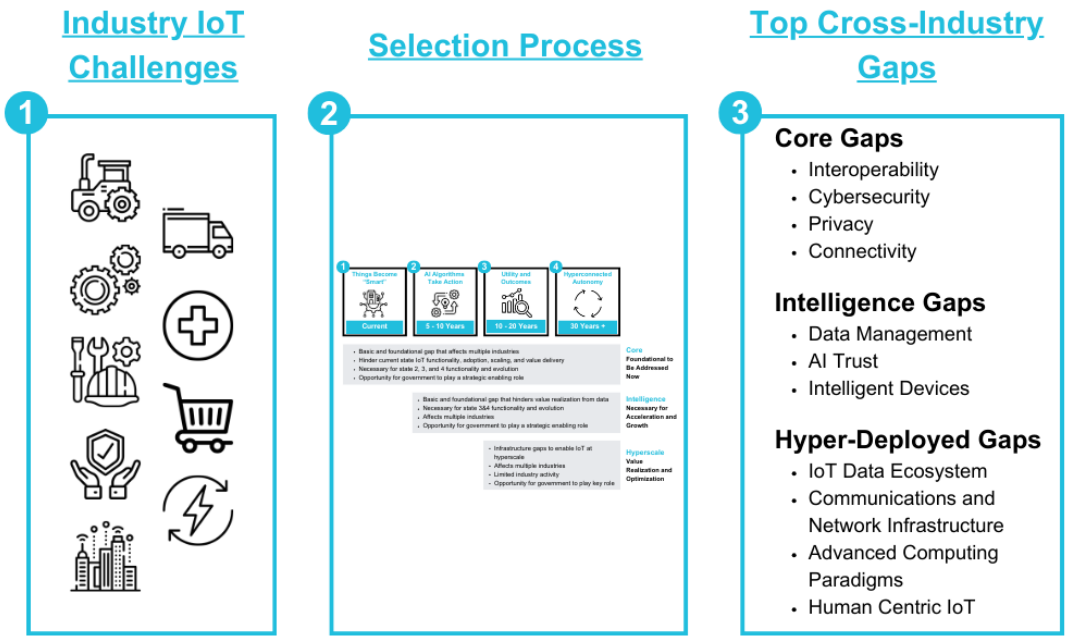


Figure 6-1: Overview of Process used to Identify Key Gaps

The identification of the top cross industry IoT technology infrastructure gaps considers the maturity and evolution of IoT over the next 10 to 30 years by mapping them to one of three categories. These categories are:

© Strategy of Things, 2025. All rights reserved.

- **Core**. The core gaps are gaps in foundational IoT technology infrastructure. Foundational infrastructure and capabilities are essential for the function and operation of IoT. They are needed in all industries and span all four stages of the IoT evolution as shown in Figure 4-7. Examples of foundational capabilities include connectivity and interoperability. The inability to overcome core gaps hinders IoT adoption and operation today and limits the further evolution of IoT. Core IoT technology gaps meet the criteria shown in Figure 6-2.
- **Intelligence**. The Intelligence gaps are gaps in technology infrastructure that support and enable the intelligent and autonomous operation of IoT. They are needed in all industries and span three stages (2, 3 and 4) of the IoT evolution. Examples of intelligent IoT capabilities include data management and edge computing. The inability to overcome intelligence gaps hinders the integration of intelligence into IoT today and limits the further evolution of an intelligent and autonomous future state IoT.
- **Hyper-Deployed**. The future IoT-enabled economy and society may contain billions of interconnected devices working autonomously in a secure and trusted manner. Hyper-Deployed gaps are gaps in technology infrastructure that if addressed, support and enable the intelligent and autonomous operation of a hyperconnected IoT at scale. They need to be addressed in all industries and span the last two stages (3 and 4) of the IoT evolution. Examples of hyper-deployed IoT gaps include the need for a hyperconnected communications infrastructure and human centric artificial intelligence. The inability to overcome hyper-deployed gaps hinders the emergence of a hyperconnected autonomous economy integrated with billions of IoT devices and systems.

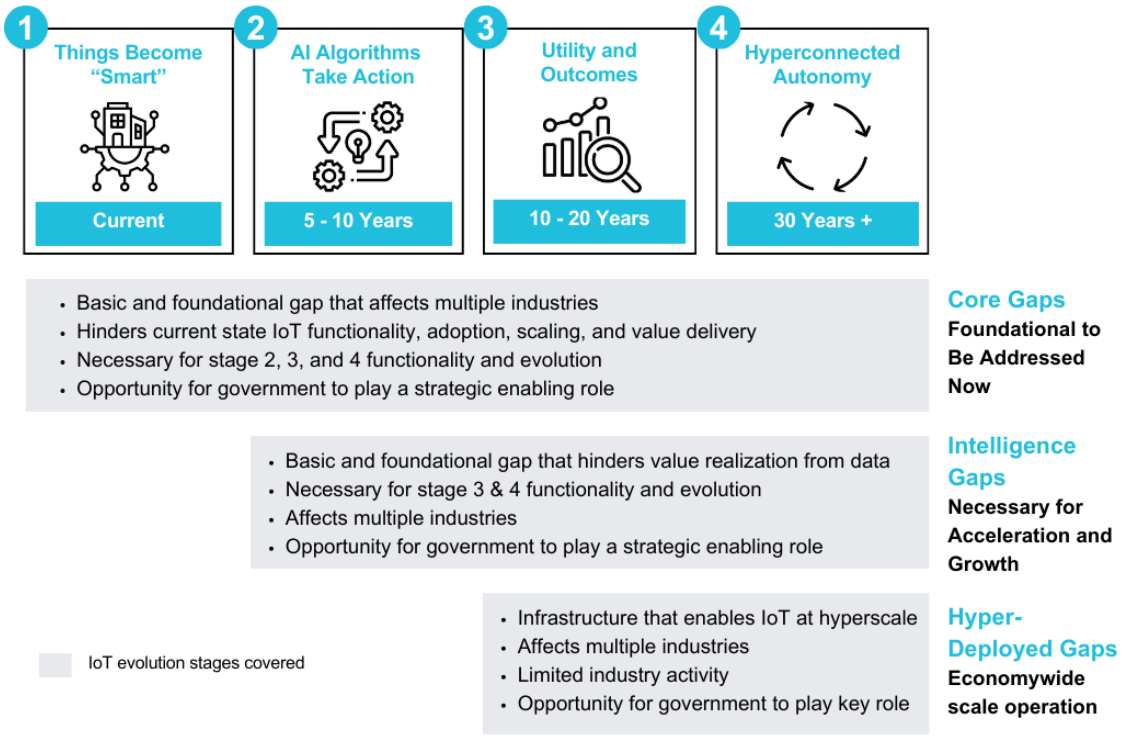


Figure 6-2: IoT Technology Infrastructure Gap Categories and Criteria

© Strategy of Things, 2025. All rights reserved.

Using this approach, Figure 6-3 shows the cross industry IoT technology infrastructure gaps that were identified for each category.

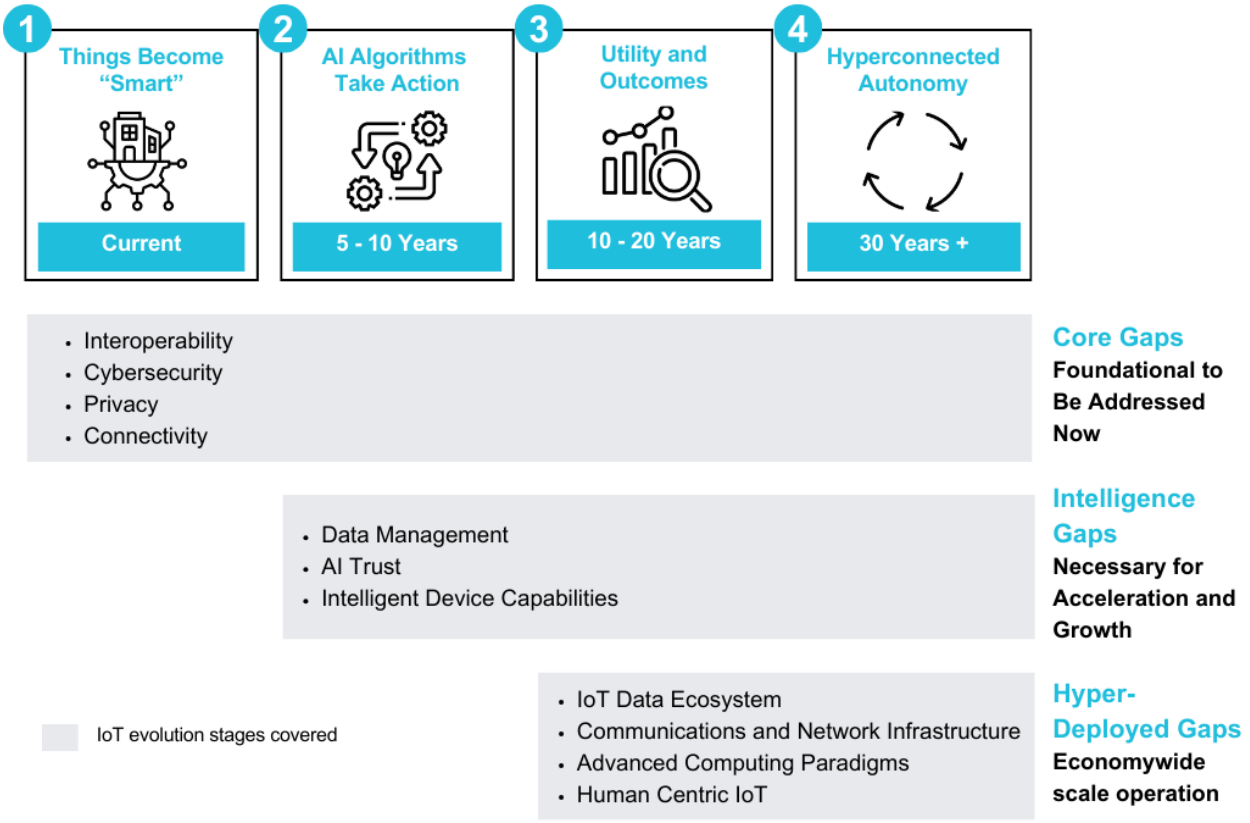


Figure 6-3: Cross industry IoT Technology Infrastructure Gaps by Category.

For the remainder of this section, each of these gaps is discussed as they fall in their respective categories.

6.1. Core gaps

The following is a list of core gaps discussed in the section below:

- Interoperability
- Cybersecurity
- Privacy
- Connectivity

6.1.1. Core: Interoperability

Interoperability was identified as a top challenge in seven of the nine industries studied. These industries include agriculture, manufacturing, construction, cities, transportation and logistics, healthcare and renewable energy.

© Strategy of Things, 2025. All rights reserved.

The lack of interoperability slows the full realization of benefits offered by IoT by preventing IoT devices from connecting, communicating and collaborating with each other and with other systems. It also hinders IoT's evolution to future stages where intelligence and hyperconnectivity combine at scale and bring national economic and society-wide transformational benefits. Other ways it hinders IoT are described below:

- **Difficult to integrate devices and systems.** Interoperability challenges lead to situations where devices and systems from one vendor may not work with a similar system from a competing vendor due to incompatible communication protocols. Data may be in different formats and have different meanings. In some instances, older systems may not work with newer systems from the same vendor.
- **Inability to innovate and realize the full benefits of interconnected and automated IoT systems.** In manufacturing, factories have substantial existing investments in legacy and modern industrial and Operations Technology (OT) systems. The inability of IoT technologies to integrate with these systems to share information and services creates operational inefficiencies and increases production costs.
- **Unable to realize cost savings and revenue opportunities.** In healthcare, the lack of medical device interoperability has the potential to lead to $35 billion in missed annual cost savings across the U.S. healthcare system.[145] In renewable energy, attaining interoperability can lead up to $10 billion annually in estimated savings from lower transaction costs, increased operating efficiency, lower operations and maintenance needs and lower design and installation costs.[146]
- **Create adverse environmental impacts due to inefficient operations.** In renewable energy, interoperability challenges, some attributed to a lack of standards, hinder integration of energy efficiency and renewable energy technologies, resulting in decreased adoption of these technologies. In contrast in transportation and logistics, interoperability enables data sharing of logistics data in near real-time to facilitate operations and can reduce global freight emissions by 22%.[147]
- **Create vendor lock-in and switching barriers.** The lack of interoperability creates a fragmented market of "walled garden" IoT solutions that work with a small set of "compatible" equipment, leading to reduced choices and vendor "lock-in."

The federal government supports and facilitates interoperability through the development of standards. Except in matters related to safety, environmental and health concerns, the U.S. government's approach to standards development is "industry leads, government supports." In this capacity, the federal government provides the foundational pre-standards research and development necessary for industry to establish technical standards.

Federal agencies may participate in standard-setting organizations, both domestically and internationally, to advocate for U.S. interests and ensure that U.S. standards are harmonized with

[145] "The value of medical device interoperability," West Health Institute, 2013. Link

[146] "Financial Benefits of Interoperability," Harbor Research, Gridwise Architecture Council, 2009. Link

[147] "Solving the Global Supply Chain Crisis with Data Sharing," M. Westervelt, R. Aland and I. Dupraz. Center for Reimagined Mobility, June 28, 2022. Link

© Strategy of Things, 2025. All rights reserved.

global practices. Finally, the government promotes consensus standards by adopting technologies with those standards and incorporating their requirements into federal regulations and procurement processes to facilitate broader adoption and adherence.

Interoperability issues are broad, complex and differ between industries. At an aggregate level, our research identified some representative opportunities for the federal government to facilitate IoT interoperability. These include the following:[148]

- **Semantic and syntactic interoperability.** The heterogeneity of IoT devices in standards, datasets and formats reduces interoperability. While interoperability challenges vary by industry, new methods and approaches to facilitate interoperability that are developed or investigated have the potential to address these concerns.
- **Cross-platform interoperability.** IoT applications may cut across industry domains, such as in transportation and smart cities. Many standards focus on the device and network levels and less on the platform levels and their interactions, which if addressed, have the potential to address issues head-on.
- **Interoperability testing of solutions and standards**. IoT solutions follow certain standards and testing is performed to verify that those standards have been implemented correctly. Support for the development of testbeds facilitates the verification of interoperability and that standards have been implemented correctly.
- **AI-facilitated interoperability.** The use of AI technology to translate between formats and meanings can facilitate interoperability. Examples include mapping and aligning data schemas to translating protocols and adapting to changes in devices. AI offers the potential to facilitate interoperability as systems evolve.
- **Interoperability of future IoT technologies.** IoT continues to evolve with technologies at varying stages of maturity. Pre-standardization initiatives, such as developing frameworks and the science to develop standards, are needed to facilitate the development of standards for these evolving technologies.

The federal government plays a key role in achieving industry interoperability through a variety of actions. This role and representative actions are discussed in detail in Section 8.

6.1.2. Core: Cybersecurity

Cybersecurity was identified as a top challenge in manufacturing, insurance, healthcare and renewable energy and frequently mentioned as an area of concern in the remaining industries.

Cybersecurity concerns slow the realization of benefits offered by IoT by reducing user trust and confidence, preventing its adoption and use and hindering its integration and interconnection with other information technology and industrial operations technology systems. It also slows IoT's evolution where intelligence and hyperconnectivity combine at scale to bring economy and society-wide transformational benefits.

Cybersecurity concerns slow IoT adoption, scaling, value realization and delivery and evolution in many ways including those listed below:

[148] "Interoperability in Internet of Things: Taxonomies and Open Challenges," Link

© Strategy of Things, 2025. All rights reserved.

- **Increasing intrusion risks.** Cybersecurity risks were identified as one of the top three project risks that hinder IoT adoption.[149] IoT presents a new and massive attack surface for cybercriminals to exploit. Some IoT devices and systems may have weak authentication and authorization controls, inadequate encryption and vulnerabilities in hardware, firmware and software that cybercriminals can exploit.
- **Raising cybersecurity risks across entire industries.** IoT technology provides cybercriminals with new ways to access certain industries. Manufacturing is the number one industry in North America targeted by cybercriminals.[150] In factories and industrial environments, the introduction of IoT into formerly "air gapped"[151] environments containing Operations Technology (OT) systems provides cybercriminals with potential entry points.[152]
- **Disrupting operations and services.** One consequence of cyberattacks is the potential to disrupt operations and services, especially in critical applications. For example, IoT devices in the smart grid have the potential to be compromised, resulting in a disruption of electricity supply and delivery to downstream consumers. In healthcare, ransomware and malware are able to spread to medical devices, resulting in potential risk to patient outcomes.[153]
- **Losing personal and proprietary information.** Device intrusions may allow cybercriminals lateral access to the backend systems, where confidential and proprietary data are stored. This data is attractive to cybercriminals.
- **Incurring financial damages.** Cybersecurity incidents involving IoT devices can result in significant economic losses due to downtime, recovery costs, legal fees and damage to business operations.
- **Creating regulatory compliance issues.** Some industries are subject to regulations and compliance standards governing data protection and cybersecurity. Cybersecurity challenges could lead to non-compliance with these regulations, leading to fines, legal penalties and other regulatory consequences.
- **Incurring reputational, safety and national security risks.** Cybersecurity breaches may lead to a variety of risks. Companies and organizations that fail to secure IoT devices risk damaging their reputation and losing the trust of customers, partners and stakeholders.

IoT cybersecurity is a complex and wide-ranging challenge. Each industry has different operating environments that create unique cybersecurity challenges. For example:

---

[149] "Three Main Risks That Prevent Companies From Adopting Iiot Solutions", IIoT World, November 24, 2021. Link

[150] "X-Force Threat Intelligence Index 2022", IBM Security Report, February 2022. Link

[151] An air-gapped system is isolated from other systems and cannot connect wirelessly or physically with other systems and the Internet.

[152] "2022 State of Operational Technology and Cybersecurity Report", Fortinet report, 2022. Link

[153] "Total Cost of Ownership Analysis on Connected Device Cybersecurity Risk," Asimily Report, 2023. Link

© Strategy of Things, 2025. All rights reserved.

- Factories employ industrial automation and control systems and devices in a "cybersecurity by air gap" environment that is now exposed to the outside world through IoT.
- Hospitals are filled with medical devices 10 to 30 years old with infrequent to no firmware updates. Many of these devices collect and access patient data without requiring user authentication or credentials.
- The distribution of millions of solar panel and battery systems into homes and communities decentralizes cybersecurity responsibility to the individual system owner.

This section focuses on the industry-agnostic aspects of cybersecurity. Our research identified the following IoT technology infrastructure opportunities that will partially address the cybersecurity challenges. These include the following:

- Artificial intelligence based IoT cybersecurity
- Post Quantum Cryptography (PQC)
- Other areas of research

Each of these is discussed in the following sections.

6.1.2.1. Artificial intelligence based IoT cybersecurity

Many studies have identified the use of artificial intelligence as an important capability in addressing IoT cybersecurity threats.[154,155] AI is well suited for analyzing vast amounts of data from IoT devices, detecting and recognizing patterns and responding to potential attacks in a proactive and timely manner.

The integration of AI into the broader "cybersecurity fabric" of capabilities and tools enables organizations to have comprehensive visibility of all their IoT devices, perform unified threat analysis and automate threat containment.[156] Management consultancy Deloitte calls AI a "force multiplier that enables organizations not only to respond faster than attackers can move, but also to anticipate these moves and react to them in advance."[157]

Many cyberattacks can be mitigated or prevented by early detection and recognition of unusual activities and traffic patterns. Some attacks are subtle and less obvious, escaping the notice of people, algorithms and AI. Threats are evolving, with the newest ones being the least detectable. These attacks and how to defend against them effectively are critical topics for research. Representative areas of related research include those listed below:

---

[154] "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review," U. Tariq, I. Ahmed, et al. Sensors 2023, 23(8), 4117, April 19, 2023. Link

[155] "Cybersecurity Risk Analysis in the IoT: A Systematic Review," T. AlSalem, M. Almaiah and A. Lutfi. Electronics 2023, 12(18), 3958; September 20, 2023. Link

[156] "The Role of Artificial Intelligence in IoT and OT Security," BrandPost, CSO, October 30, 2018. Link

[157] "Cyber AI: Real defense," E. Bowen, W.Frank and D. Golden, Deloitte Insights, Deloitte Consulting. December 7, 2021. Link

© Strategy of Things, 2025. All rights reserved.

- Research, development and enhancement of AI cybersecurity algorithms, exploring ensemble learning approaches and implementing real-time adaptive cybersecurity systems.[158]
- Research and development of lightweight and efficient ML and AI models for IoT devices with limited resources while ensuring their security and privacy.[159]
- Approaches to detect and protect AI algorithms against input and data poisoning attacks[160]

One research publication, an extensive literature survey of the use of AI in cybersecurity, noted research gaps for further study. These gaps were identified and organized into specific topic categories.[161] These are:

- **Emerging areas of AI cybersecurity applications.** Research gaps to be addressed include real time automated retrieval of key risk indicators to create an early-warning system, detection of new attacks, and improving predictive intelligence and analytics to support automated decision-making. Other topics of research include studying AI-powered cyber defense and resilience, data breach prevention and discovery and context driven alert processing triage and AI powered incident response.
- **Data representation.** Research gaps include refined data representation, context aware adaptive cybersecurity, incremental learning and recency mining.
- **Advanced AI methods.** Research gaps include multiple data source analysis, explainable AI and augmented human-AI intelligence.
- **Infrastructure to support AI.** Research gaps include the development of information sharing hubs at national and international levels to enable threat intelligence platforms at the economy wide level and the evaluation and development of AI models using new, real-time and broader datasets.

6.1.2.2. Post Quantum Cryptography (PQC)

Quantum computing is a rapidly emerging technology that uses the principles of fundamental physics to solve extremely complex problems in a very short amount of time. While traditional computer systems use digital processors to perform calculations, quantum computing uses "specialized hardware and algorithms that take advantage of the principles of quantum mechanics."[162]

---

[158] "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review," U. Tariq, I. Ahmed, et al. Sensors 2023, 23(8), 4117, April 19, 2023. Link

[159] See note 154

[160] "Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity," M. Kuzlu, C. Fair and O. Guler, Discov Internet Things 1, 7 (2021). February 24, 2021. Link

[161] "Artificial intelligence for cybersecurity: Literature review and future research directions," R. Kaur, D. Gabrijelčičand and T. Klobučar. Information Fusion, Volume 97, 2023, 101804, ISSN 1566-2535. Link

[162] "Quantum computing could threaten cybersecurity measures. Here's why – and how tech firms are responding," S. Torkington, World Economic Forum, April 23, 2024. Link

© Strategy of Things, 2025. All rights reserved.

However, this technological advancement poses significant challenges to cybersecurity. One of the primary concerns is that "quantum computers have the potential to bypass the encryption locks that currently protect the world's communications and data."[163] According to the 2022 White House National Security Memorandum/NSM-10 on Quantum Computing, "a quantum computer of sufficient size and sophistication, also known as a Cryptanalytically Relevant Quantum Computer (CRQC), will be capable of breaking much of the public-key cryptography used on digital systems across the United States and around the world."[164]

IoT devices are particularly vulnerable to the risks posed by quantum computing. Professionals often operate IoT devices in environments with limited computational and energy resources, making them ill-equipped to handle the sophisticated encryption algorithms required to resist quantum attacks. Additionally, the sheer scale and diversity of IoT deployments make it challenging for users to implement security updates and patches uniformly across all devices. As a result, cybercriminals could exploit vulnerabilities in IoT devices to gain unauthorized access to sensitive data or launch large-scale attacks, potentially causing widespread disruption and damage.

While the concerns about the ability of quantum computers to break today's encryption algorithms are valid, the availability of cryptanalytically relevant quantum computers (CRQC) powerful enough to do so will not be developed until at least the 2030s.[165] To prepare for the post-quantum computing era, NIST is soliciting, evaluating and standardizing a number of quantum-resistant public-key cryptographic algorithms.[166]

However, integrating post-quantum (or quantum-safe or quantum-resistant) cryptography into IoT devices is a balance between security, performance and resource limitations. The PQC algorithms are computationally intensive but IoT devices are compute, memory and energy constrained. Latency is introduced during encryption and decryption, which requires limiting the size of public keys for low latency applications but makes the PQC less resistant.[167] The PQCs must be backward compatible and work with existing IoT communication protocols. Opportunities exist for continued research to identify, understand, evaluate and optimize lightweight quantum safe algorithms that are suitable for use on resource constrained IoT devices for various domains and applications.

---

[163] See note 162

[164] "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," NSM-10, The White House, May 4, 2022. Link

[165] "When a Quantum Computer Is Able to Break Our Encryption, It Won't Be a Secret," E. Parker, RAND, September 13, 2023. Link

[166] "NIST Asks Public to Help Future-Proof Electronic Information," U.S. National Institute of Standards and Technology, December 20, 2016. Link.

[167] "Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms," R. Asif. IoT 2021, 2(1), 71-91; February 5, 2021. Link

© Strategy of Things, 2025. All rights reserved.

6.1.2.3. Other areas of research

A scan of the research literature has identified other areas of research opportunities. Some of these opportunities include the following:[168]

- **Context-aware adaptive cybersecurity frameworks.** Evolving cybersecurity threats render static cybersecurity measures and responses inadequate and irrelevant. Context-aware adaptive approaches assess and dynamically adjust security measures based on real-time threat intelligence.
- **Secure firmware and hardware design.** The security of IoT devices heavily depends on the integrity of their firmware and hardware components. Studies emphasized the importance of implementing secure development practices and utilizing hardware security modules to safeguard against physical attacks and firmware tampering. Future research should address the challenges of secure firmware updates, hardware-based attestation and supply chain security.
- **Lightweight encryption algorithms.** IoT devices are resource constrained and cannot process computationally intense algorithms. Encryption algorithms designed to work with resource constrained IoT devices are needed to provide strong cybersecurity.[169]
- **Alternative approaches to cryptography.** Approaches such as "friendly jamming" that can be used with existing resource constrained devices and do not require extra computing power should be studied.[170]
- **Hardware-based security solutions.** Adoption of pervasive hardware-based security solutions such as trusted execution environments, secure boot and secure storage would strengthen the security of IoT devices and prevent physical tampering and attacks.[171]
- **Blockchain.** Integration of adaptive and scalable blockchain technology would enable secure and transparent data sharing and management among IoT devices and stakeholders.[172]

While there are considerable industry efforts to address cybersecurity, the problem cannot be solved by industry alone. Achieving robust cybersecurity requires a long-term multi-stakeholder effort with active participation from buyers, manufacturers, consultants, academia and government. The federal government plays a key role in helping to minimize cybersecurity risks through a variety of actions. This role and representative actions are discussed in Section 8.3.1.2.

---

[168] Link

[169] "LSEA-IOMT: On the Implementation of Lightweight Symmetric Encryption Algorithm for Internet of Medical Things (IoMT)," S. Saif, P. Das and S. Biswas. Lecture Notes in Networks and Systems, vol 519. Springer, Singapore. Link

[170] "Securing Internet of Medical Things with Friendly-jamming schemes," X Li, H. Ning Dai, et al. Computer Communications, Vol 160, pp 431-442. July 1, 2020. Link

[171] See note 154

[172] See note 154

© Strategy of Things, 2025. All rights reserved.

6.1.3. Core: Privacy

The need to address privacy appeared as a gap in five of the nine industries. These industries include agriculture, insurance, retail, smart cities and healthcare.

Privacy concerns slow the realization of benefits offered by IoT by reducing user trust and willingness to participate. This hinders IoT adoption, limiting its use and slows integration and interconnection with other information technology and industrial operations technology systems.

In response to these concerns, IoT adopters and users may forgo purchase, purchase a smaller quantity, limit how the devices are used and limit the sharing of personal and proprietary data. Key privacy concerns hindering adoption revolve around the following:

- **Surveillance and monitoring.** IoT devices and systems may collect data without people's knowledge or consent. For example, Amazon's Alexa smart speakers recorded a private family conversation and sent that recording to someone.[173] Residential doorbell cameras capture video footage that, under certain conditions, may be accessed by police to support law enforcement activities.[174]
- **Discriminatory and unfair outcomes.** Data collected from IoT systems may be applied incorrectly or without controls and yield improper or incorrect outcomes. Facial recognition systems are one common IoT application used in a number of industries. A national drugstore chain, in a settlement with the Federal Trade Commission (FTC), was barred from using these systems for five years because "the system generated thousands of false-positive matches" and its "reckless use of facial surveillance systems left its customers facing humiliation and other harms and its (FTC) order violations put consumers' sensitive information at risk."[175]
- **Theft and disclosure of private and proprietary data.** IoT devices and systems collect, store and transmit sensitive personal or proprietary data, such as Personally Identifiable Information (PII), Personal Health Information (PHI), asset and people location tracking data and behavioral patterns. This data may be disclosed inadvertently such as the example of a well-known fitness app that published a map showing all the sports activity locations and routes of its users, including sensitive locations of military bases and spy outposts.[176]
- **Secondary use of data without user consent.** Private and proprietary IoT data may be collected with user approval for a specific purpose. Concerns arise, however, when that IoT data are repurposed by the IoT solution owner or shared with third parties for unrelated purposes without the user's knowledge or consent.

---

[173] "Woman says her Amazon device recorded private conversation, sent it out to random contact." G. Horcher, KIRO 7 News, May 25, 2018. Link

[174] "The privacy loophole in your doorbell," A. Ng, Politico, March 7, 2023. Link

[175] "Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards," Press Release, Federal Trade Commission, December 19, 2023. Link

[176] "Fitness tracking app Strava gives away location of secret U.S. army bases," A. Hern, The Guardian, January 28, 2018. Link

© Strategy of Things, 2025. All rights reserved.

- **Ownership of data collected from IoT devices and systems.** While the value of IoT is clear, the ownership of the data collected is less so. For example, a factory uses IoT to predict maintenance, optimize production and improve product quality. The sensors collect data on how the machines are used and their usage patterns. Ownership issues arise if the equipment manufacturer wants to sell the data to third parties or the solution vendor wants to create an offering based on the data to the factory's competitors. The ambiguity surrounding data ownership in this context raises critical questions about who has the right to control, access and monetize this valuable resource.

While there are various industry efforts to address privacy, the problem cannot be solved by industry alone. The federal government plays a key role in addressing privacy concerns through a variety of actions, including research. This role and representative actions are discussed in Section 24.

Our research identified the following IoT technology infrastructure opportunities that will partially address the privacy challenges. The three example technology areas of opportunity are listed below:

- Privacy by Design (PbD)
- Privacy enhancing technologies
- Context aware privacy

Each of these is discussed in the following sections.

6.1.3.1. Privacy by Design (PbD)

This system engineering approach to building privacy-compliant products and services embeds privacy considerations throughout the product development process instead of "bolting" it on afterwards. A detailed description of PbD is found in Section 16.3.1.2

Despite the value offered by PbD, there is no agreed-upon methodology to support the systematic engineering of privacy into systems.[177]

IoT devices integrate into complex environments with IoT, OT and IT systems. For example, future smart cities, farms and factories contain thousands of IoT devices of various types and capabilities that may communicate with each other. Designing privacy for the systems that IoT operate in is much more complex than designing privacy by design for individual products. Further research and development is required in understanding how privacy can be embedded into the underlying infrastructure and systems to create "Privacy by Design" infrastructures, platforms and systems at scale.

6.1.3.2. Privacy enhancing technologies.

Privacy Enhancing Technologies (PETs) are a "broad set of technologies that protect privacy by removing personal information, by minimizing or reducing personal data or by preventing

[177] "The challenges of privacy by design," S. Spiekermann, Communications of the ACM, July 1, 2012. Link

© Strategy of Things, 2025. All rights reserved.

undesirable processing of data, while maintaining the functionality of a system."[178] A detailed discussion of privacy enhancing technologies is found in Section 17.3.1.2.

The use of PETs in IoT is not widespread. PETs suffer from "the need for more research and development, limited technical expertise, perceived and possible risks, financial cost and the lack of generalizable solutions."[179] According to the 2023 National Strategy to Advance Privacy-Preserving Data Sharing and Analytics report, while cryptographic technologies have demonstrated initial success for real world adoption in simple applications, scalability and efficiency challenges must still be addressed in the context of a broader set of threats model."[180]

Furthermore, PET technologies lack consensus industry standards. The National Strategy to Advance Privacy-Preserving Data Sharing and Analytics report found that "there are no widely adopted standards for data formats, application programming interfaces or system architectures that are necessary to facilitate the interoperability and deployment of PPDSA technologies."

While some standards development is underway for homomorphic encryption and zero knowledge proofs, there is a need for "more standards that specify foundational cryptographic primitives and other Privacy Preserving Data Sharing and Analytics (PPDSA) technologies which facilitate adoption and trust in solutions."

6.1.3.3. Context aware privacy.

Context-aware privacy is an advanced systems approach to privacy that recognizes that different situations and conditions warrant various levels of data collection. Context-aware privacy considers the location, the environment and the specific situation and seamlessly adjusts how and what data are collected, processed and shared. A more detailed discussion of context-aware privacy can be found in Section 17.3.1.2.

Several broad research areas need to be addressed for the implementation of context-aware computing and privacy for smart cities and other domains. These include context definition, context-aware architectures, context sensing, context prediction based on limited to no data, context representation, context interpretation and adaptation, evaluation of context aware systems and privacy control. Other areas requiring additional research include notification and consent, context-aware privacy protection methods, algorithmic explainability, risk assessment of potential harms and user-centric tools, processes and interfaces.

6.1.4. Core: Connectivity

IoT technologies and other smart equipment require connectivity to send data to edge servers and remote data centers in the cloud for processing and storage. While connectivity challenges were directly identified in two of the nine industries studied, agriculture and manufacturing, the lack of connectivity availability in rural and underserved communities affects other industries

---

[178] "National Strategy to Advance Privacy-Preserving Data Sharing and Analytics," Fast-track action committee on advancing privacy-preservation data sharing and analytics, Networking and information technology research and development subcommittee, National Science and Technology Council Report, March 2023. Link

[179] "Advancing a Vision for Privacy-Enhancing Technologies," A.Macgillivray and T. deBlanc-Knowles, White House Office of Science and Technology Policy blog, June 28, 2022. Link

[180] See note 178

© Strategy of Things, 2025. All rights reserved.

operating in those areas. For example, a variety of healthcare, smart city, community and transportation and logistics IoT applications would not be available or be significantly limited.

Connectivity challenges that affect IoT operations come in a variety of forms, including a lack of supporting broadband infrastructure, poor signal coverage, interference from man-made and natural sources and lack of affordable service. These challenges vary for urban, rural and remote communities.

Connectivity challenges slow the realization of benefits offered by IoT use by limiting those who can connect, where they can connect and what applications can be supported. These factors hinder IoT adoption by limiting its use and outcomes and slowing integration and interconnection with other information technology and industrial systems. They also delay IoT's evolution where intelligence and hyperconnectivity combine at scale to bring economic and society-wide benefits.

Key connectivity concerns slowing adoption are discussed below:

- **No connectivity service to access.** Without connectivity, IoT cannot operate. The U.S. Federal Communications Commission (FCC) reported that as of December 2022, 45 million Americans lack access to both 100/20[181] Mbps fixed download and upload service and 35/3 Mbps mobile 5G-NR service.
- **Inability to support a full range of IoT applications.** IoT devices rely on the type and quality of the available connectivity. For a rural community lacking high speed broadband service, IoT applications are limited to those that are non-latency sensitive and require low bandwidth, such as air quality, soil moisture and equipment condition monitoring.
- **Inability to realize IoT application benefits.** Connectivity challenges reduce the reliability, functionality and outcomes of IoT applications. For example, an IoT application may work intermittently in an area with high interference, reduced coverage or unreliable service. This intermittency results in missed data collection and transmission, reducing the application's ability to perform consistently.
- **Inability to fully connect and automate.** Many IoT devices are integrated into operations systems and designed to improve efficiency by automating processes and systems. The inability to connect compromises the operations of these systems and prevents benefit realization.
- **Reduced trust in IoT.** Timeliness of data and the reliability and quality of the connectivity service are crucial in many IoT applications, especially in sectors like healthcare, industrial automation and public safety where quick decisions are needed. Without reliable and consistent connectivity, the reduced availability of data can lead to the use of outdated information in the decision-making processes.
- **Inability to scale.** Connectivity challenges slow the scaling of IoT deployments. Insufficient infrastructure and coverage limit what types of IoT applications can be

[181] On March 14, 2024, the FCC has updated its definition of broadband service from 25/3 to 100/20 Mbps. Source: "FCC increases broadband speed benchmark," FCC News Press Release, Federal Communications Commission, March 14, 2024. Link

© Strategy of Things, 2025. All rights reserved.

supported as well as limiting the number of supported IoT applications that can be deployed, connected and operated.

- **Increased security risks.** Connectivity issues can exacerbate security risks in IoT networks. Weak or intermittent connections may create vulnerabilities that malicious actors could exploit. Additionally, without a reliable connection it becomes difficult to implement over-the-air security updates and patches, leaving devices and networks more susceptible to cyber-attacks.

Achieving ubiquitous connectivity at the most appropriate service level is a long-term multi-stakeholder effort with active participation from connectivity service providers, technology developers and manufacturers, regulators, academia and government. The federal government plays a key role in facilitating connectivity through a variety of actions, from research, grants, spectrum management and policies. This role and representative actions are discussed in Section 24.

Research opportunities exist in improving performance of existing and niche connectivity methods, spectrum sharing and management, interference management, energy efficient connectivity approaches and Beyond 5G (6G) technologies. These efforts complement current industry efforts to deploy, operate and optimize services.

Our research identified the following IoT technology infrastructure gaps. While some of these were mentioned as gaps in specific industries such as agriculture or manufacturing, they are aggregated here and discussed in an industry-agnostic context. The three areas of gaps are:

- Broadband ubiquity
- “Last Acre” coverage
- Evolving connectivity capabilities with future needs

Each of these is discussed in the following sections.

6.1.4.1. Broadband ubiquity

The availability of broadband infrastructure is a prerequisite for enabling connectivity services. Without this infrastructure, the data collected by IoT devices and networks cannot be transmitted to the cloud data centers for storage and processing.

Multiple approaches are needed to enable ubiquitous broadband as there is no “one size fits all” approach. Existing approaches have strengths but also challenges. They include the following:

- Fiber infrastructure provides high capacity, but is expensive, takes decades to deploy and may not reach all areas.
- Service from wireless carriers and operators is best for high density areas but the lack of sufficient financial returns stops wireless operators from entering rural and tribal communities with low population densities.
- Geosynchronous satellite broadband service offers coverage over wide areas but suffer from latency and interference challenges.

© Strategy of Things, 2025. All rights reserved.

- Low Earth Orbit (LEO) broadband satellites offer low latency service but require high investments. Satellite operators face complexities in managing multi-satellite fleets.

In addition to these, there are alternative or niche approaches, such as TV White Spaces (TVWS) which utilize the unused UHF/VHF frequencies to carry Internet traffic and Power Line Communications (PLC) which carry broadband over power lines. These niche approaches may be appropriate in some cases for specific situations.

6.1.4.2. "Last Acre" coverage

In addition to the availability of broadband, wireless coverage in the actual areas where the IoT devices and systems are operating is critical. For example, IoT in agriculture requires that the sensors in the field, or the "last acre" be connected.[182] This is a major challenge as farms occupy vast stretches of land, with the largest farm in the United States spanning 190,000 acres.[183] Bringing broadband to the farmhouse doesn't address the need to connect the sensors in the field. Besides agriculture, other applications where "last acre" coverage is needed include environmental monitoring, forest monitoring and management, rural emergency services, remote infrastructure monitoring (electrical, oil pipelines, water infrastructure) and wildlife conservation.

Another area, although not land-based, is ocean transport and offshore oil rig operations. To address these issues for agriculture, the "Last Acre" bill was introduced in July 2023.[184] However, this bill does not address the needs of the other non-agriculture "last acre" applications.

Special "gap-filler" approaches, such as satellite-based services, TV White Spaces (TVWS) and Power Line Communications (PLC) may partially address some of these "last acre" challenges for specific applications. These include:

- **TV White Spaces.** TVWS utilizes the unused UHF/VHF frequencies to provide wireless internet service.[185] It suffers from a lack of standards-based products and limited or uneven performance based on terrain and interference susceptibility.[186]
- **Power line communications.** Power lines are used to carry Internet traffic and are increasingly used for smart grid communications. These are susceptible to radio frequency interference and performance is compromised by electrical noise and the overall quality of the power line infrastructure.[187]

---

[182] "Examining Current and Future Connectivity Demand for Precision Agriculture", Interim Report FCC, Precision Agriculture Connectivity Task Force, December 2022, Page 2. Link

[183] "Top 5 Farms with the Largest Acreage in the U.S.", E. O'Keefe, Successful Farming, September 28, 2019. Link

[184] "Last Acre Act", Fact Sheet, Senators Deb Fischer (R-Nebraska) and Ben Ray (D-New Mexico). Link

[185] "What is TV White Space?" Everything RF. Link

[186] "TV White Space: a work in progress," Broadband Center of Excellence, University of New Hampshire. Link

[187] "Broadband over Power Line," DevX, October 11, 2023. Link

© Strategy of Things, 2025. All rights reserved.

- **Satellite IoT.** Coverage to the "last acre" is provided by satellites in space. A number of complex technological challenges must be addressed to "fully unleash the potential of satellite IoT."[188]

6.1.4.3. Evolving connectivity capabilities to support future needs

As IoT evolves, as described in Section 22.1, the capabilities of the connectivity services must evolve to accommodate future applications. Today's communication networks and architectures are not designed to manage the diverse needs of IoT at scale. The network must support heterogeneous devices of all types, brands and models and variations of those models. The traffic from these IoT devices ranges from small bits of data on a periodic basis to continuous streams of high bandwidth video traffic.

To support future IoT needs, researchers need to address a number of connectivity considerations. These include service bandwidth, spectrum allocation, connectivity technologies, energy efficiency, interference and sixth generation (6G). Each of these is discussed below.

- **Service bandwith.** Future IoT applications will increasingly involve autonomy, robotics, computer vision and large amounts of sensor data. These applications require a stable and continuous connection, higher bandwidth, low latency and symmetric upload and download speeds. The level of service bandwidth will require new infrastructure and augmentation of existing infrastructure.
- **Spectrum allocation.** As IoT adoption grows, so does the need for spectrum. A 2017 U.S. Government Accountability Office report stated that "rapid increases in IoT devices that use large amounts of spectrum, called high-bandwidth devices, could quickly overwhelm networks, as happened with smart phones."[189]
- **Connectivity technologies.** Future connectivity technologies must support billions of connected devices. A survey of current IoT connectivity technologies identified some technical shortcomings that compromise this ability, including high signaling overhead, wireless resource scarcity and inefficient wireless resource usage.[190] Research to develop new technologies that can address the existing shortcomings is important to enable deployment of IoT at scale.

[188] "A survey on technologies, standards and open challenges in satellite IoT," M. Centenaro, C. Costa, et al., IEEE Communications Surveys & Tutorials PP(99):1-1, May 2021. Link

[189] "Internet of Things: FCC Should Track Growth to Ensure Sufficient Spectrum Remains Available," Report to Congressional Requesters GAO 18-71, U.S. Government Accountability Office, November 2017. Link

[190] "IoT Connectivity Technologies and Applications: A Survey," J. Ding, M. Nemati, C. Ranaweera and J. Choi., arXiv:2002.12646, IEEE Access (Volume: 8) 2020, February 28, 2020. Link

© Strategy of Things, 2025. All rights reserved.

- **Energy efficiency.** A study of IoT wireless communication technologies identified energy-efficiency as a challenge. [191] [192] Reducing energy consumption reduces grid demand and extends the useful life of those IoT devices that use non-rechargeable batteries. Research into future connectivity technologies that support energy-efficient communications would help address this challenge.
- **Interference.** As the number of devices grows, concerns about interference increase, especially for low bandwidth IoT devices that communicate in unlicensed bands such as LoRaWAN. While the FCC will consider adding additional spectrum to alleviate congestion issues, research is needed to alleviate communications interference within existing frequency bands including spectrum sharing techniques and interference aware power control.[193]
- **Sixth Generation (6G).** 6G is in the early stages of standards development with the first release of specifications expected in 2028 and commercial launch expected by 2030.[194] 6G offers transformational capabilities for IoT, including terabit speeds, 1 millisecond latency, ubiquitous coverage due to its integration with satellites, AI integration and energy efficiency.[195] Research into advancing 6G technologies is critical to maintaining U.S. competitiveness and leadership.

6.2. Intelligence gaps

One of the core capabilities of IoT systems and devices is to sense, collect and analyze data of the physical environment to allow users to make informed decisions and take relevant actions. However, the intelligence capabilities of these systems and devices varies. Some systems, such as air quality sensors and vibration sensors collect and route data to cloud-based servers in remote data centers for processing and analysis. Other systems, such as autonomous vehicles where low latency processing is a requirement, process and analyze data on the system itself so that it can take action immediately.

In the second stage of IoT evolution as discussed in Section 4.2.1, the system's intelligence capabilities evolve from analyzing data to support human decision-making to analyzing data and taking action in real-time without human involvement. Enabling and supporting the intelligence capabilities of IoT requires a multitude of technologies, from low latency connectivity methods,

---

[191] "Wireless Communication Technologies for IoT in 5G: Vision, Applications and Challenges," Q. Khanh, N. Hoai, et al. Cyber-Physical Mobile Computing, Communications and Sensing for Industrial Internet of Things and Industry 4.0 2021. February 7, 2022. Link

[192] "Energy Efficiency in Short and Wide-Area IoT Technologies—A Survey," E. Zanaj, G. Caso, et al., March 19, 2021, Technologies 2021, 9(1), 22. Link

[193] "Interference-Aware Power Control for Spectrum Sharing Massive-IoT Communications," A. Anzaldo and A. Andrade. In: Bravo, J., Ochoa, S., Favela, J. (eds) Proceedings of the International Conference on Ubiquitous Computing & Ambient Intelligence (UCAmI 2022). UCAmI 2022. Lecture Notes in Networks and Systems, vol 594. Springer, Cham. Link

[194] "3GPP commits to develop 6G specifications," J.P. Tomás, RCR Wireless, December 6, 2023. Link

[195] "What is 6G? Everything you need to know," S. McCaskill, TechRadar, December 20, 2020. Link

© Strategy of Things, 2025. All rights reserved.

AI and machine learning algorithms, data management, to microprocessors capable of running the algorithms.

Our research identified intelligence-related gaps across several industries. For example, artificial intelligence (AI) explainability was identified as a challenge in insurance, retail, transportation and logistics and healthcare. Data management, which supports and facilitates the intelligence capabilities of IoT, was identified in the renewable energy and transportation and logistics industries.

Based on our research, a number of technology infrastructure gaps related to intelligence in IoT were identified. These gaps fall across a number of broad areas, including:

- Data management challenges
- Challenges that affect trusting AI
- Challenges involving intelligent device capabilities

Each of these is discussed below.

6.2.1. Intelligence: Data management

Managing the volumes of data collected from IoT devices and systems is a major challenge. As IoT scales, so does data management complexity.

The IoT data collected comes in a variety of types, formats and sizes. It resides and operates in a distributed environment, with data processed on the device, in moving vehicles, and on edge servers and in remote servers in the cloud. Some data are time-sensitive and must be processed immediately while others are stored for future actions. Data may be required to comply with industrial, state and national regulations.

Robust data management capabilities simplify these challenges and help unlock the value of IoT by enabling massive amounts of data to be collected, processed, stored, discovered, queried and analyzed. Without these capabilities, IoT deployments face challenges such as data silos, scalability issues and compromised data integrity. In some industries, including healthcare, robust data management is required to comply with strict data privacy regulations.

In addition, robust data management and governance are foundational for artificial intelligence powered IoT systems.[196] Robust data management ensures the availability, accessibility, quality and security of data, laying a foundation for AI applications to generate effective decisions and relevant outcomes. Moreover, well-managed data facilitates the development of more accurate and reliable AI models, leading to better predictions, better recommendations and automation of various operations.

The lack of data management capabilities slows the adoption, operation and value realization of IoT and AI-enabled IoT. For example:

- **Inability to harness data to unlock and maximize value.** IoT devices collect vast amounts of data in various formats. Without effective data management capabilities,

[196] "Data management and governance key to successful AI use," S. Catanzano, TechTarget, February 13, 2024. Link

© Strategy of Things, 2025. All rights reserved.

organizations struggle to process, store, analyze and derive actionable insights from this flood of data.

- **Inability to scale IoT.** As deployments scale up, so will the number and variety of heterogeneous devices. The data collected from these devices may be stored and processed on the device itself, on mobile devices, or in the cloud. The lack of standardized data formats, interfaces and APIs complicates data exchange and integration efforts.
- **Increased security and privacy risks.** IoT devices and systems collect a variety of data, from equipment condition to images of people. Without proper encryption, access controls and data governance policies in place, sensitive information collected by IoT devices may be susceptible to exploitation by malicious actors, leading to reputational damage, regulatory and legal liabilities.
- **Increased compliance and regulatory risks.** In regulated industries such as healthcare, finance and utilities, organizations must comply with stringent data protection regulations and industry standards. Without proper data governance, organizations may struggle to demonstrate compliance with data privacy laws such as GDPR, HIPAA, or PCI-DSS, undermining trust and credibility among customers, partners and regulators.
- **Increased operational inefficiencies and costs.** IoT data management is complex and challenging. Poor data management increases operational costs. Organizations may invest in unnecessary storage, struggle with data integration and face compliance challenges.

Furthermore, the convergence of AI with IoT and the likely pervasiveness in the economy creates a need to accelerate the development of "beyond big data" data management approaches and technologies.

Given the strategic importance of data management to IoT in enabling powerful AI models and AI-enabled IoT systems, potential opportunities for the federal government to augment and accelerate industry efforts may include the following areas:

- **Scalable and efficient data storage.** Innovative and more effective approaches, including ways to improve storage efficiency, are needed to manage the increasing volume of data.
- **Real-time data processing.** Research into ways to enhance real-time and energy efficient processing of IoT-generated streaming data, including advanced algorithms, edge computing and in-memory processing techniques is relevant.
- **Security and privacy.** Research into methods and approaches to protect a diverse set of data that is increasingly stored on distributed devices, mobile and edge systems, as well as data that are streamed to other systems is important.
- **Data quality assurance methodologies.** Research into approaches to ensure the accuracy and reliability of IoT-generated data, such as developing calibration techniques for sensors, anomaly detection algorithms and data validation processes is necessary.
- **Data governance.** New approaches and mechanisms for data oversight and management are needed as separate parties own their own data and it is increasingly distributed and decentralized.

© Strategy of Things, 2025. All rights reserved.

- **Lifecycle management of IoT data.** As new IoT applications emerge and industry adoption increases, the management of the distributed and decentralized data, from attribution, traceability, collection, storage, processing, analysis and archiving becomes more important.
- **Data fabric architectures.** As data sources and creators are increasingly decentralized and distributed on a massive scale, future scalable architectures to interconnect and access this data are required.

6.2.2. Intelligence: AI Trust

The use of AI in combination with IoT devices and systems enables users to extract insights from volumes of data. Furthermore, AI models running on IoT devices analyze data streams in real-time, identify patterns, predict outcomes, make intelligent decisions and may take autonomous action without human supervision. AI-driven analytics enable continuous learning and adaptation, allowing IoT systems to evolve and improve over time, leading to more accurate predictions and better resource utilization.

Despite its transformational potential, artificial intelligence faces several challenges that slow its broader adoption and scaling. Our research identified the lack of use of artificial intelligence as a gap in insurance, retail, healthcare and transportation and logistics sectors. AI is also an important capability in agriculture, smart cities and renewable energy.

AI trustworthiness is a common concern identified in our research. The outcomes produced may not be explainable, nor fair or ethical, leading to a lack of trust. Some AI models employ "black box" approaches, such as deep learning, that "produce decisions and outcomes that are not easily explained as compared to their less powerful and accurate "white box" counterparts such as linear and decision tree methods."[197]

The results and outcomes from the AI algorithms may not be easily explainable based on the underlying decision-making or inference patterns. The models may not always be peer reviewed nor shared with others because of intellectual property concerns. The inability to explain outcomes in healthcare, for example, makes it difficult for physicians, regulators and others to determine whether a model is safe, usable and supports efficacious outcomes.

Another cause of poor algorithm predictive performance is the inability to collect a representative set or enough of the right data, leading to data bias. The biased data may be used to train AI models, which in turn leads to inaccurate or improper outcomes when AI models analyze data outside the range of their training set.

In the transportation and logistics industry, our research reported that the "reluctance of the various industry participants to share data creates incomplete data sets used to train the AI models, resulting in algorithmic bias."[198]

AI trust challenges hinder future functionality and usefulness, adoption, scaling, value realization and delivery in a number of ways:

---

[197] As discussed in Healthcare in Section 19.3.1.3

[198] As discussed in Transportation and Logistics Section 18.3.1.3

© Strategy of Things, 2025. All rights reserved.

- **Poor and limited functionality.** Intelligent IoT systems monitor the cyber-physical environment to create insights and support automated and human-led actions. A system's inability to process, analyze or interpret the data properly or in a timely manner leads to poorly informed conclusions and decisions, incorrect or inappropriate actions and poor and inconsistent results.
- **Create poor outcomes that erode user trust.** AI challenges can erode user trust in IoT devices and services. For example, when AI algorithms in facial recognition camera systems fail to accurately interpret data, it leads to incorrect actions or recommendations and diminishes user confidence.
- **Create unsafe actions and conditions.** The complexity of IoT environments often necessitates AI models that can adapt to dynamic conditions with a myriad of responses and actions. They may, however, exhibit unexpected or unintended behavior if they encounter scenarios not covered during training.
- **Hinder automation and limit the value provided to users.** Technology challenges that slow the use of intelligence in IoT systems limit its ability to monitor and process large volumes of data, analyze and make informed decisions and automate and control processes.
- **Hinder the future development of "smarter" IoT.** For IoT to support growth and autonomous operations and applications, its intelligent capabilities must continue to develop. Future applications, such as IoT device swarms, which are clusters of more than 100 IoT devices that operate collectively as one to perform certain tasks, but with each device operating individually, require autonomous operating capabilities.

AI trust challenges are complex and involve multidisciplinary factors. These challenges, however, must be addressed before AI can be adopted in a broader way with IoT. At an aggregate level, our research identified some representative AI opportunities for the federal government to facilitate its scaling and usage in IoT. These include:

- **Development of ethical AI algorithms.** The convergence of AI with IoT enables fully autonomous operations, rapid responses to complex incidents without human intervention and augmentation of humans in high skilled operations. The use of AI in IoT, however, raises questions of fairness, privacy, ethics, maleficence, accountability and transparency. The use of AI based facial recognition camera systems may lead to improper conclusions and actions against certain demographic groups. AI algorithms used in systems for autonomous vehicles can potentially take a different set of actions based on the country where it was trained. Creating ethical AI algorithms is complex and involves multiple technical and non-technical disciplines.
- **Explainable AI tools and processes.** For AI controlled operations to be trusted and adopted at scale, its users must be able to understand and assess the AI algorithm's decision-making processes, its alignment and precision to target outcomes under a variety of planned and unplanned conditions and its consistency in creating and acting on the outcomes. Explainable AI is defined as the "set of processes and methods that allows human users to comprehend and trust the results and output created by machine learning

© Strategy of Things, 2025. All rights reserved.

algorithms."[199] Continued research in the design, development and deployment of innovative tools and operations is needed to overcome some of the challenges facing explainable AI, including evaluation metrics, scalability, model suitability, interpretability and explanation communications.[200]

6.2.3. Intelligence: Intelligent device capabilities

On-device and edge processing of data is increasingly common and are needed for applications that are autonomous, latency sensitive or operate in an area with unreliable service. Other edge applications include IoT device swarms and ambient IoT use cases that require contextual information from other nearby devices.

Our research has identified intelligent device capabilities to support intelligent IoT as a top challenge in both agriculture and smart cities. Edge computing remains, however, a critical enabler in industries where AI-enabled applications are used. This includes healthcare, transportation and logistics and renewable energy.

Challenges in intelligent devices that slow adoption, scaling and value realization include:

- **Inability to perform complex tasks and operations:** IoT devices are resource-constrained and lack the computational, storage and power capacity to perform complex tasks and applications.
- **Increased complexity and costs:** Technical challenges in IoT edge computing significantly increase both the complexity and costs associated with IoT deployments and maintenance.
- **Increased security risks:** Edge devices often lack robust security measures such as encryption and advanced firewalls due to resource limitations, making them vulnerable to attacks such as malware infiltration or data breaches.
- **Increased energy consumption:** As IoT devices and edge servers are deployed in increasing numbers, particularly those systems that run complex applications and cannot be powered by batteries, the amount and cost of electricity to power these systems increases.

While there are existing industry development efforts and solutions for the development of intelligent devices, these efforts are focused on short term objectives. To enable and support a future scaled up, hyperconnected and autonomous IoT ecosystem, the federal government would do well to focus on research and commercialization of innovative IoT technologies. A representative set of innovation areas is listed below:

- **Increase device processing capabilities.** As more IoT applications shift to the edge, the complexity and intensity of the workloads processed is expected to increase. For

[199] "What is Explainable AI?", V. Turri, Software Engineering Institute, Carnegie Mellon University, January 17, 2022. Link

[200] "Explainable AI (XAI): A Systematic Meta-Survey of Current Challenges and Future Opportunities", W. Saeed and C. Omlin, November 11, 2021. Link

© Strategy of Things, 2025. All rights reserved.

example, IoT applications that need real time sensor fusion or AI enabled systems require substantial edge processing abilities. Processor development for edge applications, regardless of whether that processing occurs on the devices or on servers, must continue to increase their ability to support complex and process intensive workloads.[201]

Neuromorphic processing, inspired by the brain's architecture, offers significant research and innovation opportunities for IoT.[202] By mimicking neural networks, neuromorphic chips can process data more efficiently and with lower power consumption compared to traditional processors. One area of opportunity for neuromorphic processing is for industrial radar applications.[203] This advancement is particularly beneficial for IoT devices, which often operate under power constraints and require real-time data processing at the edge.

- **Reduce power consumption of microprocessors.** Smarter IoT devices incorporate more capable microprocessors and microcontrollers. More capable processors, however, consume more power. In many cases, the power supplied for these IoT devices is from batteries. Low power AI capable processors that can operate on battery operated devices[204] must be developed to support both current and future needs.
- **Develop energy harvesting technologies.** Battery powered IoT devices have a limited lifetime. With billions of IoT devices to be deployed, replacing those batteries is neither realistic nor practical. Energy harvesting technologies can augment or replace batteries in IoT devices.[205] While today's energy harvesting technologies are limited to augmenting battery life in select IoT applications, developments can yield solutions that remove the need for batteries.
- **Development of AI algorithms capable of running on resource constrained IoT devices.** Research in the development of algorithms that can operate on resource constrained devices is critical to the creation of new applications and scaling of IoT.

  Research into the development of more computationally efficient algorithms also benefits edge and cloud data centers. The energy consumed by high power processors and servers running computationally intensive AI models is significant. The development of more efficient algorithms that run on these servers provides opportunities for energy and cost savings. As the adoption and deployment of AI-enabled IoT systems increase, the energy savings are likely to become significant.

---

[201] "Intel Thinks IoT Devices Are Going to Get a Lot More Powerful", A. Braun, IoT Tech Trends, April 10, 2019. Link

[202] "Neuromorphic computing: The future of IoT," H. Joshi, Financial Express, March 3, 2024. Link

[203] "NeuroRadar: A Neuromorphic Radar Sensor for Low-Power IoT Systems," K. Zheng, K. Qian, et. al. SenSys '23: Proceedings of the 21st ACM Conference on Embedded Networked Sensor Systems. Pages 223 – 236. Link

[204] "Designing Ultra Low Power AI Processors", A. Mutschler, Semiconductor Engineering, April 9, 2020. Link

[205] "Energy Harvesting Starting to Gain Traction", J. Koon, Semiconductor Engineering, April 18, 2022. Link

© Strategy of Things, 2025. All rights reserved.

6.3. Hyper-Deployed gaps

An IoT-enabled economy and society, teeming with billions of interconnected devices working autonomously and collaboratively across industries and communities, is a vision enabled by the evolution of the Internet of Things described in Section 4.2.1.

The current IoT technology infrastructure, however, is not ready to support such a massive, complex ecosystem. For example, existing networks are already challenged to detect, manage and mitigate security threats, but to do so effectively in a future network infrastructure with billions of new devices requires a new paradigm of an adaptive, autonomous self-defending, self-healing network. Similarly, the AI-enabled decisions and outcomes created by IoT devices today experience issues with accuracy, explainability and trust. These issues must be fully resolved in a future economy and society reliant on autonomous and connected devices and systems.

The envisioned future "hyper-deployed IoT" economy and society require a technology infrastructure much different than the one we have today. This infrastructure must support billions of heterogeneous connected IoT devices and systems reliably and predictably. It must allow for the seamless exchange of data and information and do so such that it can be made available and acted upon in a timely manner. It must support an economy where intelligent autonomous systems and human AI collaboration are the norm. It must protect against a variety of known and yet to be discovered future cybersecurity threats and autonomously contain and mitigate the impact of these threats. The algorithms used to analyze and act on the collected data must do so in a way that is accurate, fair and explainable.

Our inability to develop and deploy the technologies enabling this future infrastructure hinders the IoT functionality and usefulness, adoption, scaling, value realization and delivery in a number of ways:

- **Slows IoT evolution.** Continuing technology advancements are necessary for IoT to evolve in response to future needs. Existing technologies may be based on legacy approaches that are technologically obsolete, designed for a different set of requirements and capabilities and cannot extend to support future needs, or nearing end of life.
- **Limits the number of devices connected and what they can do.** The IoT ecosystem is comprised of heterogeneous devices and systems that impose unique requirements and complex needs on the supporting technology infrastructure. These systems have varying bandwidth requirements, some have specific latency requirements while other applications require high processing loads. The inability of the infrastructure to support this variety of conflicting requirements prevents users from adopting and integrating IoT devices and systems.
- **Hinders the economy-wide and society-wide realization of benefits.** IoT-enabled systems, such as smart cities and supply chains, require "network effects" (i.e., scale of users) to create value. The more users, the more systems that are connected and the more data generated, leads to more value. Future generation IoT technology infrastructure is necessary to support the deployment and operation of billions of IoT devices across the economy and society.

© Strategy of Things, 2025. All rights reserved.

Substantial investments in research and development are needed to enable the advancements required for an infrastructure capable of supporting these billions of devices. While industry participants conduct a variety of research and development efforts on key technologies, they are not well suited to bring about these advancements in future generation infrastructure. Much of the industry's efforts are focused on extending their current technology investments and intellectual property portfolios. These efforts are focused on driving incremental advancements to meet existing market needs, extending the functionality and capability of existing investments with short term return on investment potential.

Because of this, the federal government plays a significant role in developing and supporting research and facilitating the advancements that will lead to the future IoT technology infrastructure needed. Some of this research is fundamental in nature and explores uncharted topics beyond the immediate commercial interests of industry. Other research may be high risk and involve novel approaches that demand substantial financial backing, a long-term perspective and have an uncertain outcome.

To support the continued evolution, scaling and full realization of the value created by IoT described in the evolution framework (Figure 4-7), this report has identified several critical technology areas for further research and innovation.

6.3.1. Hyper-Deployed: Enabling an IoT data ecosystem

One of the foundations of the future digital economy and society is the massive volumes of data generated by billions of smart devices and IoT-enabled systems. These data are distributed and decentralized as it is produced, consumed, stored and managed on fixed and mobile devices and on edge devices as well as on servers and cloud data centers.

The data are owned, used and managed by a variety of parties, including individuals, business organizations, cities and communities along with government agencies. These data may be proprietary or public and may be used exclusively by the data owner or may be monetized and shared with others to realize benefits and outcomes.

The future IoT data ecosystem is envisioned to be a highly interconnected network where data generated by IoT devices and systems is seamlessly shared, monetized and utilized across various sectors. An IoT data ecosystem is needed to support this digital economy and society. One of the key features of this ecosystem is its decentralized nature, allowing data to be processed and analyzed closer to where it is generated, thus reducing latency and improving efficiency.

The European Union’s (EU) European Data Strategy aims to create a robust data ecosystem by establishing a single market for data, ensuring that data flows freely and securely across sectors and member states.[206] This strategy offers valuable insights into how the United States can approach the creation of its own IoT data ecosystem.

The strategy is based on creating common data spaces, which share common data infrastructures and governance frameworks to facilitate data pooling, access and sharing. These data spaces make more data available for economic and societal use while keeping control in the hands of the

[206] “European Data Strategy,” European Commission. Link

© Strategy of Things, 2025. All rights reserved.

data generators. Initial data spaces include agriculture, energy, health, manufacturing, mobility (transportation) and nine other economic areas.[207]

In the United States, efforts like the National Institute of Standards and Technology's (NIST) Smart Grid Interoperability Framework show the way for a more integrated IoT data ecosystem for energy areas.[208] This framework focuses on ensuring interoperability and security in the smart grid. By establishing standards and guidelines, NIST aims to create a cohesive environment where data from various sources can be integrated and utilized.

There are, however, a number of technical challenges to building such an IoT data ecosystem. One of the primary challenges is ensuring data quality and interoperability. With data being generated by a multitude of devices and systems, maintaining consistent data quality and ensuring that different data sources can seamlessly interact with each other is crucial. Additionally, data privacy and security concerns must be addressed, as the sharing and monetization of data can expose sensitive information to risks.

Data sovereignty is an important challenge that ensures that the information produced within the country is retained by its owners and protected from external threats while fostering domestic innovation. In addition, the volume of data generated by IoT devices poses scalability issues. Efficiently storing, processing and analyzing these data require significant computational resources and innovative solutions.

The lack of universally accepted standards for IoT data management and integration slows the development of a cohesive ecosystem and additional research is needed to address these data ecosystem challenges.

6.3.2. Hyper-Deployed: Communications and network infrastructure

Research firm IDC estimated that by 2025, there will be 55.9 billion IoT devices generating 79.4 zettabytes (ZB) of data.[209] The traffic from these IoT devices ranges from small bits of data on a periodic basis to continuous streams of high bandwidth video traffic. The network must be able to support devices of all types, brands and models and variations of those models. Current communication networks and architectures are not designed to manage the needs of IoT at scale.

Some IoT data are time sensitive and must be acted upon immediately, while other data are stored for future analysis. Some data that support critical applications, such as public safety require a reliable communication network.

To support time-sensitive and critical applications, some data are processed in servers integrated into the network near the point of use (edge) and in vehicles (mobile edge), while other data are sent to remote data centers (cloud).

New processes and technologies for configuring, managing, operating and maintaining the hyperconnected network will be necessary. For example, automation will evolve to autonomous

---

[207] "Common European Data Spaces," European Commission, updated July 3, 2024. Link

[208] "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0", A. Gopstein, C. Nguyen, et al., U.S. National Institute of Standards and Technology, July 2020. Link

[209] "How You Contribute to Today's Growing DataSphere and Its Enterprise Impact," D. Reinsel, IDC Blog, November 4, 2019. Link

© Strategy of Things, 2025. All rights reserved.

maintenance and operations with the use of AI technologies that support network operations.[210] Continuous innovation is required to address communications network scaling and operation challenges. Some representative areas for innovation include:

- Spectrum sharing and management
- Network infrastructure to support AI and complex IoT applications
- Fault tolerant and resilient network infrastructure
- Self-defending adaptive network security
- Management of the distributed IoT network at scale
- Optimizing and maintaining performance and Quality of Service under continuously varying conditions
- Improving middleware to support scaling

Each of these is discussed below.

6.3.2.1. Spectrum sharing and management.

There is a finite amount of wireless spectrum available for IoT applications. In dense urban environments, this can become problematic as the number of IoT devices scales up and data traffic volumes grow, leading to network congestion and radio frequency interference. New ways of spectrum sharing and management are needed.

Spectrum sharing techniques, such as that implemented in the Citizens Band Radio Service (CBRS) for the narrow band within the 3.5 GHz band, is one approach that facilitates the shared use of the spectrum. Another technique is cognitive radio, an approach that enables IoT devices to sense the spectrum usage of surrounding users, determine what unused spectrum exists and connect and communicate through the available spectrum.

6.3.2.2. Network infrastructure to support AI and complex IoT applications

A 2021 survey of 211 data scientists, AI/ML practitioners and systems architects revealed that 42% of respondents reported challenges with their companies' AI infrastructure and compute capacity.[211] This is not surprising as AI and autonomous IoT applications impose high performance requirements for communications networks. These requirements include:

- **High throughput, low latency.**[212] AI models analyze large amounts of data sourced from sensors and devices. For example, algorithms trained and deployed for use ("inference

[210] "How AI is Changing the Role of Network Managers and Teams", J. Edwards, Network Computing, July 15, 2021. Link

[211] "Run:AI State of AI Infrastructure Survey 2021," Run:AI blog, Run:AI, October 26, 2021. Link

[212] "High-Performance Networking to Support Critical Workloads for AI and ML", M. Pierce, Redapt blog, July 16, 2020. Link

© Strategy of Things, 2025. All rights reserved.

models") stream and process the data from a variety of sensors, often in real time, for immediate action.

- **Distributed computing resources.** Depending on the application, processing for AI applications is performed in cloud data centers, near the point of data collection (edge) or on the device. In other cases, AI models may be distributed to multiple nodes over the network for processing. These nodes may collaborate with each other to add processing resources and to improve model accuracy.[213]
- **Scalability of resources.** Compared to traditional IT workloads processing static and structured data, AI workloads process "free flowing" data that can be structured and unstructured and that are computationally intensive and dynamic in nature.[214] The dynamic nature of the AI workloads requires the scaling of compute resources from the existing node or from nearby nodes.
- **High performance computing.** Complex AI workloads require parallel processing of multiple tasks on multiple servers. These servers are often networked together to form High Performance Computing (HPC) clusters, containing 100,000 servers or more. HPCs require specialized hardware capable of high bandwidth, low latency operations for networking, memory, storage and file systems.[215]

AI and autonomous IoT applications impose challenges on the communications network infrastructure. Further research and innovation are necessary to develop the network to meet these needs. Example areas of needed continued research include network interconnect architectures to support scalability and high bandwidth needs,[216] computation offloading to edge and mobile edge to address resource and latency needs,[217] transport designs for distributed AI training,[218] and AI workload and network joint optimization for resource allocation.

6.3.2.3. Fault tolerant and resilient network infrastructure

The ability of the network infrastructure to tolerate faults and remain functional and resilient is critical to the operation of IoT applications that are expected to last for years. As additional IoT devices with varying levels of quality and performance levels are integrated into the network, they introduce operating conditions and faults that could disrupt operations. These conditions and faults affect the operations that the IoT application is managing and could potentially spread to other processes through a chain of cascading failures.

---

[213] "What is Distributed AI?", W. Chong et al, IBM, December 8, 2021. Link

[214] "How AI Will Change Network Infrastructure," A. Cole, Enterprise Networking Planet, October 25, 2018. Link

[215] "What is High Performance Computing (HPC)?", IBM. Link

[216] "Interconnection Networks", ScienceDirect. Link

[217] "Computation Offloading", ScienceDirect. Link

[218] "Meta Launches New Research Award Opportunity in Networking for AI at NSDI 2022", Meta Research, April 5, 2022. Link

© Strategy of Things, 2025. All rights reserved.

The resilient network must be able to defend, detect, remediate and recover from faults. It must also be able to further diagnose and refine its responses to fault conditions.[219] Systems resilience, a key capability of sustainable IoT networks, is accomplished through a combination of design and functional redundancy, fault tolerance and operational adaptation. For example, some devices contain software written in "safe" programming languages[220] and developed using rigorous software development methodologies, while others may not be as conscientiously developed.

The need for reliability and stability requires the communications networks to support heterogeneity in both the device quality and the network configurations, be adaptive to the actual state of resources on the device, support the specific device reliability requirement and the current state of the operating physical environment for the device.

Key areas of research are needed to develop and refine the methodologies, algorithms and tools to detect and recover from the various failure mechanisms, such as correlated failures, unpredictable failures, debugging failures and human caused errors.[221]

Other areas of research include understanding and integrating the role of context or situational awareness in detecting and diagnosing faults, the role of people in the specification and design of resilient systems and the use of network function virtualization in resilient systems.[222] Finally, the integration of autonomic network management (self-configuration, self-healing, self-optimization, self-protection) with software defined networking (SDN), is another area for further innovation and development.[223] As IoT networks continue to grow in size and become more complex, continued research into the development of existing and innovative approaches, including those that employ software service-oriented architecture (SOA)[224] and AI[225] is necessary to ensure future systems resilience.

---

[219] "Architecture and Design for Resilient Networked Systems," D. Hutchison and James P.G. Sterbenz, Computer Communications, Volume 131, 2018, Pages 13-21, ISSN 0140-3664. Link

[220] "Memory Safe Programming Languages Are on the Rise. Here's How Developers Should Respond", l. tung, ZDNET, January 25, 2023. Link

[221] "New Frontiers in IoT: Networking, Systems, Reliability and Security Challenges", S. Bagchi et al, DOI 10.1109/JIOT.2020.3007690, IEEE Internet of Things Journal. Link

[222] "Architecture and Design for Resilient Networked Systems," D. Hutchison and James P.G. Sterbenz, Computer Communications, Volume 131, 2018, Pages 13-21, ISSN 0140-3664. Link

[223] "Self-healing and SDN: Bridging the gap", L. Ochoa-Aday et al, Digital Communications and Networks, Volume 6, Issue 3, 2020, Pages 354-368, ISSN 2352-8648. Link

[224] Zhou, S. (2015). Supporting Fault Tolerance in the Internet of Things. UC Irvine. ProQuest ID: Zhou_uci_0030D_13722. Merritt ID: ark:/13030/m5cc5mzg. Link

[225] "Design and Implementation of Fault Tolerance Technique for Internet of Things (IoT)," 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), 2020, pp. 154-159, doi: 10.1109/CICN49253.2020.9242553, S. Kumar, P. Ranjan, P. Singh and M. R. Tripathy. Link

© Strategy of Things, 2025. All rights reserved.

6.3.2.4. Self-defending adaptive network security

IoT devices introduce new attack surfaces that can be exploited to breach the network. This is exacerbated by the rise of AI facilitated cyberattacks.[226] The ability to detect, mitigate and recover from an exponentially growing number of cyberattacks using existing approaches and tools is untenable. New innovative approaches and solutions are needed.

One such potential innovative approach is self-defending adaptive networks. A self-defending and adaptive network "defends itself from security breaches. It is a system that knows and recognizes the level of threat faced by an intrusion across a network. It uses a new method of machine learning to track threats, which can include ransomware, code hijackers, intrusion and illegal entry, theft and unauthorized use. Such a network uses a set of modules that can be added or removed to operate and achieve specified goals. It can change its behavior by modifying network devices."[227]

To be successful, self-defending and adaptive networks must "be effective in an unstructured, unstable, rapidly changing, chaotic, adversarial environments; able to learn in real-time and under extreme time constraints, using only a few observations that are potentially erroneous, of uncertain accuracy and meaning, or even intentionally misleading and deceptive." [228] Continued areas of research and innovation are needed in three enabling areas:

- Software control enables adaptive operations, including the creation and deployment of network services.
- Programmable infrastructure combines software, cloud native virtual network functions with the physical hardware to respond to changing needs.
- Algorithms process the data streams and provide the necessary analysis and insights which is used by the software and programmable infrastructure to take the appropriate actions.[229]

6.3.2.5. Management of the distributed IoT network at scale

With billions of devices, routers and servers of all types soon operating in a multi-layer architectural environment, the network operator and data center's ability to monitor, manage, operate and support this infrastructure over its life cycle is a complex undertaking.[230] In addition to the hardware, managing the software that the hardware operates is equally complex. While automation of the management tasks is a necessity, the scale of massive IoT networks and

---

[226] "FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence," Federal Bureau of Investigation, May 8, 2024. Link

[227] "What are Self-Aware and Self-Defending Adaptive Networks?", B. Kommadi, Open Source for U, November 3, 2021. Link

[228] "Intelligent Autonomous Agents are Key to Cyber Defense of the Future Army Networks," A. Kott, U.S. Army Research Laboratory, pre-print version of the article appearing in the the Cyber Defense Review journal, Fall 2018. Link

[229] "What are Self-Aware and Self-Defending Adaptive Networks?", B. Kommadi, Open Source for U, November 3, 2021. Link

[230] "Edge Management: The Next Big IoT Challenge", J. White, Embedded Computing Design, April 19, 2021. Link

© Strategy of Things, 2025. All rights reserved.

distributed nature of the heterogeneous devices and components adds a lot of complexity. New models, approaches and tools to manage, orchestrate, automate and support resources, activities and schedules is critical.

6.3.2.6. Optimizing and maintaining performance and Quality of Service under continuously varying conditions

The professional's ability to detect workload demand and allocate appropriate resources to collect, process and store the data, whether on a scheduled or dynamic basis, is crucial to IoT performance. This is made more complex by the addition of new devices of varying capabilities to the environment. These devices may consume existing resources, drop in and out of the network (e.g., mobile devices, etc.) and have varying resource demands and availability of resources. Advanced resource allocation algorithms and methodologies must continually be developed to support the rapidly scaling IoT environment.

6.3.2.7. Improving middleware to support scaling

The environment IoT operates in is characterized by diverse heterogenous devices, connecting to each other and on-premise, edge and cloud servers through a variety of communications protocols and exchanging data in a range of formats. Some of the data are processed on the device, while others are processed on the gateway and in servers in remote data centers. As more IoT devices are added to the network of the future, the ability of these devices to be integrated into the network and interoperate with existing and older devices and systems is critical to scaling.

Middleware, the software that sits between increasingly diverse and heterogeneous devices and applications and allows them to communicate with each other, is essential to integration and scaling of IoT networks. Middleware, however, must also evolve to support future IoT infrastructure needs.

For example, the middleware must reside in the cloud as well as on resource constrained edge gateways and devices. The middleware of the future must support development of context specific applications for new types of devices, dynamically discover and connect to new devices and services that can come online and leave at any time and ensure the security and privacy of the devices that it connects to.[231] Further innovation and development is necessary to close these gaps.

6.3.3. Hyper-Deployed: Advanced computing paradigms

Complexity grows as the number of deployed IoT devices increases. To support all these devices and their unique requirements, the initial device to cloud architecture is quickly evolving to a multi-layer distributed architecture of cloud data centers, local edge servers, processors in routers and gateways and fixed and mobile (e.g., cars and drones) devices.

There is no "one size fits all" architecture and the requirements of the specific IoT applications will determine what architecture works best. For example, applications that are latency sensitive

[231] "IoT Middleware: A Survey on Issues and Enabling Technologies", IEEE Internet of Things Journal. PP. 1-1. 10.1109/JIOT.2016.2615180, Ngu, Anne & Gutierrez, Mario & Metsis, Vangelis & Nepal, Surya & Sheng, Quan. (2016). Link

© Strategy of Things, 2025. All rights reserved.

or operate in an area with unreliable connectivity service may process data on the device or on a nearby edge server.

IoT operates in an expansive ecosystem of interconnected heterogenous devices collecting, processing and exchanging data in real-time across the economy and society. It integrates several computing paradigms, including distributed computing, context-aware computing and swarm intelligence, to create intelligent and adaptive systems. These paradigms form the core of IoT architectures, but as this field continues to expand, several open research challenges need to be addressed to fully realize their potential.

The interplay between distributed computing, context-aware computing and swarm intelligence drives the development of intelligent IoT systems capable of handling complex, dynamic environments. Distributed computing provides the infrastructure for these systems to scale, while context-aware computing enables them to adapt to real-time environmental data. Swarm intelligence offers a decentralized approach to collaboration, allowing large networks of IoT devices to work together without centralized oversight.

The combined use of these paradigms holds significant promise for the future of IoT. As technology advances, the integration of distributed computing, context-aware computing and swarm intelligence will continue to drive innovation and efficiency in IoT systems.

6.3.3.1. Distributed computing

Distributed computing provides the backbone of IoT, allowing devices across vast networks to share workloads, process data in parallel and maintain robust system functionality even when individual nodes fail. By spreading tasks across a network of interconnected devices, distributed computing enhances scalability, performance and resilience in IoT applications.

A number of challenges exist for distributed computing, including resource allocation and management, fault tolerance and reliability and latency and real-time processing. These were briefly discussed in Section 6.3.2. Representative areas of potential innovation for distributed computing in IoT were highlighted in Section 17.3.1.3 for smart cities. These are intelligent caching (positioning and storage of content and data on the network to alleviate traffic congestion and latency issues), collaborative edge computing (sharing of computing tasks and resources with nearby edge servers) and cooperative and sustainable load balancing (balancing of workload between servers to avoid performance issues, excessive energy usage and high operating costs).

6.3.3.2. Context-aware computing

Context-aware computing empowers IoT systems to adapt their behavior based on real-time environmental and user-specific information. By leveraging data from sensors and devices, context-aware systems optimize operations and offer personalized responses to dynamic conditions. This adaptability is crucial for creating intelligent systems in smart homes, cities, healthcare and industrial automation.

Context-aware systems perform a series of functions, including context acquisition (collecting data from sensors and systems), context representation (transforming the collected data into a standardized format for sharing), context storage (store data for use over its lifecycle), context interpretation (determine high level situational context from data) and context adaptation

© Strategy of Things, 2025. All rights reserved.

(respond based on the context).[232] Opportunities for further research and innovation in context-aware computing include:[233]

- Context definition: Frameworks for identifying parameters determining and defining a situation or context.
- Context-aware models: Context-aware architectures, standards and tools.
- Sensing context data: Devices for sensing and collecting data about the environment.
- Predicting context: Techniques to predict context based on the data collected and the defined context.
- Representing and storing context information: Standardized approaches to facilitate context interpretation and context sharing.
- Information inferring context and adapting system behavior: Interpret context and adapt responsive behavior and systems.
- Evaluation of context aware systems: Criteria and measures for quality control and end-user satisfaction of context-aware products.
- Privacy control: Protection of contextual information collected from participating entities.

6.3.3.3. Swarm Intelligence

As IoT adoption scales and the number of devices grows, IoT will transition from devices working individually to create individual outcomes to a collection of IoT devices working together to create an overall greater outcome. Information from one device is communicated locally to another device, where it will be processed to take a certain course of action. These IoT swarms may act independently of people in the background or may act collaboratively with people in various ways.

Each IoT device may be acting on its own, performing its individual tasks, but collectively, the devices will be acting with an intelligence that transcends the intelligence of each device. Key benefits of these intelligent swarm IoT systems include flexibility to changes, robustness against individual failures, the ability to be self-organizing instead of predefined, adaptive to changes and decentralized control.[234] Collective intelligence is a new technology and is immature at this time. Some challenges and gaps that need to be addressed include the development of higher processing capability microprocessors that can run the swarm AI algorithms, the lack of a platform for swarm applications, operations with limited connectivity and needed algorithm development for various operating scenarios.[235]

6.3.4. Hyper-Deployed: Facilitating human centric IoT systems

---

[232] "Future challenges in context-aware computing," N. Malik et al., Conference Paper, IADIS International Conference, 2017. Link

[233] See note 232

[234] "The Collective Power of Swarm Intelligence in AI and Robotics", T. McClean, Forbes, May 13, 2021. Link

[235] Interview notes. Dr. Kiju Lee, Texas A&M University, December 16, 2021

© Strategy of Things, 2025. All rights reserved.

Although IoT connects "things" and machines with other "things" and machines, its value is felt and realized by people. In a future hyperconnected world with billions of smart devices, IoT is embedded and integrated transparently into all aspects of our lives where it is used in our work, our studies, our recreation and our homes. While this "ambient intelligence" world is a vision of the future, human centric IoT is necessary for this vision to become reality.

Consider today's smart phones. A smart phone is an IoT device and many people rely on its maps feature to direct them to a place where they have never been before, along a route that minimizes their transit time.

Despite this, some drivers prefer to use GPS navigation devices instead of the maps feature on their smart phones. GPS navigation devices have larger screens, which makes it easier to read for drivers who may be driving in traffic conditions where they can only take their eyes off the road for a fraction of a second. Others are concerned about their privacy and do not wish to be tracked, while others may have a mobile phone without an unlimited data plan.

Finally, some prefer the GPS navigation units as it is well integrated into their car's auto pilot system and offers a seamless driving experience. As there is a move towards a hyperconnected world with billions of IoT devices, research and innovation in human centric considerations in several areas are critical to driving user adoption and value realization.

Representative areas for future consideration are discussed below.

6.3.4.1. Design for human-AI interaction and collaboration

As adoption of AI-enabled IoT systems becomes more prevalent, some activities normally done by humans will be performed autonomously by AI systems. The role of humans will evolve to jobs where both humans and AI systems are needed to complete a task safely and accurately. As these technologies are adopted, the jobs will change as automation augments human workers, leading to increases in productivity, safety and decreased operational costs.

Human-AI collaboration requires both to "work together as partners to achieve a common goal, sharing a mutual understanding of the abilities and respective roles of each other."[236] The AI system must be enabled to take the most appropriate actions based on an understanding of the current task and real time assessment of the situation by observing the users, predicting their actions and anticipating their needs. Successful collaboration requires the development of new techniques, methods and components to enable a tightly coupled perception-action integration between humans and the AI system.[237]

For replicable and successful collaboration between humans and AI-enabled IoT systems, continued research is necessary to understand how AI systems can most effectively augment humans, how AI systems can enhance what humans do best and how to redesign operations and algorithms to support the collaboration. Some characteristics that impact such collaboration for AI systems include interaction modes, adaptability, performance predictability and

[236] "A Simple Guide to Collaborative AI", AI-on-Demand Platform. Link

[237] See note 236

© Strategy of Things, 2025. All rights reserved.

explainability.[238] For humans, characteristics such as operator age, any specific needs of the operator and culture and language expectations, impact human-AI-IoT collaboration.

6.3.4.2. Enabling generative AI for IoT

AI systems offer transformative opportunities for IoT, capitalizing on the synergy between data generation, processing and interaction with IoT devices. However, adoption of AI systems faces a number of significant challenges due to the resource constraints of IoT devices and the complexity of generative models.[239] One major challenge is the high resource demands of generative AI models, which typically consist of billions of parameters. IoT devices, such as wearables and sensors, often have limited memory and computational power, making it difficult to run these large AI models locally. Techniques such as model compression, quantization and parameter pruning are being explored, but these often lead to trade-offs in model accuracy and performance. Additionally, on-device inference is problematic because IoT applications frequently require real-time responses, which is difficult to achieve given the limited processing capabilities of these devices. Other challenges include prompt engineering for IoT applications that involve multimodal data, such as video, audio and sensor input. Designing efficient and contextually relevant prompts for generative AI to respond to real-world IoT scenarios is complex.

6.3.4.3. Facilitate trust

Human-AI collaboration breaks down or becomes less productive if one or both sides do not execute as expected. For example, an intelligent driving assistance system may apply the brakes on a truck if it detects stopped traffic ahead on the road. But if the system applies the brakes one time and does not in other times, the driver cannot rely on it to work. He may not use it, or only use it under certain conditions. In other situations, the AI system may work as designed, but people are not able to explain why it works and why it did what it did.

To develop more trustworthy human-AI collaboration, a holistic approach to understanding trust is needed. The human side of collaboration is equally important. Factors such as age, gender and cultural background affect trust. The conditions in which the human-AI collaboration operate is another factor, with people over-trusting a machine's recommendations in high stress scenarios.

6.3.4.4. Facilitate accessibility and inclusion

Despite the value that IoT provides, its benefits may not be available or accessible to everyone. For example, many cities are implementing "smart parking" technologies that help drivers find open parking spaces by communicating that information on a smart phone app. However, 11% of U.S. adults have non-smart cellphones[240] and do not have access to this information.

This simple example illustrates a broader challenge. No matter how prevalent and connected IoT is, the real world is filled with people who cannot fully access the benefits of a fully connected society. People who have low vision cannot access and interact with information displayed on

[238] "Human - AI Collaboration Framework and Case Studies", Partnership on AI, September 2019. Link

[239] "IoT in the Era of Generative AI: Vision and Challenges," X. Wang, Z. Wan et al., January 2024. Link

[240] Mobile Fact Sheet, Pew Research Center, April 7, 2021. Link

© Strategy of Things, 2025. All rights reserved.

monitors and smart phone screens. People with low digital literacy struggle to perform complex operations, while those with poor reading proficiency struggle to use text-based applications.

To be inclusive and accessible to as many people as possible, a connected society must develop interaction models and user interfaces that are intuitive, easy to use and program and consistent with the way people expect to interact with human-AI and IoT systems. Interactions may be performed through gestures, voice, neural scans, proximity through wearable devices or other means. As human-AI collaborations become more common, continued research and innovation in enabling more effective user experiences and user interaction are required.

© Strategy of Things, 2025. All rights reserved.

7. Economic Analysis of Gaps

The objective of the economic analysis of gaps is to determine the best allocations of public resources to IoT infrastructure. These allocations were calculated to provide the maximum benefit to the economy. This required integrating information on the role of the public sector, the importance of the single technology components, the likely future value of IoT in that industry along with financial ratios such R&D expenditure as a percentage of revenue and gross margins for each industry.

In quantifying the economic impact of addressing the IoT gaps, our study employed the perspective of federal government executives planning research investment decisions. These executives face several questions, including:

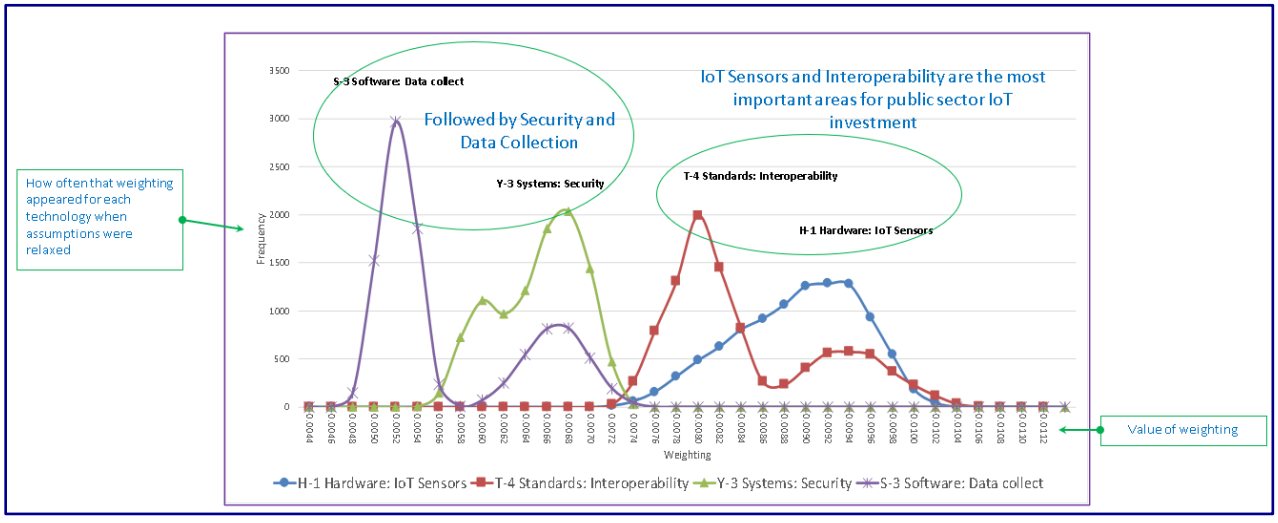
- "If I had to invest a limited amount of money for research, what gaps do I spend it on?"
- "How and where should I allocate that investment to maximize its impact?"
- "How can I minimize the overall risks to my investments?"

Our study employed a portfolio investment approach to address these questions. The economic model considers a nominal public sector investment of $10 million distributed across the nine industries for each single technology component. The results for the single technology components were then used in different combinations to assess the economic impact of the core and intelligence gaps.

In integrating the quantitative survey results with the qualitative information, two arbitrary decisions were required. Section 25.2 provides details on these decisions to produce the quantified relative ranking of the importance of each of the 25 single technology components by industry.

To confirm which of the single technology components were the most important, a Monte Carlo method was applied to the two values replacing their single values with a value randomly selected from a range and then repeating the calculation. Details are provided in Section 26.3

Figure 7-1 below shows the frequency diagram of this repeated calculation on the importance of the top four single technology components. This shows that Hardware IoT sensors and Standards Interoperability are equal first followed by Systems Security and Software Data Collect.



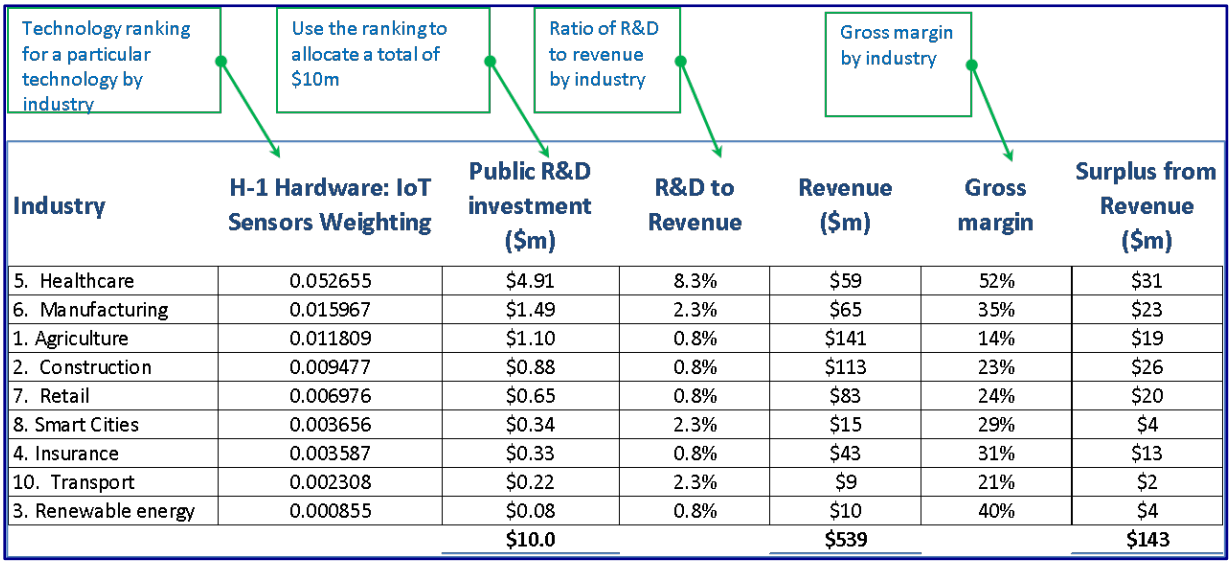
© Strategy of Things, 2025. All rights reserved.

Figure 7-1: Ranking Confidence for the Four Most Important Single Technology Components

The industry values were then used to allocate a nominal $10 million dollar investment in R&D[241] by the public sector for each of the four most important single technology components. The model then used industry ratios of R&D to revenue and gross margins to estimate the impact by industry of R&D investment in that technology on economic surplus.[242]

7.1.1. Public sector technology investments

This section looks at the impact of a nominal public sector investment of $10 million. As this analysis relies on strong assumptions the calculations should be seen as indicative and used to illustrate the concept rather than as a business case. Figure 7-2 below outlines the flow of the calculation from ranking to R&D investment to Revenue to Surplus.



Industry	H-1 Hardware: IoT Sensors Weighting	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
5. Healthcare	0.052655	$4.91	8.3%	$59	52%	$31
6. Manufacturing	0.015967	$1.49	2.3%	$65	35%	$23
1. Agriculture	0.011809	$1.10	0.8%	$141	14%	$19
2. Construction	0.009477	$0.88	0.8%	$113	23%	$26
7. Retail	0.006976	$0.65	0.8%	$83	24%	$20
8. Smart Cities	0.003656	$0.34	2.3%	$15	29%	$4
4. Insurance	0.003587	$0.33	0.8%	$43	31%	$13
10. Transport	0.002308	$0.22	2.3%	$9	21%	$2
3. Renewable energy	0.000855	$0.08	0.8%	$10	40%	$4
		$10.0		**$539**		**$143**

Figure 7-2: Public Sector Investment to Surplus

7.1.2. Surplus estimates by single technology component

At this stage of the analysis the model has provided a ratio ranked list of the economic importance of public sector investments in different single technology component[243] technology by industry. This list incorporates the economic value of the IoT investment, information from the survey, interviews and desk research and the role of the public sector.

Figure 7-3 below shows these results of a nominal $10 million public sector investment in each of the top four single technology components using the weighted average revenue to R&D ratio

[241] The nominal $10 million is considered as the value of a combination of different government initiatives and support.

[242] As a formula: Surplus = ($ 10 million * Weighting) / R&D to revenue ratio) * Gross Margin

[243] See Figure 2-2.

© Strategy of Things, 2025. All rights reserved.

and gross margin.

Single Technology Component	Investment ($m)	R&D to Revenue	Revenue from investment ($m)	Gross Margin	Surplus from Revenue ($m)
H1: Hardware Sensors	$10	1.8%	$549	26%	$143
T4: Standards Interoperability	$10	2.3%	$438	24%	$106
S3: Software Data Collection	$10	3.7%	$269	27%	$72
Y3: Systems Security	$10	1.7%	$578	26%	$150

Figure 7-3: Economic Impact of Single Technology Component Investments

Figure 7-4 through Figure 7-7 below provides the detailed allocation by industry for each of the $10 million public sector investments. A number of observations were made from an examination of these gap specific analyses, including:

- In each of the four single technology component investments, healthcare is allocated a material part of the investment. This is a result of the importance of healthcare to the U.S. economy.
- Similarly, renewable energy only receives modest allocations. This is a result of the comparatively small role renewable energy plays in the economy, rather than any view on the importance of decarbonizing the economy.
- The size of the investment allocations, for a particular technology gap, should be viewed in comparison with other industries and not solely on its own. Not doing so will lead to incorrect conclusions. For example, Figure 7-4 shows the renewable energy industry received a small investment allocation (0.8% of a nominal $10 million public sector investment). It would be erroneous to draw the conclusion that public sector research investments for IoT sensors are underfunded in renewable energy. However, when viewed from a broader perspective of how IoT sensor investments should be allocated across a number of industries to maximize economic surplus to the economy, the investment allocation percentages are logical.

The remainder of this section shows the detailed allocations, revenues and surplus for each of the single technology components.

Figure 7-4 below shows an associated revenue of $549 million and a surplus of $143 million based on R&D to revenue ratios and a gross margin for each industry from an investment in the IoT single technology component of Hardware Sensors (H-1)

© Strategy of Things, 2025. All rights reserved.

Industry	H-1 Hardware: IoT Sensors Weighting	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
5. Healthcare	0.037467	$4.90	8.3%	$59	52%	$31
6. Manufacturing	0.009951	$1.30	2.3%	$57	35%	$20
1. Agriculture	0.009056	$1.18	0.8%	$152	14%	$21
2. Construction	0.007115	$0.93	0.8%	$119	23%	$27
7. Retail	0.004772	$0.62	0.8%	$80	24%	$19
8. Smart Cities	0.002978	$0.39	2.3%	$17	29%	$5
4. Insurance	0.002649	$0.35	0.8%	$44	31%	$14
10. Transport	0.001849	$0.24	2.3%	$11	21%	$2
3. Renewable energy	0.000623	$0.08	0.8%	$10	40%	$4
		$10.0		**$549**		**$143**

Figure 7-4: Investment Return for Hardware H-1

Figure 7-5 below shows an associated $106 million surplus from a $10 million public investment in the IoT single technology component of Standards Interoperability (T-4)

Industry	T-4 Standards: Interoperability Weighting	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
5. Healthcare	0.018956	$2.48	8.3%	$30	52%	$16
1. Agriculture	0.008197	$1.07	0.8%	$137	14%	$19
6. Manufacturing	0.005940	$0.78	2.3%	$34	35%	$12
7. Retail	0.005454	$0.71	0.8%	$91	24%	$22
2. Construction	0.004318	$0.56	0.8%	$72	23%	$16
8. Smart Cities	0.002978	$0.39	2.3%	$17	29%	$5
10. Transport	0.002659	$0.35	2.3%	$15	21%	$3
4. Insurance	0.001926	$0.25	0.8%	$32	31%	$10
3. Renewable energy	0.000486	$0.06	0.8%	$8	40%	$3
		$10.0		**$438**		**$106**

Figure 7-5: Investment Return for Standards Interoperability T-4

Figure 7-6 below shows an associated $72 million surplus from a $10 million public investment in the IoT single technology component of Software Data (S-3)

© Strategy of Things, 2025. All rights reserved.

Industry	S-3 Software: Data collect Weighting	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
5. Healthcare	0.025620	$3.35	8.3%	$40	52%	$21
2. Construction	0.004318	$0.56	0.8%	$72	23%	$16
1. Agriculture	0.003433	$0.45	0.8%	$58	14%	$8
6. Manufacturing	0.002807	$0.37	2.3%	$16	35%	$6
7. Retail	0.002727	$0.36	0.8%	$46	24%	$11
10. Transport	0.002589	$0.34	2.3%	$15	21%	$3
8. Smart Cities	0.001276	$0.17	2.3%	$7	29%	$2
4. Insurance	0.000642	$0.08	0.8%	$11	31%	$3
3. Renewable energy	0.000243	$0.03	0.8%	$4	40%	$2
		$10.0		**$269**		**$72**

Figure 7-6: Investment Return for Software Data Collection S-3

Figure 7-7 below shows an associated $150 million surplus from a $10 million public investment in the in the IoT single technology component of Systems Security (Y-3)

Industry	Y-3 Systems: Security Weighting	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
5. Healthcare	0.016586	$4.43	8.3%	$54	52%	$28
1. Agriculture	0.004807	$1.28	0.8%	$165	14%	$22
7. Retail	0.004091	$1.09	0.8%	$140	24%	$34
6. Manufacturing	0.004010	$1.07	2.3%	$47	35%	$16
10. Transport	0.002219	$0.59	2.3%	$26	21%	$5
8. Smart Cities	0.002127	$0.57	2.3%	$25	29%	$7
4. Insurance	0.001926	$0.51	0.8%	$66	31%	$20
2. Construction	0.001178	$0.31	0.8%	$40	23%	$9
3. Renewable energy	0.000486	$0.13	0.8%	$17	40%	$7
		$10.0		**$578**		**$150**

Figure 7-7: Investment Return for Systems Security Y-3

Another way to understand the context of the investment allocations is to compare those allocations with other technologies within the industry. For example, Figure 7-8 below shows that for the renewable energy industry, IoT sensors (H-1) received $.08 million of a $10 million nominal public sector investment, standards interoperability (T-4) received $.06 million, software data collection (S-3) received $.03 million and systems security (Y-3) received $.13 million.

These allocations show the relative importance of security investments, which were two and four times that for standards interoperability and software data collection, respectively. This result is consistent with industry research which highlighted cybersecurity as one of the top three IoT

© Strategy of Things, 2025. All rights reserved.

technology challenges (See Section 5.3.9.2).

Industry	H1 Hardware: IoT Sensors	T-4 Standards: Interoperability	S-3 Software: Data Collection	System: Security (Y-3)
Healthcare	$4.90	$2.48	$3.35	$4.43
Manufacturing	$1.30	$0.78	$0.37	$1.07
Agriculture	$1.18	$1.07	$0.45	$1.28
Construction	$0.93	$0.56	$0.56	$0.31
Retail	$0.62	$0.71	$0.36	$1.09
Smart cities	$0.39	$0.39	$0.17	$0.57
Insurance	$0.35	$0.25	$0.08	$0.51
Transport/Logistics	$0.24	$0.35	$0.34	$0.59
Renewable Energy	$0.08	$0.06	$0.03	$0.13
Total	**$10.0**	**$10.0**	**$10.0**	**$10.0**

Figure 7-8: Investment Allocations by Industry and Technology ($m).

Figure 7-8 shows from an economic modeling perspective, what single technology component, of the four listed, receives the highest allocation for the industries studied.

It is observed that across two-thirds of the industries, the economic model identified System Security (Y-3) as a top technology gap from a research investment perspective while investments in IoT sensors is most important in the other three industries.

In contrast, data collection was the least important in two-thirds of the industries examined. The way to interpret and understand this result is to note that while data collection capabilities are important, there are other technologies that are more critical from an investment perspective.

Some of the results in Figure 7-8 can be partially explained from an industry research perspective. For example:

- In healthcare, IoT sensors and security are roughly at the same level of importance. Research investments in sensors can lead to new opportunities for monitoring more diseases, or better monitor existing diseases and conditions, leading to better health outcomes. (See Section 5.3.7.1). Similarly, investments in security are important because medical devices and IoMT systems are especially vulnerable to cyber threats. (See Section 5.3.7.2).
- In smart cities, sensors and standards for interoperability are equally important, behind security. From an adoption perspective, research in sensors enables new smart city opportunities to address city challenges (See Section 5.3.5.1) while standards and interoperability allow these smart city systems to integrate and exchange information with other systems. In smart cities, the lack of interoperability is a major barrier. (See Section 5.3.5.2).
- In transportation and logistics, standards and interoperability and data collection have equal investment importance. This result is attributed to the lack of information sharing

© Strategy of Things, 2025. All rights reserved.

and legacy systems that are hindering end-to-end supply chain visibility in the industry. (See Section 5.3.6.2).

- While security is an important consideration in most industries, the economic model generated a low investment allocation in the construction industry. One reason for this is that while IoT can provide benefits to the construction industry, our research found that the industry is largely "behind the curve" in digitalization. (See Section 5.3.5.1). As a result, concerns about cybersecurity are not as high as they would be in industries that are further along the digitalization path.
- In agriculture, the model showed sensors, interoperability and standards and security are roughly allocated the same research investment amounts. This is consistent with the importance of smart or precision agriculture and the need to digitalize and automate as many aspects of agriculture operations as possible. In addition, many farms have a large stock of existing and legacy equipment, which hinders integration with modern systems and IoT solutions. (See Section 5.3.1.2).

7.1.3. Surplus estimates by core and intelligence gaps

The analysis provided a set of core and intelligent gaps. Each gap maps to one or more of the 25 single technology components indicated in the IoT taxonomy in Figure 2-2. For example, interoperability allows different devices and systems to connect to each other, communicate and exchange data. Achieving interoperability requires addressing the underlying technology drivers – standards and middleware/integration.

Informed by our understanding of the Internet of Things (see Section 4), our economic model uses the following assignments to analyze each of the gaps:

Core Gaps:

- Interoperability: Y-1 Systems Middleware + T-4 Standards: Interoperability
- Privacy: Standards: T-3 Standards Privacy + Y-3 Systems Security + T-1 Standards Security
- Security Standards: Y-3 Systems Security + T-1 Standards Security
- Connectivity N-1: Network Gateways + N-2: Network Connectivity + A-2 Application Network Management

Intelligence Gaps:

- Data management: A-3 Application Data Management
- Artificial intelligence: A-4 Apps: Data analytics + Y-4 Systems Artificial Intelligence
- Intelligent devices: H-3 Hardware: Processing + H-4 Hardware: Edge Devices + H-1 Hardware IoT Sensors

Our research findings and economic analysis suggest that investments to address the gaps should be considered from the perspective of a portfolio. The Internet of Things is built on a diverse set of technologies at varying stages of maturity. Furthermore, the gaps are not discrete but

© Strategy of Things, 2025. All rights reserved.

dependent on each other and are comprised of a portfolio of individual technology components (See Figure 2-2).

The framework for identifying and classifying technology infrastructure gaps is aligned to the continuing evolution of IoT and the framework takes into account the interdependence of the gaps.

The investment allocations consider the specific gaps, their relationships with other gaps, the state of maturity relative to the IoT evolution stage and the specific technological challenges within the industry.

Given the uncertainty both within and between the individual technology analyses a portfolio approach is proposed. Rather than maximize the return for a particular risk preference, the portfolio approach considers the uncertainties associated with the inputs. Investing all monies in the single industry or technology that has the highest ratio of surplus to investment would strain the model and lead to a resource misallocation.

A portfolio approach balances these considerations to prioritize and allocate investments to maximize the opportunities to advance IoT development, accelerate IoT adoption across industry by removing technological barriers and reduce the risk of poor outcomes from those investments and priorities.

Figure 7-9 below repeats the analysis of the impact of a nominal $10 million public sector investment using the research and development to revenue ratios along with gross margins.

Gap	Investment ($m)	R&D to Revenue	Revenue from investment ($m)	Gross Margin	Surplus from Revenue ($m)
Core: Interoperability	$10.0	1.5%	$650	25%	$162
Core: Privacy	$10.0	1.8%	$548	27%	$149
Core: Security	$10.0	1.8%	$566	27%	$150
Core: Connectivity	$10.0	1.2%	$822	23%	$189
Intelligence: Data Management	$10.0	1.1%	$889	27%	$239
Intelligence: Artificial Intelligence (Trust)	$10.0	1.5%	$670	25%	$167
Intelligence: Intelligent Devices	$10.0	1.6%	$626	25%	$158

Figure 7-9: Revenue and Surpluses from Public Sector Investment in Core and Intelligence Gaps

The model produces estimates of associated surplus ranging from $149 million to $239 million for the identified gaps. A number of observations were made from this analysis, including:

© Strategy of Things, 2025. All rights reserved.

- A $10 million investment produces a range of quantitative revenue and surplus outcomes dependent on the sum of the technology weightings and accounting ratios.

  From a technology perspective, the addressing of specific IoT technology infrastructure gaps will lead to a range of economic outcomes. For example:

  - Addressing interoperability gaps will allow different devices and systems to integrate, resulting in improved integration and the potential to automate certain processes, leading to increases in efficiencies and productivity.
  - Improvements in data management allow organizations to make better use of their data to support more informed and timely decision-making, leading to improved operations and lowered risks.
  - Addressing the security gaps leads to significantly better outcomes in protection of data with some improvements in protection of systems from operational disruption.
  - Gaps in IoT cybersecurity leads to vulnerabilities that expose private data. As more devices and systems are connected to the Internet, manufacturing and industrial systems that were formerly "air gapped" are now exposed, increasing the risk of cybersecurity breaches.

- There is likely some correlation between the technologies where improvements in one area cascade on to other areas. For example:
  - Addressing interoperability challenges will allow more connected devices to communicate and exchange data with each other but will also increase the cybersecurity risk profile of the entire system.
  - Gaps in data management will hinder artificial intelligence, which relies on timely access to high quality data to train models and to act on the information to drive insights, create responses and automate operations. Gaps in intelligent device capabilities hinder them from incorporating and executing complex AI models on the device.
- While the analysis provides an indicative economic impact of a nominal $10 million public sector investment, it does not indicate how much investment should be allocated to address the specific gaps. Those considerations are beyond the scope of this study and involve other factors including technology maturity and complexity, policy, roles of industry and federal priorities.

Figure 7-10 through Figure 7-16 below show the detailed industry allocations and economic impacts of the core and intelligence gaps in the industries studied. A number of observations were made from an examination of these gap specific analyses, including:

- In some cases where there has been minimal mention in the survey or desk research of a particular technology in an industry, no allocation was made to that industry for the particular technology. For example, Figure 7-13 shows that the Core: Connectivity gap is addressed by allocating research investments to support the needs of only three industries: agriculture, insurance and manufacturing.

© Strategy of Things, 2025. All rights reserved.

- The industry investment allocations differ for each technology infrastructure gap. For example, the analysis estimated that $3.68 million out of the $10 million nominal research investment (37%) be allocated to the healthcare industry while only 1.1% be allocated to the renewable energy industry. The healthcare industry plays a large role in the economy and the public sector along with a high gross margin and received a substantial allocation of the $10 million investment for a number of gaps, including interoperability, privacy, security, artificial intelligence and intelligent devices.
- Not all investments enjoy the same returns. Figure 7-10 shows that allocating 13% of a nominal investment to address interoperability in manufacturing provides a 43-fold (56/1.3) return for revenue and a 15-fold surplus (20/1.3). In contrast, a 5.3% allocation to address the same gap in the transportation and logistics industry creates a return on revenue of 47 (23/.53) and a 9-fold surplus (5/.53) surplus.

Core: Interoperability

Industry	Sum	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
1. Agriculture	0.0089	$1.38	0.8%	$177	14%	$24
2. Construction	0.0055	$0.85	0.8%	$109	23%	$25
3. Renewable energy	0.0007	$0.11	0.8%	$15	40%	$6
4. Insurance	0.0026	$0.40	0.8%	$51	31%	$16
5. Healthcare	0.0237	$3.68	8.3%	$44	52%	$23
6. Manufacturing	0.0083	$1.30	2.3%	$56	35%	$20
7. Retail	0.0075	$1.16	0.8%	$149	24%	$36
8. Smart Cities	0.0038	$0.59	2.3%	$26	29%	$7
10. Transport	0.0034	$0.53	2.3%	$23	21%	$5
		$10.0		**$650**		**$162**

Figure 7-10: Impact of Public Sector Investment in Core: Interoperability

Core: Privacy

Industry	Sum	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
1. Agriculture	0.0082	$0.93	0.8%	$119	14%	$16
2. Construction	0.0027	$0.31	0.8%	$40	23%	$9
3. Renewable energy	0.0010	$0.11	0.8%	$14	40%	$6
4. Insurance	0.0058	$0.65	0.8%	$83	31%	$26
5. Healthcare	0.0379	$4.27	8.3%	$52	52%	$27
6. Manufacturing	0.0112	$1.26	2.3%	$55	35%	$19
7. Retail	0.0082	$0.92	0.8%	$118	24%	$29
8. Smart Cities	0.0068	$0.77	2.3%	$33	29%	$10
10. Transport	0.0071	$0.80	2.3%	$35	21%	$7
		$10.0		**$548**		**$149**

Figure 7-11: Impact of Public Sector Investment in Core: Privacy

© Strategy of Things, 2025. All rights reserved.

Core: Security						
Industry	Sum	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
1. Agriculture	0.0062	$1.06	0.8%	$136	14%	$18
2. Construction	0.0016	$0.27	0.8%	$35	23%	$8
3. Renewable energy	0.0007	$0.13	0.8%	$16	40%	$6
4. Insurance	0.0032	$0.55	0.8%	$71	31%	$22
5. Healthcare	0.0237	$4.06	8.3%	$49	52%	$26
6. Manufacturing	0.0072	$1.24	2.3%	$54	35%	$19
7. Retail	0.0061	$1.05	0.8%	$135	24%	$33
8. Smart Cities	0.0047	$0.80	2.3%	$35	29%	$10
10. Transport	0.0049	$0.84	2.3%	$36	21%	$8
		$10.0		**$566**		**$150**

Figure 7-12: Impact of Public Sector Investment in Core: Security

Core: Connectivity						
Industry	Sum	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
1. Agriculture	0.0030	$3.40	0.8%	$436	14%	$59
2. Construction		$0.00	0.8%	$0	23%	$0
3. Renewable energy		$0.00	0.8%	$0	40%	$0
4. Insurance	0.0010	$1.17	0.8%	$149	31%	$46
5. Healthcare		$0.00	8.3%	$0	52%	$0
6. Manufacturing	0.0049	$5.43	2.3%	$236	35%	$84
7. Retail		$0.00	0.8%	$0	24%	$0
8. Smart Cities		$0.00	2.3%	$0	29%	$0
10. Transport		$0.00	2.3%	$0	21%	$0
		$10.0		**$822**		**$189**

Figure 7-13: Impact of Public Sector Investment in Core: Connectivity

Intelligence: Data Management						
Industry	Sum	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
1. Agriculture		$0.00	0.8%	$0	14%	$0
2. Construction		$0.00	0.8%	$0	23%	$0
3. Renewable energy		$0.00	0.8%	$0	40%	$0
4. Insurance		$0.00	0.8%	$0	31%	$0
5. Healthcare		$0.00	8.3%	$0	52%	$0
6. Manufacturing	0.0024	$4.64	2.3%	$202	35%	$71
7. Retail	0.0028	$5.36	0.8%	$688	24%	$167
8. Smart Cities		$0.00	2.3%	$0	29%	$0
10. Transport		$0.00	2.3%	$0	21%	$0
		$10.0		**$889**		**$239**

Figure 7-14: Impact of Public Sector Investment in Intelligence: Data Management

© Strategy of Things, 2025. All rights reserved.

Intelligence: Artificial Intelligence						
Industry	Sum	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
1. Agriculture	0.0079	$1.44	0.8%	$185	14%	$25
2. Construction	0.0059	$1.08	0.8%	$139	23%	$32
3. Renewable energy	0.0008	$0.15	0.8%	$19	40%	$8
4. Insurance	0.0023	$0.43	0.8%	$55	31%	$17
5. Healthcare	0.0179	$3.29	8.3%	$40	52%	$21
6. Manufacturing	0.0084	$1.54	2.3%	$67	35%	$24
7. Retail	0.0049	$0.89	0.8%	$114	24%	$28
8. Smart Cities	0.0045	$0.84	2.3%	$36	29%	$11
10. Transport	0.0018	$0.34	2.3%	$15	21%	$3
		$10.0		**$670**		**$167**

Figure 7-15: Impact of Public Sector Investment in Intelligence: Artificial Intelligence

Intelligence: Intelligent Devices						
Industry	Sum	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
1. Agriculture	0.0180	$1.34	0.8%	$171	14%	$23
2. Construction	0.0138	$1.03	0.8%	$131	23%	$30
3. Renewable energy	0.0020	$0.15	0.8%	$19	40%	$8
4. Insurance	0.0039	$0.29	0.8%	$38	31%	$12
5. Healthcare	0.0588	$4.37	8.3%	$53	52%	$28
6. Manufacturing	0.0144	$1.07	2.3%	$46	35%	$16
7. Retail	0.0143	$1.06	0.8%	$137	24%	$33
8. Smart Cities	0.0055	$0.41	2.3%	$18	29%	$5
10. Transport	0.0037	$0.28	2.3%	$12	21%	$3
		$10.0		**$626**		**$158**

Figure 7-16: Impact of Public Sector Investment in Intelligence: Intelligent Devices

© Strategy of Things, 2025. All rights reserved.

8. Opportunities for Government

As new technologies are discovered and their practicalities explored, they can diffuse into the broader economy if they can provide material benefits. Figure 8-1 below shows an historical view of how earlier consumer technologies found their place in the economy.

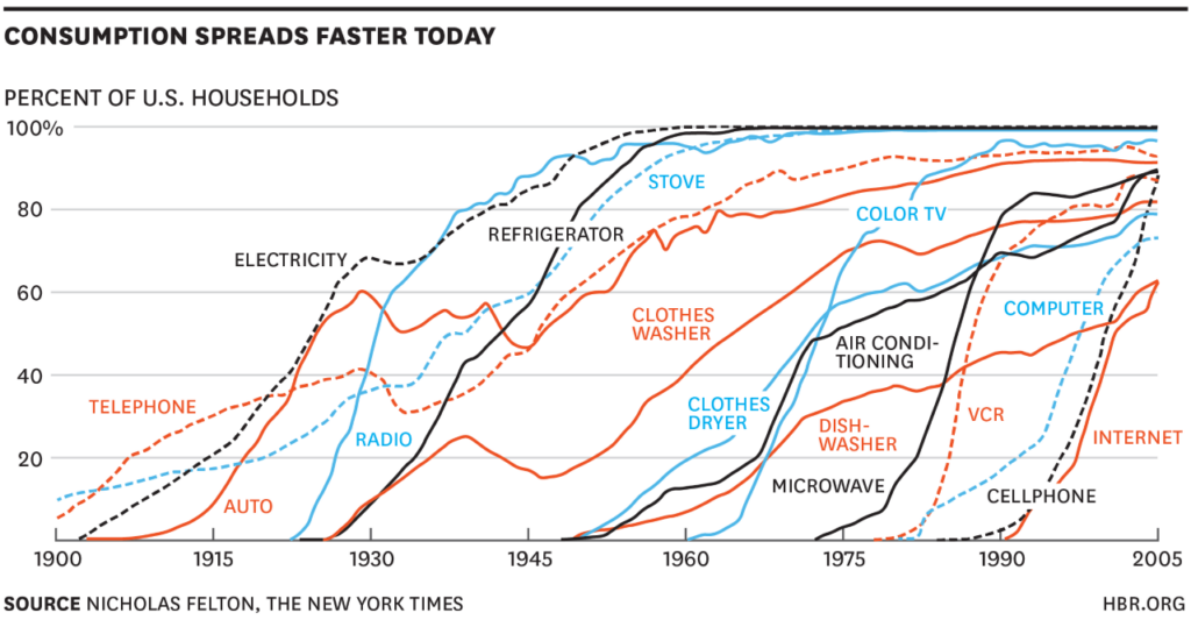


Figure 8-1: Technology Diffusion

These curves represent the rate at which new technology is embraced by the market.[244] Initially, a small percentage of early adopters utilize the new technology. These early adopters are often risk-takers, willing to experiment with innovative solutions despite potential uncertainties. This phase is critical for validating the technology's viability and functionality.

As the technology gains market traction and matures, the technology experiences rapid adoption driven by consumers' increased awareness and realization of benefits, such as increased productivity, cost savings and enhanced safety. Adoption reaches a tipping point when the technology is widespread and integrated into everyday use.

Upon reaching the tipping point, the rate of consumers' adoption slows and reaches a plateau as the technology becomes ubiquitous, reaching its maximum penetration within the market. Further adoption is limited and comes from technology latecomers or laggards.

The rate and extent of technology diffusion can be influenced by several factors, such as the availability of supporting infrastructure, the type of benefits as well as safety and risk, which all can play a role in facilitating the spread of the technology's adoption.

Government policies and actions, including research and development, regulations and legislation and workforce development can also slow or advance this technology diffusion. For

[244] "The Pace of Technology Adoption is Speeding Up," R. McGrath, Harvard Business Review, November 25, 2013. Link.

© Strategy of Things, 2025. All rights reserved.

example, policies promoting digital skills development increase the pool of adopters able to use and adapt to new technologies. On the other hand, onerous regulations may increase the price of the technology and reduce its affordability for the adopter wanting to purchase it.

8.1. IoT Considerations for policymakers

While IoT offers significant and transformational outcomes, several factors must be considered to facilitate its scaling into the economy and civil society. Policymakers play an important role in driving adoption and acceleration of IoT in ways that industry cannot do. Factors that government policymakers should consider supporting include:

- **Technology maturity.** IoT is not one technology, but a variety of disparate standards, hardware, software and connectivity technologies at different levels of maturity and adoption. Furthermore, IoT is converging with adjacent technologies, such as blockchain and artificial intelligence, which are also at various levels of maturity. To support effective adoption of IoT overall, policymakers can align governmental actions with the technology maturity stage to drive effective outcomes.
- **Cybersecurity**. IoT devices create new attack surfaces and expose vulnerabilities that can be exploited by cybercriminals. This can lead to breaches of IoT systems and the broader integrated IT networks with unauthorized access and theft of data and information, disruption of businesses and critical infrastructure and compromised safety. In addition, IoT devices can be "hijacked" and used in attacks on other systems. Policymakers should consider actions to facilitate IoT that are safe to use and to scale.
- **Data privacy, ownership and governance**. IoT devices collect and generate large volumes of data, raising questions about consent, ownership, access, usage, sharing and control. To prevent abuse and promote fair data governance practices, policymakers should consider actions around data ownership and usage rights and responsibilities.
- **Interoperability and Standards.** The IoT ecosystem comprises a diverse array of devices from different manufacturers, operating on various protocols and platforms with a range of users. Furthermore, to have a functional ecosystem, IoT must be able to integrate and interoperate with legacy technology systems with proprietary protocols. To ensure seamless communication and compatibility between devices and systems, policymakers should consider actions around the challenge of establishing interoperability standards.
- **Liability and Accountability.** Liability concerns arising from known and unknown outcomes for owners and users slow the development and adoption of IoT systems. This is further exacerbated by artificial intelligence used in autonomous systems, where actions taken by algorithms are not always transparent and explainable. Policymakers should consider undertaking actions that facilitate and clarify responsibility and ensure accountability for any harm caused by IoT devices or networks.
- **Regulatory Frameworks**. Existing regulatory frameworks may not adequately address the unique challenges posed by employing innovative IoT technologies, especially those that operate in regulated industries such as healthcare, insurance and energy. To address issues such as cybersecurity, data protection, safety, consumer rights and environmental

© Strategy of Things, 2025. All rights reserved.

impact in the context of IoT, policymakers need to adapt existing regulations or develop new ones.

- **Ethical and Social Implications**. IoT deployments can have profound societal impacts, affecting employment, healthcare, transportation and urban planning. The outcomes provided may not be accessible, equitable or inclusive. To ensure efficacious outcomes, policymakers should consider actions that address ethical and socio-economic concerns, including issues related to surveillance, discrimination, inequality and the digital divide.
- **International collaboration and coordination.** IoT ecosystems operate across national borders, requiring international cooperation and coordination among policymakers to address regulatory gaps, harmonize standards and facilitate cross-border trade and data flows while respecting sovereignty and cultural differences.
- **New and emerging business models**. IoT changes and creates new innovative business models and ecosystems. For example, some businesses that sell hardware may sell digital services, information and "IoT as a service." Policymakers would do well to consider undertaking actions that facilitate the development, adoption and operation of these new business models into the economy.

8.2. Framework for IoT policymaking

This section proposes a framework to examine government policymaking actions to address IoT technology infrastructure gaps identified in this research. The gaps identified are complex and in many cases long running. Addressing these gaps will require both individual and coordinated interagency action. The framework, shown below in Figure 8-2, focuses on five areas that the U.S. federal government can consider to facilitate the resolution of the IoT technology infrastructure challenges.

© Strategy of Things, 2025. All rights reserved.

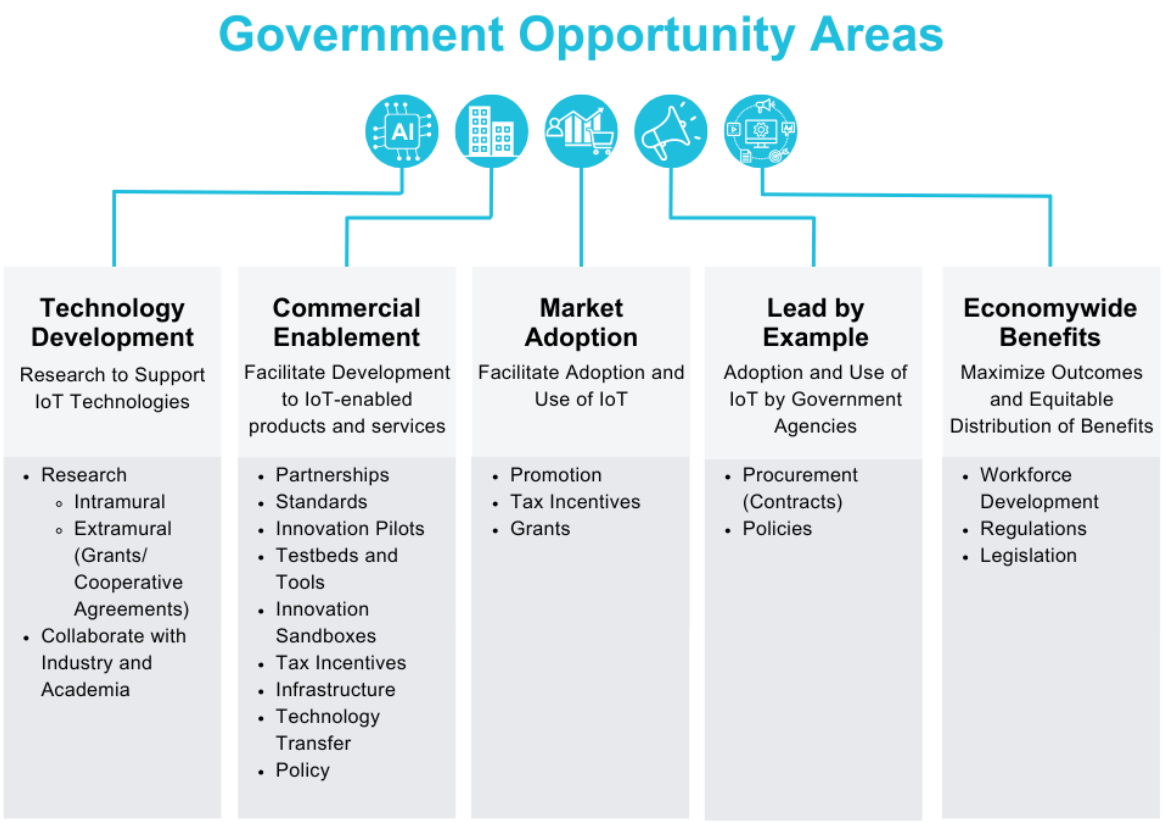


Figure 8-2: Government Opportunity Framework

A brief description of the five areas of government opportunity is provided below. The federal government is active in each of the five areas in supporting other technologies. A more detailed discussion of these areas can be found in Section 24.2.

Technology development. Research is fundamental to the United States' ability to develop and advance new technologies and innovations. The federal government supports research in several ways, including conducting research through its network of national laboratories and Federally Funded Research and Development Centers (FFRDC), funding and supporting research through industry and universities and transferring federal research to market (technology transfer). A number of federal organizations conduct and support research, including the National Science Foundation (NSF), the National Institute of Standards and Technology (NIST), Department of Energy (DOE), Department of Defense (DoD) and the Department of Transportation (DOT). In addition, research is also funded by several Advanced Research Projects Agency (ARPA) organizations. These agencies, modeled after the Defense Advanced Research Projects Agency (DARPA), include ARPA-E (energy), ARPA-H (healthcare), ARPA-I (infrastructure) and IARPA (intelligence) and fund breakthrough, high-risk and high reward research.

© Strategy of Things, 2025. All rights reserved.

Commercial enablement. Commercial enablement refers to U.S. government activities and initiatives that facilitate the commercialization of products and services from research. This includes supporting the technologies developed through federal intramural research, industry and university research as well as independent industry efforts. The federal government supports the commercialization of innovative technologies in several ways. These include facilitating standards development, providing tax incentives for technology development, collaborative public/private partnerships, developing testbeds and tools, innovation sandboxes, enabling infrastructure development and technology transfer.

Facilitate market adoption. Innovative and emerging technologies, such as IoT, face market adoption challenges. Technology adopters fall along an adoption continuum, from visionary early-adopters trying the "latest and greatest" to laggards who are the last to adopt. These actions by the federal government help drive market awareness, interest and ability to adopt new technologies. The federal government plays an important role in facilitating market adoption by promoting awareness, offering incentives and providing funding and resources.

Lead by example. Lead by example refers to a set of actions that the federal government can undertake to signal both support and interest. In 2021, the federal government spent $645 billion in contracts for products and services, up from $513 billion in 2017.[245] This substantial buying power allows the federal government to influence and drive desired outcomes in technology development and adoption. The government can utilize direct procurement, implementation of contracting policies and innovation pilots to support market developments. Examples of government action include procurement for internal use, development of procurement policies and innovation pilots.

Broaden economy wide benefits. Accelerate economy wide benefits refers to policymaking activities that remove structural barriers to maximize benefits to the economy on a broader scale and facilitate equitable distribution of outcomes while minimizing negative outcomes such as compromised safety, cybersecurity and misuse. Potential activities include workforce development, infrastructure development, and enacting regulations and legislation.

8.3. Government opportunities to address key gaps

This section offers some possible opportunities for government action to address the IoT technology infrastructure gaps identified in our research. The gaps, shown in Figure 8-3, are discussed in Section 6. A detailed description of the gaps is found in Section 23.

[245] "Federal Contract Spending in the Last 5 Years," K. Bernal, GovConWire, May 25, 2022. Link

© Strategy of Things, 2025. All rights reserved.

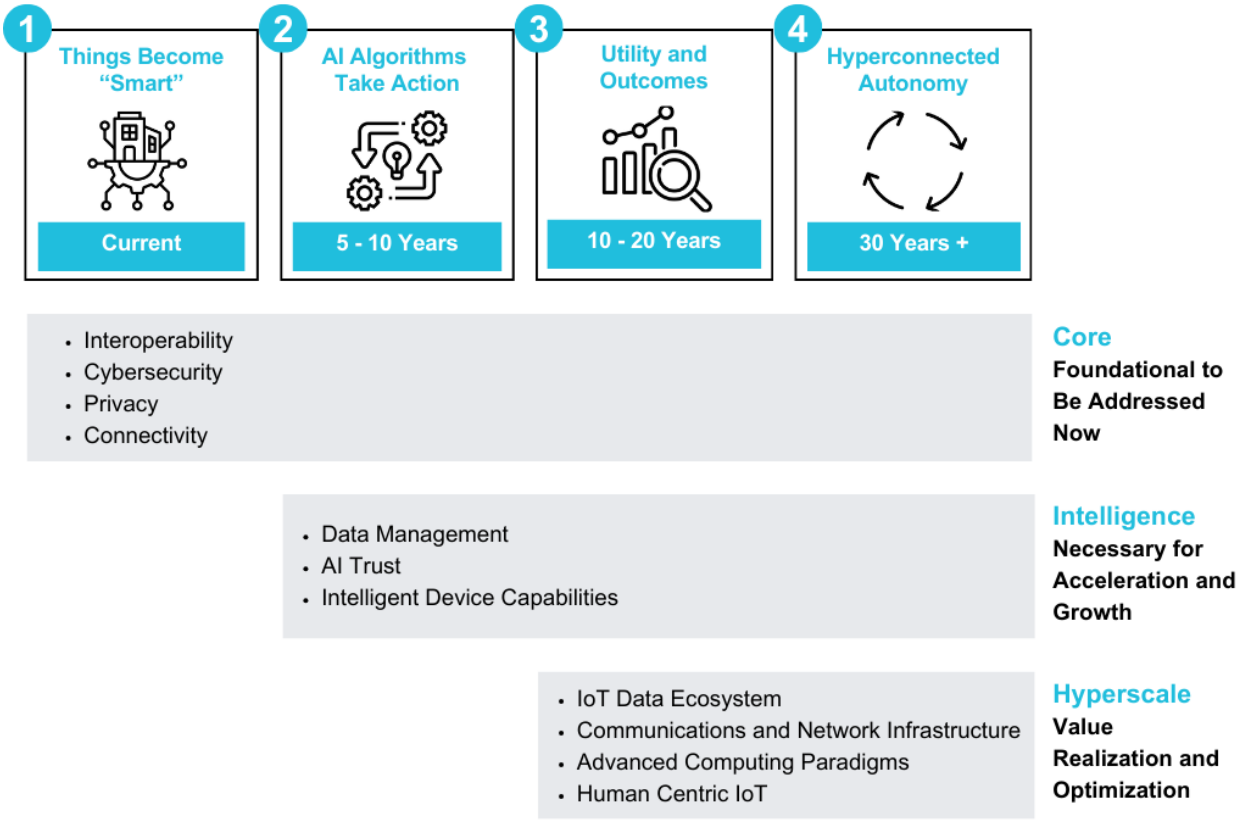


Figure 8-3: Four Stage IoT Evolution

For each gap category, the possible opportunities considered are organized into the five groups as shown in the Opportunity Framework in Figure 8-2 The remainder of this subsection discusses government opportunities from the perspective of each of the categories.

8.3.1. Government opportunities: Core gaps

The core category represents foundational IoT technology infrastructure gaps that should be addressed in the near term and are essential for the function and operation of IoT. The core IoT technology infrastructure gaps include the lack of interoperability, cybersecurity, privacy and connectivity. Possible areas of action, aligned to the opportunity framework, are highlighted below in Figure 8-4.

	Possible Government Opportunity				
IoT Gap (Core)	Develop Technology	Commercial enablement	Facilitate Market Adoption	Lead by Example	Broaden Economy wide Benefits
Inter-operability	Research	Standards Testbeds Partnerships	Promotion Grants	Procurement	

© Strategy of Things, 2025. All rights reserved.

	Possible Government Opportunity				
IoT Gap (Core)	Develop Technology	Commercial enablement	Facilitate Market Adoption	Lead by Example	Broaden Economy wide Benefits
Cybersecurity	Research	Partnerships Standards	Promotion	Procurement Policies	Regulations Workforce Development
Privacy	Research	Standards Partnerships	Promotion	Procurement Policies	Legislation Regulations Workforce Development
Connectivity	Research	Infrastructure Policy	Promotion Grants	Procurement	Regulations

Figure 8-4: Core Gaps: Government Opportunities

8.3.1.1. Interoperability

This research identified the lack of interoperability as a gap in seven of the nine industries studied. Interoperability challenges reduce the ability of IoT devices to connect, communicate and collaborate with each other and with other systems in the industry ecosystem. Furthermore, interoperability challenges will hinder the scaling and evolution of the future IoT.

Interoperability is a long-running challenge and the federal government has been involved with some of the activities identified in Figure 8-4 at various levels for many years. Achieving interoperability requires a long-term multi-stakeholder effort with active participation from buyers, manufacturers, consultants, academia and government. Some barriers to achieving interoperability include limited focus of standards initiatives, resistance to open and industry consensus standards, regional standards and standards implementation errors and deviations. These barriers are discussed in detail in Section 24.4.1.1.

In addition to the general areas of opportunity shown in Figure 8-4, there are also select opportunities for acceleration. Some examples include:

- **Specification of interoperability needs in infrastructure and related grants.** Billions of dollars of "once in a lifetime" grants, arising from the Bipartisan Infrastructure Law, the Inflation Reduction Act and the CHIPS Act are available to industry and communities. These federal grants represent opportunities for the federal agencies to specify and incorporate IoT systems and include provisions to consider those solutions and technologies that are built to industry consensus and open standards. (Facilitate Market Adoption)
- **Specify interoperability requirements for IoT solutions for internal procurements.** The federal government has significant buying power and procures billions of dollars of products and services every year for use in agency operations. The federal government would do well to consider incorporating interoperability requirements for solutions and technologies that are built to industry-consensus and open standards. (Lead by Example)

© Strategy of Things, 2025. All rights reserved.

- **Research the use and risks of Artificial Intelligence to facilitate interoperability.** AI can assist in establishing semantic interoperability by its algorithms understanding the meaning of data elements. Ontology-based approaches, where AI models understand the relationships between different concepts, can be used to map and align data schemas, enabling seamless communication between systems. AI can help translate communication protocols between different systems, enabling different protocols to effectively communicate and exchange information. AI-powered systems can dynamically adapt to changes in the environment or data formats, ensuring continuous interoperability even as systems evolve. (Research)

8.3.1.2. Cybersecurity

This research identified cybersecurity as a gap, appearing in four of the nine industries studied and frequently mentioned as an area of concern in the remaining five industries. Lack of sufficient cybersecurity protections can lead to operational disruptions, loss of sensitive data and compromised IoT and system operation. These impacts are amplified as IoT systems are increasingly integrated into the economy, leading to a loss of trust and resistance to adoption and scaling by owners and users.

Cybersecurity concerns and issues are a long-running challenge experienced in many industries. It is difficult to fully eliminate cybersecurity risks for several reasons. There is no "one size fits all" approach because IoT devices and systems are diverse and heterogeneous. Devices are resource constrained and have limited ability to implement robust measures. Threats are continuously evolving. Other factors include large and growing numbers of unpatched devices, the continued use of legacy systems, interoperability issues, a lack of standardized security protocols and human factors. These barriers are discussed in detail in Section 24.4.1.2.

Cybersecurity is a long-running challenge and the federal government has been involved with some of the activities identified in Figure 8-4. In addition to the general areas of opportunity in Figure 8-4, there are also select opportunities for acceleration of cybersecurity protections. Some examples include:

- **Specification of cybersecurity provisions in smart infrastructure and related grants.** The previously discussed grant programs (BIL, IRA, CHIPS) represent an opportunity for the government to specify cybersecurity measures and requirements. (Facilitate Market Adoption)
- **Grow the cybersecurity workforce.** The National Cyber Workforce Education Strategy[246] was released in 2023 although implementing it will take time and funding. In addition, the previously discussed grants do partially support the development of a cybersecurity workforce. (Economy wide Benefits)
- **Specify cybersecurity requirements for IoT solutions for internal procurements.** The federal government should consider incorporating or expanding cybersecurity requirements and provisions into the procurements. (Lead by Example)
- **Research the use and risks of Artificial Intelligence to facilitate cybersecurity.** In addition to analyzing vast amounts of data to identify suspicious patterns and anomalies,

[246] "National cyber workforce education strategy," Office of the National Cyber Director, The White House, July 31, 2023. Link

© Strategy of Things, 2025. All rights reserved.

AI has the ability to predict potential vulnerabilities and threats before they are exploited. (Research)

- **Fund research in advanced cybersecurity methods.** Representative examples include lightweight encryption algorithms, alternative approaches to cryptography such as "friendly jamming" that works with resource constrained devices, lightweight quantum safe algorithms, integration of blockchain with IoT and the use of privacy enhancing technologies in IoT. (Research)

8.3.1.3. Privacy

Privacy concerns appeared as a gap in four of the nine industries. Privacy challenges include the unauthorized collection, storage and use of data, unauthorized disclosure of private information through theft and data sharing, as well as the misuse of private information. These challenges are exacerbated as IoT systems are increasingly integrated into the economy, leading to a loss of user trust and resistance to IoT adoption and scaling. Figure 8-4 below shows some areas where the federal government has an opportunity to address the privacy gap.

Privacy protection is a complex, long-running challenge and is difficult to fully achieve for several reasons. These include a fragmented regulatory environment with state level (e.g., California CCPA) and federal level industry (e.g., HIPAA) regulations, continuing cybersecurity attacks, businesses incentivized to collect and use personal data, inadequate privacy consent mechanisms and the potential to deanonymize private data through aggregation. These barriers are discussed in detail in Section 24.4.1.3

Privacy protection is a top-of-mind issue and the federal government has a variety of ongoing activities and initiatives in some of the areas of opportunity shown in Figure 8-4. However, there are also select opportunities for acceleration. Some examples include:

- **Enact national comprehensive privacy legislation.** Privacy laws in the United States are a mix of federal and state laws covering specific topics.[247] At the federal level, there are several: HIPAA (healthcare), FCRA (credit), FERPA (education records), GLBA (consumer financial), ECPA (communications), COPPA (child data), VPPA (VHS rentals) and the FTC Act (app/website privacy). At the state level, three states, California, Colorado and Virginia, have comprehensive data privacy laws. Enacting a national level comprehensive privacy law or legislation promises to reduce confusion, simplify compliance and alleviate IoT privacy concerns. (Economy wide Benefits)
- **Promote and advocate for Privacy by Design.** This concept emphasizes integrating privacy into products, services and system designs from the start. While privacy-by-design is incorporated as one of three core principles of the FTC privacy framework[248] and its principles inform the NIST privacy framework,[249] adoption of privacy by design

[247] "The state of consumer data privacy laws in the U.S. (and why it matters)," T. Klosowski, Wirecutter, September 6, 2021. Link

[248] "Privacy By Design and the New Privacy Framework of the U.S. Federal Trade Commission," E. Ramirez, Public Statement, United States Federal Trade Commission, June 13, 2012. Link

[249] "The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management", U.S. National Institute of Standards and Technology, January 2020. Link

© Strategy of Things, 2025. All rights reserved.

concept in the United States is not widespread. Many organizations still prioritize functionality and convenience over privacy considerations, especially in sectors where data-driven decision-making and targeted advertising are prevalent. Additionally, smaller organizations with limited resources may struggle to implement comprehensive privacy by design practices. While national comprehensive privacy legislation is being considered, ongoing efforts are needed to raise awareness, provide guidance and incentivize organizations to prioritize privacy in their operations. (Commercial enablement)

- **Fund and conduct technology research to address IoT privacy challenges.** While legislation and privacy by design may address some privacy challenges, research in new technologies is required due to the growth and integration of IoT devices into the economy and civil society. Research is essential to develop innovative technologies and methods, including advanced encryption techniques, privacy-preserving data analytics, decentralized architectures and user-centric privacy controls tailored to the unique challenges posed by IoT systems. These technologies are required to foster trust among users, encourage widespread adoption of IoT technologies and realize the potential of the IoT ecosystem while maintaining user privacy and autonomy. (Research)

8.3.1.4. Connectivity

IoT and other smart equipment rely on connectivity to send their data to edge servers and remote data centers in the cloud for processing and storage. While connectivity challenges were identified in two of the nine industries studied, the lack of connectivity availability in rural and underserved communities affects other industries operating in those areas. For example, the lack of connectivity prevents the development of IoT enabled healthcare services in those communities. For this reason, connectivity challenges have been included as a core gap. Figure 8-5 below shows some areas where the federal government has an opportunity to address the connectivity gaps.

Connectivity challenges are multi-dimensional in nature and challenging to solve due to various factors, including requiring substantial infrastructure investment, a no “one size fits all” approach, market economics, available funding and incentives, “last acre” coverage and spectrum. These barriers are discussed in detail in Section 24.4.1.4.

Connectivity availability is a top-of-mind issue and the federal government has a variety of ongoing activities and initiatives in some of the areas of opportunity shown in Figure 8-4. However, there are also select opportunities for acceleration. Some examples include:

- **Service availability.** Ensuring reliable and ubiquitous connectivity remains a challenge, particularly in remote or rural areas where private carriers are not present. Policymaking opportunities should focus on ubiquitous connectivity coverage, expanding both broadband infrastructure and affordability of service. The Bipartisan Infrastructure Law provides a unique opportunity and funding to close the “digital divide.” (Commercial enablement, Facilitate market adoption)
- **Spectrum.** IoT devices operate on wireless networks, competing for limited radio frequency spectrum. While spectrum challenges are less of an issue in rural communities, they are critical in dense urban areas. Spectrum allocation is a critical issue, as the increasing number of IoT devices exacerbates congestion and interference problems.

© Strategy of Things, 2025. All rights reserved.

Efficient spectrum management and allocation policies are needed to accommodate the growing demand for IoT connectivity while minimizing interference and ensuring fair access for all users. (Commercial enablement)

- **Technology.** To support the further scaling and evolution of IoT, continued research is needed to develop new connectivity technologies and management approaches. Some areas of research include spectrum-efficient communication technologies, innovative network architectures, security and privacy enhancements and interoperability standards. (Research)
- **Regulatory Frameworks and Standards.** Regulatory frameworks and standards promote the development and deployment of IoT connectivity technologies, foster innovation and safeguard public interests. Regulatory agencies such as the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA) enact rules and standards to ensure spectrum efficiency, interoperability, security and privacy in IoT networks. (Commercial enablement)
- **International Collaboration and Coordination.** International collaboration and coordination efforts are essential to harmonizing spectrum policies, promoting global interoperability standards and addressing cross-border challenges in IoT connectivity. Through participation in international forums, conferences and standards bodies, the government collaborates with international partners to develop common frameworks, resolve regulatory conflicts and facilitate seamless connectivity for IoT devices worldwide. (Commercial enablement)

8.3.2. Government opportunities: Intelligence gaps

The Intelligence category represents key IoT technology infrastructure gaps that should be addressed to enable an intelligent and autonomous future IoT in the near to mid-term. The Intelligence IoT technology infrastructure gaps are data management, AI trust and intelligent device capabilities. Possible areas of action, aligned to the opportunity framework are highlighted in Figure 8-5.

© Strategy of Things, 2025. All rights reserved.

	Potential Government Opportunities				
IoT Gap (Stage 2)	Develop Technology	Commercial enablement	Facilitate Market Adoption	Lead by Example	Broaden Economy wide Benefits
Data Management	Research Technology Transfer	Partnerships Standards Pilots Testbeds			
AI Trust	Research Technology Transfer	Partnerships Standards Pilots Testbeds Sandboxes Infrastructure Policy	Promotion Tax incentives	Procurement	Workforce Development Regulations
Intelligent Device Capabilities	Research Technology Transfer	Partnerships Standards Pilots Testbeds Infrastructure	Promotion	Procurement	

Figure 8-5: Intelligence Gaps: Government Opportunities

8.3.2.1. Data Management

Adequate data management was identified as a gap in two industries. However, in its robust form, it is also an enabler for the three other industries where the use of artificial intelligence was identified as a gap. As IoT scales, the ability to manage the data created is critical. Robust data management capabilities help unlock the value of IoT by enabling massive amounts of data to be collected, processed, stored and analyzed. Without these capabilities, IoT deployments face challenges such as data silos, scalability issues and compromised data integrity. Furthermore, robust data management is foundational for artificial intelligence systems use.

Robust data management ensures the availability, accessibility, quality and security of data, laying a foundation for AI applications to generate effective decisions and relevant outcomes. Moreover, well-managed data facilitates the development of more accurate and reliable AI systems, leading to better predictions, recommendations and automation across various domains. Figure 8-5 shows some areas where the federal government can address the data management gaps.

Addressing data management challenges for IoT is not easy and is complicated by a number of factors. These include exponential growth in data volume and velocity, privacy considerations, cybersecurity factors, interoperability concerns and regulatory compliance requirements. These barriers are discussed in detail in Section 24.4.2.1

© Strategy of Things, 2025. All rights reserved.

There are extensive existing industry efforts to develop commercially available market solutions from a variety of data management solution providers. However, the convergence of AI with IoT and the future pervasiveness across the economy creates a sense of urgency to accelerate the development of "beyond big data" data management approaches and technologies for users and researchers. Given the strategic importance of data management to IoT, the federal government would do well to focus on research and commercialization enablement efforts around novel and innovative "beyond big data" technologies and architectures that support the future of a scaled up, hyperconnected, decentralized and autonomous IoT ecosystem (Figure 8-5). Some examples and representative areas for federal research to augment and accelerate industry efforts, discussed previously in Section 23.2.1, may include, but are not limited to:

- **Scalable and efficient data storage.** Innovative and more effective approaches are needed to manage the increasing volume of data. For example, distributed storage architectures, compression techniques and data deduplication (removing duplicate data) methods to improve storage efficiency.
- **Real-time data processing.** Research into ways to enhance real-time and energy efficient processing of IoT-generated streaming data, including advanced algorithms, edge computing and in-memory processing techniques is relevant.
- **Security and privacy.** Research into methods and approaches to protect a diverse set of data that is increasingly stored on distributed devices, mobile and edge systems, as well as data that are streamed to other systems is important. Opportunities to consider include encryption techniques, access control mechanisms and privacy preserving analytics.
- **Data quality assurance methodologies.** Approaches are needed to ensure the accuracy and reliability of IoT-generated data, such as developing calibration techniques for sensors, anomaly detection algorithms and data validation processes.
- **Data governance.** Data oversight and management is increasingly important as separate parties own their data which are subject to a variety of industry and government regulations, such as HIPAA (healthcare), and Gramm-Leach-Bliley Act (consumer financial information). New approaches and mechanisms are needed to govern changes as data are increasingly distributed and decentralized.
- **Lifecycle management of IoT data.** As new IoT applications emerge and industry adoption increases, the management of the distributed and decentralized data, from attribution, traceability, collection, storage, processing, analysis and archiving becomes more important.
- **Data fabric architectures.** As data sources and creators are increasingly decentralized and distributed on a massive scale, future scalable architectures to interconnect and access this data are required.

8.3.2.2. Artificial Intelligence Trust

Our research identified the lack of use of artificial intelligence as a gap in insurance, retail, healthcare and transportation and logistics. It is also an important capability to have in agriculture, smart cities and renewable energy.

The integration and use of AI algorithms with IoT devices and systems enables users to extract insights from the collected data. The use of AI in this capacity enables IoT devices to analyze

© Strategy of Things, 2025. All rights reserved.

data streams in real-time, identify patterns, predict outcomes, make intelligent decisions and take autonomous action without human intervention. Further, where employed, AI-driven analytics enable continuous learning and adaptation, allowing IoT systems to evolve and improve over time, leading to more accurate predictions and better resource utilization.

Despite its transformational potential, establishing trust in AI-enabled IoT systems is complex due to a variety of technical, human and societal factors. Some major complicating factors include human reluctance and resistance, unclear and uncertain accountability and liability, lack of standardized guidelines for AI development and deployment and ethical dilemmas from AI generated outcomes. These barriers are discussed in detail in Section 24.4.2.2

Our research and analysis identified broad areas where the federal government has the potential to facilitate trust in artificial intelligence. Figure 8-5 shows broad areas where the federal government can address AI trust challenges and includes:

- **Research and development**. As AI technology advances across various fronts, continued research is necessary to maintain global AI leadership and ensure the development of safe, ethical, fair, transparent and explainable AI. (Research)
- **Governance and Oversight.** The federal government should research, anticipate and establish effective governance frameworks and structures to oversee AI adoption, ensuring transparency, accountability and ethical use. (Research)
- **Privacy and Security.** AI relies on a continuous pipeline of data for training and model development. Data collected from IoT systems may be subject to privacy concerns and restrictions. Balancing AI-driven insights with privacy protections and limiting unauthorized use of data is a key challenge. (Commercial Enablement)
- **Bias and Fairness.** AI algorithms may lead to results that are inaccurate, biased, irrelevant or discriminatory. Addressing bias, fairness and ethical use is a key challenge. (Research)
- **Workforce Considerations.** The use of AI may displace jobs as well as create new roles for users in which human-AI collaboration is essential. In addition, development of a skilled AI workforce is necessary to accelerate innovation and deliver economic and societal benefits. (Economy wide Benefits)
- **Interagency Coordination.** Coordinating efforts across federal agencies to promote consistency and sharing is important to policy development. (Economy wide Benefits)
- **International Cooperation.** AI cuts across international borders. Collaborating with other nations to set global standards, prevent misuse and address cross-border challenges is important. (Commercial Enablement)
- **Regulatory Framework.** AI use is advancing into all aspects of industry, government and society. Crafting policies that encourage innovation while safeguarding against the possible risks posed by AI applications is important. (Economy wide Benefits)

8.3.2.3. Intelligent device capabilities

Our research identified limited device capabilities as a gap in enabling and supporting the ability of IoT devices to process and analyze data. On-device and edge processing of data is increasingly common and is required for applications that are autonomous, latency sensitive or

© Strategy of Things, 2025. All rights reserved.

operate in an area with unreliable service. Other applications requiring on-device and edge processing include IoT device swarms and ambient IoT use cases that require contextual information obtained by communicating with other nearby devices.

Section 6.2.3 discussed some specific capability gaps. This includes the need for AI-ready processors capable of supporting complex applications while minimizing power consumption and efficient AI algorithms capable of operating on resource constrained devices.

Developing IoT devices capable of supporting AI is challenging due to the physical limitations of semiconductors and microprocessors, complex programming requirements and high upfront development costs. These barriers are discussed in detail in Section 24.4.2.3

While there are existing commercial development efforts and solutions for the development of intelligent devices from many semiconductor and microprocessor suppliers, these efforts are focused on short term objectives. To enable and support a future scaled up, hyperconnected and autonomous IoT ecosystem, the federal government has an opportunity to focus on the research and commercial enablement of advanced approaches. Our research and analysis identified broadly areas where the federal government can facilitate the development of intelligent devices as shown below in Figure 8-5. Some examples include:

- **Research and Development.** One focus for the federal government would be to fund and perform basic and applied research on the enabling technologies and infrastructure needed in the future state. These areas of research may not necessarily be an area of focus for industry as they are focused on nearer term research investments and outcomes. (Research)
- **Leverage Tech Hubs to innovate.** The federal government has established thirty-one "tech hubs" across the country. These tech hubs bring together private industry, state and local governments, institutions of higher education, labor unions, tribal communities and non-profit organizations"[250] to make transformative innovation investments. (Research, Commercial enablement)
- **Incentivize Industry Collaboration.** There are government incentives for existing federal programs. Here, the government can and does provide similar incentives for industry players to collaborate with research institutions and startups on IoT R&D projects. For example, the NSF Regional Innovation Engines facilitate the development of ecosystems that collaborate on innovation around certain critical areas.[251] Available methods include tax incentives, grants, or public-private partnership programs that encourage knowledge sharing and technology transfer. (Commercial enablement, Research)

[250] "FACT SHEET: Biden-Harris Administration Announces 31 Regional Tech Hubs to Spur American Innovation, Strengthen Manufacturing and Create Good-Paying Jobs in Every Region of the Country," Fact Sheet, The White House, October 23, 2023. Link

[251] "About NSF Engines." U.S. National Science Foundation. Link

© Strategy of Things, 2025. All rights reserved.

8.3.3. Government opportunities: Hyper-Deployed gaps

The future IoT-enabled economy and society may contain billions of interconnected devices working autonomously in a secure and trusted manner. To realize the Hyperconnected Autonomy future described in Section 4.2.1 today's communication networks and infrastructure must evolve to support real-time autonomy and complex IoT applications at scale, become fault tolerant and resilient and be able to defend and heal against security threats.

The technological developments seen as necessary to support this future state IoT infrastructure are discussed in detail in Section 23. Key desired elements of these currently unavailable technologies are represented as gaps that need to be addressed to support a hyper-deployed IoT ecosystem. These technology infrastructure gaps could be addressed by improvements in the IoT data ecosystem, communications and network infrastructure, advanced computing paradigms and human centric IoT systems.

Developing the next-generation technology infrastructure to support the hyperconnected and autonomous state of IoT is challenging for a variety of reasons. This includes complexities in the development of advanced technological innovations, high and risky investments with uncertain returns, lack of skills and resources and lagging regulatory actions and standards. These barriers are discussed in detail in Section 24.4.3

Addressing these gaps requires forward looking actions by the federal government. Figure 8-6 below identifies some areas of opportunity for the federal government.

	Potential Government Opportunities				
IoT Gap (Stages 3 and 4)	**Develop Technology**	**Commercial enablement**	**Facilitate Market Adoption**	**Lead by Example**	**Broaden Economy wide Benefits**
IoT data ecosystem	Research Technology Transfer	Partnerships Standards Pilots Testbeds Infrastructure Policy	Promotion		Workforce Development
Communications and network infrastructure	Research Technology Transfer	Partnerships Standards Pilots Testbeds Infrastructure Policy	Promotion	Policies	Workforce Development

© Strategy of Things, 2025. All rights reserved.

	Potential Government Opportunities				
IoT Gap (Stages 3 and 4)	**Develop Technology**	**Commercial enablement**	**Facilitate Market Adoption**	**Lead by Example**	**Broaden Economy wide Benefits**
Advanced computing paradigms	Research Technology Transfer	Partnerships Standards Pilots Testbeds Infrastructure Policy	Promotion	Policies	Workforce Development
Human centric IoT	Research Technology Transfer	Partnerships Standards Pilots Testbeds Infrastructure Policy	Promotion	Policies	Workforce Development Regulations

Figure 8-6: Hyper-Deployed Gaps: Government Opportunities

Key opportunities and considerations for the federal government to address challenges of building a future IoT technology infrastructure include but not limited to:

- **Funding and performing research.** The technological innovations to enable the Hyperconnected Autonomy future may not yet exist although they may be envisioned by a scientist and experimented with at bench scale or at an early pilot stage. A key role for the federal government is to continue supporting scientific research, helping to establish a vision and providing supportive funding to create enabling technologies and infrastructure for IoT.

  As a general policy prescriptive, federal investments have previously and currently helped to accelerate development in research areas that may not be undertaken by private industry given their focus on near term returns, alignment with existing technology and current intellectual property portfolios. (Research)
- **Enable supporting infrastructure.** The future state of IoT relies on a modern communications and computing infrastructure to support AI and autonomous IoT workloads at scale. These applications impose high performance requirements for infrastructure as they need to support high throughput, low latency traffic and distributed and scalable high performance computing resources. Without this infrastructure, the full benefits of the hyperconnected autonomy future will not be realized.

  The opportunities for government involve facilitating infrastructure buildout including spectrum allocation, funding, public-private partnerships and policies and initiatives to facilitate access and availability. One example is the federal government's role in enabling FirstNet, a dedicated first responder network. (Commercial enablement)

© Strategy of Things, 2025. All rights reserved.

- **Development of policies and regulations for an emerging future.** While innovative and emerging technologies often bring transformational benefits, they are often accompanied by unforeseen outcomes. A key government activity is the development of frameworks, policies and regulations to facilitate innovation and beneficial outcomes.

  Emerging technologies, however, represent a challenge for policymakers because "they don't know what they don't know." One acceleration opportunity for the federal government to undertake is the development of regulatory-innovation sandboxes that allow these innovations and policies to be tested and evaluated. This facilitates understanding, fosters industry-government collaboration and informs the development of effective policies and regulations.

  Another area of opportunity for government action is research on the ethical, social and cultural implications of advanced and autonomous IoT technologies to inform on policy and regulation development. Topics may include issues related to privacy, surveillance, discrimination, bias and inequality. (Commercial enablement)

- **Build the future workforce.** The evolution of IoT requires a workforce capable of supporting, using and benefiting from hyperconnected and autonomous applications. While there are concerns that the proliferation of AI and autonomous applications will lead to job losses, interested parties understand that the new jobs created will require human-AI collaboration. For example, people and cobots work together today in a limited capacity to assemble and produce products.[252] Section 6.3.4 discusses the need to design systems and solutions for human-AI collaboration.

  In anticipation of human-AI collaboration at scale, there exist opportunities for the federal government to consider strategies, policies investments and other actions and initiatives that build capability and skills in the future workforce. (Commercial enablement)
- **Support standards development.** Standards and interoperability are critical to the realization of the hyperconnected and autonomous future state IoT. The federal government supports standards development through research, development of frameworks, convening of stakeholders and facilitating industry cooperation to develop consensus standards.

  In addition, the federal government engages in multilateral forums, international organizations and bilateral agreements to harmonize standards, share best practices and coordinate regulatory approaches. While the federal government's approach to standards is "industry-leads, government supports", development of standards for the hyperconnected IoT autonomy provides opportunities for government to play a more active role in matters pertaining to safety, liability and other major factors. (Commercial enablement)

[252] "Cobots Improve Productivity, Shifting Workers Away From Dirty, Dangerous and Dull Jobs", J. Campbell, International Society of Automation, November/December 2019. Link

© Strategy of Things, 2025. All rights reserved.

8.4. Implications for government leaders and policymakers

In many cases, such as with core and intelligence gaps, there are significant and existing industry efforts to address the gaps identified for each of the three categories. For example, there are numerous industry efforts supporting Standards Development Organizations to develop a variety of standards across many market sectors. In addition, industry is developing commercial solutions to address a variety of gaps. However, many of these gaps are too broad, complex and challenging for industry, academia and government to address on their own. Each party plays a vital and complementary role.

For instance, standards are a key requirement for interoperability. The federal government supports standards development by performing the pre-standards research and building the underlying science needed for industry to define and develop the requisite standards. Once done, industry then builds consensus standards based on this groundwork.

At the same time, as IoT evolves, the government could consider conducting groundwork and complementary research to enable future IoT technologies, so that industry can take the next steps. In other cases, federal research may produce technological advancements that offer the potential to address these gaps in new and more novel ways. The federal government may have the opportunity to invest in research to understand and develop these novel approaches. Depending on the origin of the scientific breakthroughs there may be opportunities for federal technology transfer and licensing to industry to continue its development and commercialization.

Finally, industry may not address certain gaps because they are outside their short to mid-term priorities, may lack the expertise or capabilities or that may conflict with their own proprietary approaches. Those situations may be seen as “market failures” that the federal government then has an opportunity to address through research.

8.4.1. Government opportunities

The framework in Section 8.2 identified the five areas of government opportunities to address gaps. It lists specific tools, capabilities and other means that the federal government has to address these gaps. The list is not comprehensive but is intended to be representative. The specific gap, the industries it affects, and the state of maturity of the technologies, will determine the specific combination of these means that are deployed to address the gap. Section 8.3 identified examples of potential means that the federal government can use to address the core, intelligence and hyper-deployed gaps.

While these means and capabilities are not new and have been used by many federal agencies for a variety of purposes, government leaders and policy makers would do well to consider these capabilities as part of a broader portfolio of possible actions to provide a whole-of-government approach to more effectively address IoT technology infrastructure gaps. Some key reasons and support for such an approach follow:

IoT faces a combination of technology and non-technology challenges. Both must be addressed to facilitate its continued development, adoption, operation and value realization.
IoT faces a variety of technical and non-technical challenges. Some challenges, such as cybersecurity vulnerabilities and risks, require technical responses. Other challenges, such as

© Strategy of Things, 2025. All rights reserved.

resistance to adoption and lack of a digital workforce, are major non-technical barriers hindering adoption and scaling. Another major area of non-technology challenges are regulations, including those at the federal, state and local levels, which impact what IoT can do, how it does it, and who may use and operate it.

Other challenges have both technical and non-technical aspects. For example, while the development of technical standards provides the foundation for interoperability, some users employ technologies with proprietary approaches because it "locks in" customers and yields higher profits.

While the federal government has a variety of means to address different types of challenges, the government often applies them independently in silos with limited coordination. For example, while the federal government participates in a variety of technical activities to support industry development of standards, the federal government does not always leverage its significant buying power in procurements to specify the purchase of solutions that incorporate those standards. This "disconnect" by the federal government sends a signal to industry that standards are not an important purchasing consideration, and may result in solution providers becoming reluctant to adopt the standards that can lead to interoperable systems.

Government leaders and policymakers addressing IoT challenges have an opportunity to consider a holistic approach that addresses both the technology and non-technology aspects. Initiatives that address only the technology challenges without simultaneously addressing the non-technology issues will not lead to the intended outcomes.

IoT technology infrastructure gaps fall into three categories. Different strategies and approaches are needed to address each category.

There is not a "one size fits all" approach to addressing IoT technology infrastructure gaps. IoT is in a continuous state of evolution, driven by a variety of technology, market and regulatory forces. This evolution creates gaps that fall into three distinct categories.

Each gap category addresses unique needs and requires specific approaches. Core gaps, concerned with the foundational capabilities that hinder the short and mid-term IoT development and adoption, are well-aligned for industry to address to support their commercial interests. In this category, the role of government is more strategic and targeted.

For example, while the federal government has traditionally conducted the pre-standards research and science to enable industry to develop consensus standards, interoperability issues continue to be a major and long running core gap hindering IoT adoption and evolution.

In addition to continuing to support standards development efforts, the federal government is most effective augmenting industry efforts by addressing in general the things industry isn't able to do. One such opportunity is investigating emerging novel methods, such as the use of AI, to facilitate interoperability between incompatible devices. Furthermore, as IoT continues its evolution, continued research is needed to address broader and more massive systems to systems interoperability gaps to support the future hyperconnected economy.

In contrast, the federal government is well positioned to play a heavier research role in addressing hyper-deployed gaps. This category of gaps hinders the future IoT-enabled economy and society, teeming with billions of interconnected devices working autonomously and collaboratively. Industry, with its focus on short and mid-term priorities, does not have the

© Strategy of Things, 2025. All rights reserved.

interest nor the capabilities to address these gaps. Government investment, as a strategy, is well-suited for addressing hyper-deployed gaps because it involves the development of transformational technologies and approaches that are forward looking and high-risk.

However, IoT is not one technology, but a diverse set of underlying technologies at various stages of maturity. At any particular point in the evolution of IoT, the roles of industry, academia and government will vary. A key driver of the category approach is to consider the suitability of government to undertake and address the gaps. Some gaps, such as interoperability and cybersecurity, are so broad, complex, and challenging that no one group can address these on their own.

Other gaps, such as the hyper-deployed gaps, have no "owners" and necessitate that the federal government take a leading role. Still other gaps are addressed in multiple ways because the technology is still evolving. The federal government could consider addressing gaps that are not being undertaken by industry, those that involve high risk or novel approaches that industry lacks the expertise or capabilities to address and those that stimulate research where findings may later be transferred to industry for further development and scaling.

Government leaders and policymakers could consider the three categories of IoT technology infrastructure gaps as three portfolios of research opportunities. Each portfolio of gaps ought to have an overall research strategy and approach, and corresponding research objectives and outcomes. The federal government does have a wide range of expertise, resources and capabilities that may be directed to effectively address these gaps, within its portfolio strategy.

The federal government has a comprehensive set of capabilities that is well suited to support a whole-of-government portfolio approach to address the gaps hindering IoT. Our study has identified and categorized the federal government capabilities to address IoT gaps into a framework with five broad areas. These capabilities, offered through various agencies, form a portfolio of capabilities. Each IoT technology infrastructure gap can be addressed by a specific combination of these capabilities within this portfolio. Furthermore, each gap category has a strategy or approach attached that broadly determines what government portfolio capabilities should be utilized.

For example, hyper-deployed gaps are forward-looking and are concerned with the later stages of IoT evolution. As a result, the most relevant identified government capabilities are focused on research (technology development) and depending on the state of the technology, commercial enablement. In contrast, most current needs in the core gaps span the full range of government capabilities across the five broad areas.

Government leaders and policymakers would do well to consider taking a portfolio approach to addressing the IoT technology infrastructure gaps. The portfolio approach considered three perspectives: technology, economics and government. The technology perspective recognizes the diverse types and nature of the gaps, as well as the technology's maturity along the IoT evolution cycle. The economic model provides information on the indicative allocations (or percentages) across the industries to address the gaps that will maximize outcomes for the broader economy. The actual uses of the funding allocations are informed by the specific federal capabilities available and needed to address the IoT gaps with those investment allocations.

© Strategy of Things, 2025. All rights reserved.

This portfolio approach recognizes that multiple gaps need to be addressed simultaneously and the nature of those gaps varies depending on the evolutionary stage of IoT and its underlying technologies. In addition, some investments may be used to address gaps that may be more difficult to address than others and some gaps and industries may require more investments than others. Furthermore, the proposed set of actions undertaken by the federal government to address these gaps will vary depending on the nature of the gap, the roles of industry and academia, and the capabilities and resources available to address it.

An investment portfolio approach informs IoT research funding priorities and offers the potential to maximize economic outcomes on an economy wide basis.
Technology infrastructure gaps hinder the continued development, adoption and operation of IoT in the industries studied. While the federal government has made research investments to address some aspects of these gaps, those investments are made on an industry-by-industry basis.

This study offers an economic analysis that determined the economic outcomes of a nominal $10 million investment in addressing specific IoT technology infrastructure gaps across nine industries. Economic models from the study show that a $10 million federal investment in addressing the IoT technology infrastructure gaps offers the potential to generate an indicative 55 to 89 times in revenue and 12 to 128 times in economic surplus.

The analysis also showed an optimum distribution, based solely on economic considerations, of that investment across the nine industries based on the findings from the integrated survey, interview and desk research data. For example, in the core gap of interoperability the research results led our economic model to allocate 36.8% of that investment to healthcare followed by 14% to agriculture and 13% to manufacturing.

Government leaders and policymakers would benefit from considering a portfolio approach to address IoT technology infrastructure gaps. This approach offers a more holistic perspective to making informed allocations of limited research budgets, reduces risk, and maximizes potential economic outcomes from these investments.

However, for the government to implement a portfolio approach would require close coordination, collaboration, governance and management across and between federal agencies. With their agency specific missions and unique needs, coordination and management among agencies promises to be challenging. The potential central management and coordination of this portfolio may be done by an interagency group, such as the Networking and Information Technology Research and Development (NITRD) program, or a potential central and broader federal IoT organization[253] to be established.

While the study examined only nine industries and focused on IoT, the approach developed in this study for IoT has the potential to be replicated elsewhere to assess the economic benefits of technology investments in other emerging technologies, such as AI.

Further study

[253] In 2024, a FACA, the IoT Advisory Board recommended the formation of a national IoT office. “Report of the Internet of Things (IoT) Advisory Board (IoTAB)”, October 2024. Link

© Strategy of Things, 2025. All rights reserved.

The study developed an approach to address IoT technology infrastructure gaps that may be addressed by public sector investment. The approach could be extended to include other industries and strengthened to include more detailed economic and social impacts.

Managing the research portfolio across industries and the economy necessitates the ability to measure and monitor the economic benefits of these investments. A coordinating and collaboration structure and organization is required to design, implement and operationalize the proposed portfolio.

Finally, while the study examined nine industries and focused on IoT, the approach developed in this study has the potential to be replicated elsewhere to assess the economic benefits of public sector technology investments in other emerging technologies, such as AI.

© Strategy of Things, 2025. All rights reserved.

9. Recommendations

Based on a review of the gaps, the economic analysis and the portfolio of possible opportunities for the federal government to address these gaps, we make the following six recommendations to address the high level findings and infrastructure gaps identified in the research.

Recommendation 1. Consider research investments for the following IoT technology infrastructure gaps.

The Internet of Things is not one technology, but a diverse set of technologies at various stages of development and maturity. Based on the research findings and economic analysis, the federal government could consider research investments and initiatives to address IoT technology infrastructure gaps in the following areas:

Core gaps

- Interoperability
- Cybersecurity
- Privacy
- Connectivity

Intelligence gaps

- Data management
- Trust in AI
- Enablement of intelligent devices

Hyper-Deployed gaps

- IoT data ecosystem
- Communications and network infrastructure
- Advanced computing paradigms
- Human centric IoT systems

These gaps are well-suited for federal research investments to address. While there are significant and existing industry efforts to address some of the gaps identified, especially in the core and intelligence categories, many of these gaps are too broad, complex and challenging for industry, academia and government to address on their own.

Federal research investments complement industry and academia efforts to address these gaps. The federal government is well-suited to address research topics that are not undertaken by industry. These “market failure” situations include research that is outside of industry’s short to mid-term priorities. It also includes areas where industry participants lack the expertise or capabilities, as well as areas that may conflict with their own proprietary approaches.

Similarly, as IoT continues to evolve, the government could consider conducting groundwork research to enable future IoT technologies, so that industry can take the next steps. In other

© Strategy of Things, 2025. All rights reserved.

cases, federal research may produce technological advancements that offer the potential to address these gaps in new and more novel ways. The federal government sometimes has the opportunity to invest in research to understand and develop these novel approaches. Depending on the origin of the scientific breakthroughs there may be opportunities for technology transfer and licensing which can then be transferred to industry to continue its development and commercialization.

Recommendation 2. Consider the findings and results in this report to inform federal IoT related research and development, investment, planning and policy considerations from a "whole-of-federal government" perspective. Furthermore, consider using a portfolio management approach to plan, guide and track the direction and implementation of investments and initiatives to address the gaps.

While individual federal agencies have ongoing planning and research initiatives related to IoT in their mission areas, this research takes a broader economywide perspective of IoT. The report has identified a variety of opportunities, challenges and investment areas for IoT across nine of the most impactful and largest industries in the United States. The research takes a current state and forward-looking perspective on IoT technologies and systems.

Government leaders and policymakers would do well to consider taking a "whole of government" portfolio approach to addressing the IoT technology infrastructure gaps. The portfolio approach considered three perspectives: technology, economics and government. The technology perspective recognizes the diverse types and nature of the gaps, as well as the technology's maturity along the IoT evolution cycle. The economic model provides information on the indicative allocations across the industries to address the gaps that will maximize outcomes for the broader economy. The federal government has a portfolio of capabilities and resources to address these gaps. The actual uses of the funding allocations are informed by the specific federal capabilities available and needed to address the IoT gaps with those investment allocations.

Taking a portfolio approach to addressing these IoT technology infrastructure gaps is considered appropriate. This portfolio approach recognizes that the gaps are interrelated, that multiple gaps need to be addressed simultaneously and the nature of those gaps varies depending on the evolutionary stage of IoT and its underlying technologies. In addition, some investments may be used to address gaps that may be more difficult to address than others and some gaps and industries may require more investments than others. Furthermore, the proposed set of actions undertaken by the federal government to address these gaps will vary depending on the nature of the gap, the roles of industry and academia, and the capabilities and resources available to address it. An investment by the public sector in a portfolio of technologies covering the gaps identified in both the core and intelligence categories would likely provide commensurate benefits to the broad U.S. economy.

The portfolio approach is more efficient and brings together a whole-of-government capabilities and expertise to the table to address both technology and non-technology gaps. This approach diversifies the risk associated with any individual investment in IoT infrastructure technology and covers both short and medium to long term investment horizons. In addition to spreading federal research investment across a number of technologies, the investments are also made across a number of industries in a coordinated manner. Under the proposed framework, this

© Strategy of Things, 2025. All rights reserved.

analysis informs where the research spending should be directed to provide an optimal economic benefit for the investment.

Interagency and cross-agency groups, such as the Networking and Information Technology Research and Development (NITRD), would likely benefit from this study and review of the findings to inform and support future IoT related research initiatives. These interagency and cross-agency groups would also benefit from tracking the critical gaps and developing a set of metrics to monitor progress towards closing these gaps.

Recommendation 3. Build on this research by extending the study to additional industries.

This research had a limited scope and examined the IoT technology infrastructure gaps across nine industries. These industries were selected based on a set of criteria including contribution to the economy, strategic importance of the industry to the nation and the potential fit and importance of IoT to the industry.

However, there is great value to examining other industries that were not included in this current research. One immediate benefit would be to enable the portfolio approach to be broadened to additional key market sectors in the economy. For example, the mining and mineral processing industry has taken on strategic importance as the United States transitions to clean energy. Many renewable technologies depend on minerals like lithium, cobalt and rare earth elements. These materials are essential for manufacturing batteries, solar panels, wind turbines and electric vehicles. However, many of these minerals come from other nations, including China.

The Biden administration's Inflation Reduction Act has created a boom in proposals for "new mining operations, mineral processing facilities and battery plants, laying the foundation for domestic supply chains that could support rapid growth in electric vehicles and other clean technologies."[254]

Mining operations are labor intensive, take place in dangerous environments and conditions and are subject to a variety of environmental regulations. The application of IoT to mining operations has the potential to increase efficiency and production, safety and sustainability.[255]

Other examples of industries to be studied may include biotechnology, aerospace and defense and consumer packaged goods. These industries suffer from a variety of additional IoT technology infrastructure challenges that may not have been covered in this report.

Recommendation 4. Refresh the economic analysis on a periodic basis to inform future federal research investments and initiatives as IoT evolves.

The Internet of Things is evolving and the findings in this report represent a point of view in time. The Internet of Things is composed of a set of diverse technologies that are at various stages of maturity. Advancements in artificial intelligence and computing paradigms (distributed, context-aware and swarm) provide significant acceleration and outsized benefits for IoT.

---

[254] "US minerals industries are booming. Here's why." J. Temple, MIT Technology Review, March 13, 2023. Link

[255] "How IoT Technology is Transforming the Mining Industry," AEO Logic Blog, October 22, 2022. Link

© Strategy of Things, 2025. All rights reserved.

Existing gaps, such as interoperability and cybersecurity concerns, are long-running complex challenges that will continue to hinder IoT in the future. Finally, as IoT scales in adoption, individual connected devices become connected systems and ecosystems and create new economic value.

The economic analyses in this report are based on economic models and assumptions specific to a short time period (up to 2030). Future refreshes of the research should consider technological advancements due to current federal investments, new emerging technologies and updated economic models based on the evolution of IoT.

By continuing to refresh the data and analysis periodically, the federal government will be able to better assess and manage the performance of the research investments and efforts to address these IoT technology infrastructure gaps.

Recommendation 5. Study the economic and societal impact of the convergence of AI with IoT (AIoT) to create the AIoT-enabled economy.

From more efficiently analyzing and making sense of the massive volumes of IoT data collected, to facilitating autonomous operations of industrial systems and critical infrastructure, Artificial intelligence is transformational for maximizing the benefits and the value of IoT. This report highlights several topics related to the convergence of AI and IoT, including the evolution of IoT and several related technological infrastructure challenges.

We recommend a more dedicated future research study focusing on the impact of the convergence of Artificial Intelligence (AI) with the Internet of Things (IoT), commonly referred to as AIoT and its potential economic benefits for society. The proposed study should explore how AIoT has the potential to enhance economic growth by enabling more efficient data analysis, optimizing industrial operations and automating critical infrastructure.

By examining the specific applications of AI in IoT across industries, such as smart manufacturing, healthcare, transportation and energy, research can provide insights into how AIoT-driven automation and decision-making promise to improve productivity, reduce operational costs and create new market opportunities. This research will be instrumental in assessing how AIoT has the capacity to contribute to a more efficient, sustainable and technologically advanced economy.

At the same time, future research will need to identify the key challenges that must be addressed to fully realize these economic benefits. These challenges include examining technological barriers, such as data security, AI algorithm development and IoT device interoperability, as well as policy and regulatory concerns, such as privacy laws, data ownership and AI governance.

By understanding the obstacles in AIoT adoption, this proposed study promises to inform policymakers, regulators and industry leaders on how to create an enabling environment for AIoT innovation while mitigating risks. Moreover, the research would benefit from analyzing possible societal impacts, including workforce displacement and ethical concerns, ensuring that the benefits of AIoT are balanced with responsible and inclusive implementation.

© Strategy of Things, 2025. All rights reserved.

Recommendation 6. Disseminate the findings of this report to industry and academia. Industry and academia would benefit from considering the findings and exploring opportunities to collaborate with the federal government and agencies to address the gaps identified in this report.

The gaps identified are long-running, complex and challenging. Closing these gaps will require a coordinated effort involving collaboration and partnership between government, academia and industry. These entities must work together to develop solutions that address the technological, regulatory and infrastructure barriers currently impeding the widespread adoption of IoT. Government has an opportunity to play a key role by crafting policies that incentivize innovation, conducting research in areas that industry is not yet doing and addressing a variety of cross industry challenges.

Meanwhile, academia has the ability to contribute through research and development, focusing on technological advancements and early-stage innovations, while industry is capable of addressing near-term gaps and implementing these innovations and driving their commercial deployment. Without such collaboration, the United States risks falling behind in IoT leadership and failing to unlock the full economic potential of IoT technologies and systems.

To provide benefits to the large community, it is appropriate that the findings of this study to be disseminated broadly to academic institutions, industry organizations and government agencies for consideration, planning and action. By sharing insights on infrastructure deficiencies and policy challenges, the study promises to serve as a catalyst for strategic partnerships aimed at accelerating IoT innovation and adoption.

Additionally, the report's recommendations offer a guide to the creation of new educational programs that prepare the workforce for the IoT-driven future. These efforts would help ensure that the United States has the ability to close its existing technology gaps and fully capitalize on the economic and societal benefits that IoT has to offer.

© Strategy of Things, 2025. All rights reserved.

10. Conclusion

The Internet of Things (IoT) is an evolving technology infrastructure domain that has the potential to enhance U.S. global competitiveness, increase national resilience and increase national and economic security. A number of technological and non-technological challenges, however, hinder its development, adoption and benefit realization. The rising prominence of AI has reinforced the importance of IoT and created a sense of urgency to address these challenges. The Internet of Things provides AI with one source of data to build and train algorithms and models. In turn, AI enables IoT systems to make sense of the monitored conditions and respond to these situations.

This study aims to inform the U.S. federal government where to direct potential federal research investments and initiatives to advance the Internet of Things by identifying the top IoT technology infrastructure gaps and quantifying the economic benefits of closing those gaps.

The study's research focused on those gaps where the federal government has the potential to address and where industry is unable to fully address. The research examined the current state of IoT technology development and its use across nine of the largest and most important industries in the United States. Information was gathered through a combination of secondary desk research, an industry survey and interviews with select industry and subject matter experts.

Three frameworks and models were developed to facilitate the analysis and creation of results in this research. A framework was developed to identify and prioritize technology infrastructure gaps that is aligned with the evolution of the Internet of Things. An economic model was developed to quantify the impact of addressing the identified technology infrastructure gaps. This economic model incorporates a portfolio approach to allocating investments across technology areas, infrastructure gaps and industries. Finally, an opportunities portfolio framework was developed to facilitate the identification of representative opportunities for the federal government to consider in addressing the technology infrastructure gaps.

The research identified a portfolio of IoT technology infrastructure gaps that the federal government should consider for research investment. These gaps were segmented into three addressable categories:

- Core gaps are essential for the function and operation of IoT. The core gaps to be considered are interoperability, cybersecurity, privacy and connectivity concerns.
- Intelligence gaps that support and enable the intelligent and autonomous operation of IoT. The intelligence gaps to be considered are data management, trust in AI and intelligent device concerns.
- Hyper-Deployed gaps that facilitate the future IoT-enabled economy and society with billions of interconnected and autonomous devices. If addressed, the hyper-deployed gaps promise to enable an IoT data ecosystem and a communications and network infrastructure.

The economic analysis quantified the economic impact of addressing the core and intelligence gaps. A nominal public sector investment of $10 million in each gap was associated with a revenue of between $548 million and $889 million and an economic surplus of between $149 million and $239 million based on gross margins.

© Strategy of Things, 2025. All rights reserved.

For each of the gaps identified, the economic analysis further showed how that $10 million investment could be allocated across the nine industries studied to obtain maximum benefit to the economy. One key outcome of the economic analysis is that a financial portfolio approach to research investment funding can potentially lead to optimal economic benefits to the economy.

A portfolio framework for viewing and considering federal government opportunities for actions to close the technology infrastructure gaps was developed. The core, intelligence and hyper-deployed gaps were reviewed against this model and some broad areas of federal government action were identified.

Government leaders and policymakers would do well to consider taking a portfolio approach to addressing the IoT technology infrastructure gaps. The portfolio approach considered three perspectives: technology, economics and government. The technology perspective recognizes the diverse types and nature of the gaps, as well as the technology's maturity state along the IoT evolution cycle. The economic model provides information on the indicative allocations across the industries to address the gaps that will maximize outcomes for the broader economy. The actual uses of the funding allocations are informed by the specific federal capabilities available and needed to address the IoT gaps with those investment allocations.

This portfolio approach recognizes that multiple gaps need to be addressed simultaneously and the nature of those gaps varies depending on the evolutionary stage of IoT and its underlying technologies. In addition, some investments may be used to address gaps that may be more difficult to address than others and some gaps and industries may require more investments than others. Furthermore, the proposed set of actions undertaken by the federal government to address these gaps will vary depending on the nature of the gap, the roles of industry and academia, and the capabilities and resources available to address it.

In addition, the study offers a number of recommendations, including extending the study to other growing or impactful industries, studying the economic impact of the convergence of AI with IoT and conducting a periodic refresh to track and monitor the progress of the research investments and initiatives in closing the identified gaps. This is necessary to extend the portfolio approach to other market segments.

In closing, the federal government is well-suited to address the gaps found. These gaps are too broad, complex and challenging for industry, academia or government to address solely. Each stakeholder plays a vital and complementary role. It is the hope of the authors that the findings from this research will also drive new collaboration models and partnerships between government, industry and academia to advance the research necessary to develop and build out the vision enabled by the Internet of Things.

© Strategy of Things, 2025. All rights reserved.

For more information contact:

Benson Chan
Email: benson@strategyofthings.io

Renil Paramel
Email: renil@strategyofthings.io

Christopher Reberger
Email: christopher@strategyofthings.io

Strategy of Things
www.strategyofthings.io

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the authors, except in the case of brief quotations embodied in research reports, industry articles and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Strategy of Things LLC
1305 Franklin Street, Suite 507
Oakland, CA 94612

marketing@strategyofthings.io

Appendices

© Strategy of Things, 2025. All rights reserved.

Appendix: The Internet of Things

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

© Strategy of Things, 2025. All rights reserved.

11. Appendix: The Internet of Things

This appendix provides an overview of the Internet of Things (IoT), examples of IoT applications and their unique characteristics and introduces a classification structure to identify IoT infrastructure opportunities.

11.1. Introduction

At their simplest, an IoT application collects data from sensors that monitor a physical environment, sends that information to a processor which analyzes the data and then initiates an action or response based on the data or an analysis.[256]

These data are routed from the sensor to the processor through several wireless technologies such as Bluetooth, Wi-Fi, LoRaWAN, NB-IoT, 4G and 5G. The data are then aggregated by a local gateway router, transmission device or a remote cellular base station. Once the data reaches the gateway or base station, it is routed through a broadband infrastructure network where it is subsequently routed to a remote cloud data center.

The data center collects the data, normalizes, stores, analyzes and acts according to algorithms or by user criteria. This information is then routed or made available to execution systems, such as Enterprise Resource Planning (ERP) systems or operations execution software applications for additional action.

Not all IoT applications route data to a cloud data center for storage and processing. Edge IoT applications can process data on the device, at a local gateway or at a local processing server. A schematic of this process is shown below in Figure 11-1.

[256] For our research, we elected to use a simplified but broader definition for IoT which included the device, the system and the broader enterprise IT environment it is connected and integrated into in order to capture the gaps more fully across the current and future states of IoT. We were informed by the various definitions for IoT device, IoT component, IoT system and IoT environment as defined by NIST as specified in the IoT Definitions, January 2023 document. Link

© Strategy of Things, 2025. All rights reserved.

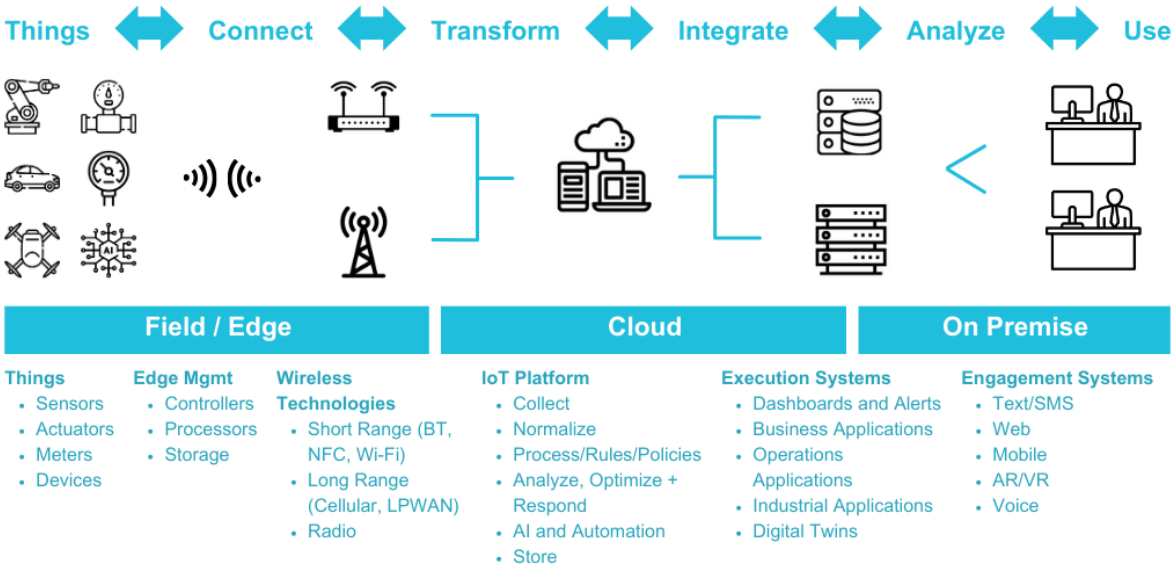


Figure 11-1: IoT Architecture Overview

11.2. IoT examples

IoT devices are part of our daily lives. Smart phones can incorporate motion, optical, audio and location sensors and can tell us where we are, how fast we are moving and interpret what we are doing. Other examples include:

- Vibration sensors on manufacturing equipment that alert the operator if the machine is behaving abnormally or if maintenance is required.
- Image sensors and cameras on drones detect areas where crops are not green enough, indicating poor plant health or presence of pests.
- Light Detection and Ranging (LiDAR) sensors on autonomous vehicles (an IoT system) that scan areas adjacent to a car and detect traffic and pedestrians. This information is sent to an onboard computer running driving algorithms, which then tells the car to act on the information and take appropriate action or to avoid a collision.

11.3. IoT product and service opportunities

Adding sensors and actuators to the physical environment and collecting data yields value from both doing old things in new ways and doing new things that were not previously possible. IoT drives value by creating opportunities for cost avoidance, increased efficiencies and productivity, reduced variability and waste, increased safety as well as creating new classes of data enabled products and services.

Figure 11-2 below shows an example of how this is possible with the example of a “smart machine” used for manufacturing products.

© Strategy of Things, 2025. All rights reserved.

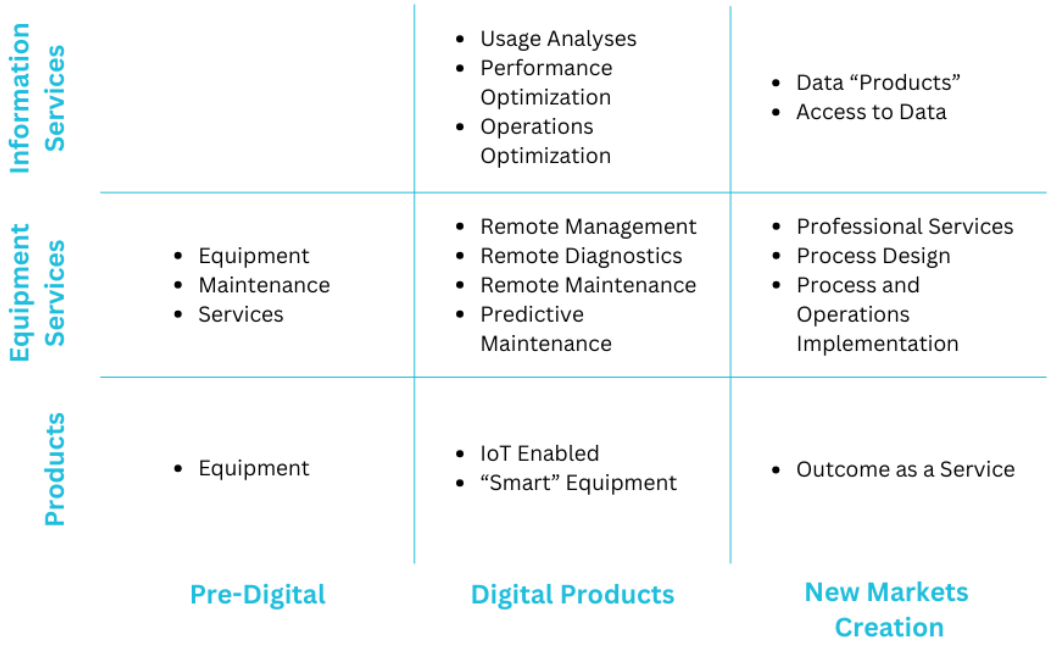


Figure 11-2: IoT Example: Manufacturing Opportunities

Prior to IoT, equipment dealers traditionally sold machinery, spare parts, warranties, maintenance contracts and installation and repair services.

The addition of IoT to the equipment creates new capabilities and value for both buyers and dealers. These "smart machines" allow dealers to offer new services and existing services in new ways.

For example, onboard IoT sensors allow a dealer's technicians to monitor and diagnose their customers' machinery remotely and avoid an onsite visit. Predictive algorithms monitor IoT sensor data and alert technicians when maintenance and repairs are needed, order a replacement part and then schedule a technician to replace the part. This helps the customer avoid unplanned machinery downtime and maintain operational productivity.

IoT devices collect substantial amounts of data. This includes machinery usage data from its customer base which is aggregated by the manufacturer to understand how their machines are used in practice. Engineers analyze this information to create new services and applications that are provided to the customers.

For example, this information can be used to create performance optimization software and consulting services. Customers purchase these new information products and services as it further enhances their operational productivity, reduces inefficiencies and enables them to scale.

IoT creates opportunities for equipment manufacturers to enter new markets. For example, the data and insights collected from its "smart machines" can be aggregated, packaged and sold to lubricant vendors, who use the information to create more effective premium formulations. The data can also be purchased by insurance companies that use it in a way to minimize on-the-job

© Strategy of Things, 2025. All rights reserved.

accidents. Consultants use the same data to help the factories plan and implement operational process improvements.

Finally, "smart machines" provide factories with the capability to create innovative new businesses, such as "Manufacturing as a Service." With full visibility into the actual utilization of their production equipment, factories can offer excess capacities and capabilities to customers. The "uberization" of factories turns manufacturers into "manufacturing utilities" that offer contract manufacturing at agilities, scales and efficiencies unmatched by traditional factories.

11.4. IoT technologies

IoT is composed of a set of diverse technologies organized collectively as a "stack." Figure 11-3 below shows the components of the IoT stack. At the bottom of the stack are devices, sensors or "things" that collect information or act. Information to and from the device is received and transmitted using one of several wireless methods. The information is communicated to the cloud using one of several data protocols.

Once the data are ingested by the cloud platform, it is processed, stored and acted upon by various applications and algorithms. The processed information is then presented to users through one of several methods.

Each IoT use case or business application uses a different combination of stack components. For example, smart city applications have a different IoT stack because they use a different combination of components than an IoT application for manufacturing.

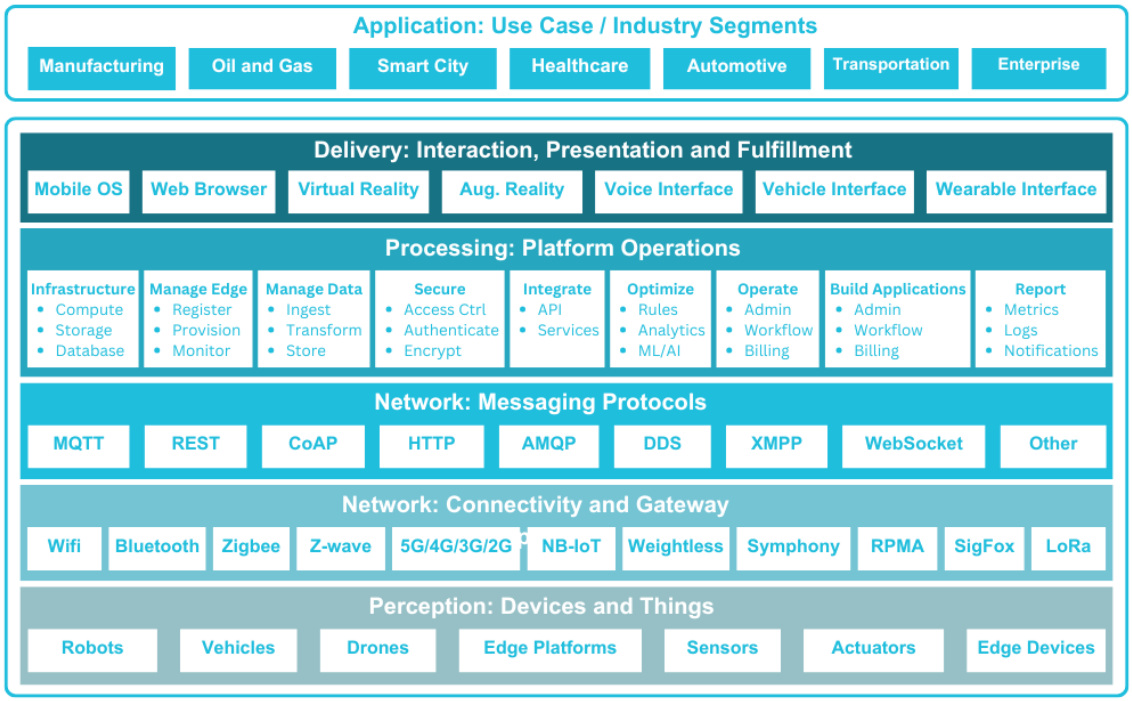


Figure 11-3: IoT Technology Stack (Non-Industry Specific)

© Strategy of Things, 2025. All rights reserved.

11.4.1. Devices and things

The IoT device combines hardware with embedded software. The hardware consists of a sensor(s) and/or actuator(s), an embedded system, storage and a wireless communications module. Embedded firmware and software manage the device and act on the data collected.

An embedded system is usually a miniscule computer that contains the microprocessor or microcontroller, memory and input and output peripheral devices. The type of sensor used will depend on the nature of the collected information. For example, a device may utilize a temperature sensor to collect the thermal characteristics of the surrounding environment or it may be a piezoelectric sensor that senses vibrations. Embedded systems are one of the core technology enablers of IoT as they provide the digital means for traditional devices to become "smart devices."

11.4.2. Connectivity and gateway components

The information is transmitted to the gateway through several ways, including Wi-Fi, Bluetooth, LoRaWAN, 4G, 5G and other wireless protocols. There is no universal wireless protocol that works for all applications. Some applications require protocols that can support high bandwidth uses such as video, while other applications require protocols that support low data bandwidth and low power consumption.

The appropriate protocol employed is application specific and is determined by a combination of factors. These include bandwidth type, range of wireless transmission, indoor/outdoor usage and IoT device power requirements.

Other key enablers making IoT possible are Low Power Wide Area Network (LPWAN) connectivity technologies such as LoRaWAN, NB-IoT and LTE-Cat M1. [257]

These technologies provide the ability to connect at scale a wide variety of devices. Examples include soil moisture sensors on acres of farmland or thousands of in-ground parking space sensors in a city communicating space availability. To be operationally feasible these applications require devices that can operate on battery power that can last for years. These requirements cannot be met with traditional connectivity technologies and are made possible with LPWAN technologies.

11.4.3. Messaging protocols

Information is received by the cloud through messaging or data protocols. Without a standard, IoT device makers are coalescing around a small set of protocols, such as REST, MQTT, HTTP, DDS, XMPP and CoAP.[258]

The specific protocol employed is a function of the IoT device, latency, speed, Quality of Service and other requirements. For example, Message Queueing Telemetry Transport (MQTT) is

[257] An acronym and initialism list is provided as an appendix.

[258] "CoAP, MQTT, AMQP, XMPP & DDS: Which Protocol Should You Choose for IoT?", N. Lukman, NexPCB. September 14, 2021. Link

© Strategy of Things, 2025. All rights reserved.

commonly used by resource constrained devices having a small code footprint and minimal network bandwidth.

In turn, the cloud platforms support these protocols, allowing them to interoperate with multiple device types. This coalescence and the support of a small set of protocols is one of the most important enablers of IoT as it allows a variety of device types using various communication methods to interoperate with the cloud platforms and provide information to other business and industrial applications.

11.4.4. Platform components

Software applications running on the platform use the IoT data once it is ingested by the cloud data centers. These applications manage the data collected, the optimization of the data, and the actions taken in response to the insights generated from analyzing the data. Other software applications manage the IoT devices and their users as well as the administration of the cloud platform.

The cloud and its supporting technologies employ new business and operating models to support IoT applications. Cloud data centers aggregate servers, databases and storage. These resources can be dynamically allocated on-demand to support the data processing and storage needs of IoT applications. Cloud-based servers provide computing resources to analyze large amounts of IoT data, by processing the machine learning and artificial intelligence algorithms that generate insights and outcomes. Cloud technologies provide scalable resources, processing power and agility that would be difficult for an IoT user to do on their own.

The ability to process, analyze and create optimized insights from large datasets is enabled by data science methods and analytics. The continuing development and maturing of data analytics tools, software and algorithms is a strategic IoT enabler in unlocking the value of the data collected from IoT devices.

11.4.5. Presentation components

Users interact with the processed IoT information through a variety of applications and interfaces. For example, information may be integrated into back-office ERP systems and then accessed through web browsers or mobile devices.

IoT differs from traditional Machine to Machine (M2M) systems, such as Supervisory Control and Data Acquisition (SCADA) in that it supports different types of devices using different protocols for connectivity and communications. This enables IoT data to be used by a variety of applications and presented to the user in a variety of formats. In contrast, SCADA systems employ devices running proprietary protocols integrating with proprietary software applications.

© Strategy of Things, 2025. All rights reserved.

11.5. IoT classifications

To facilitate information collection for this study, the underlying technology components of IoT are categorized into six categories[259] and 25 single technology components. The six categories are hardware, software, applications, networking, systems and standards as shown below in Figure 11-4.

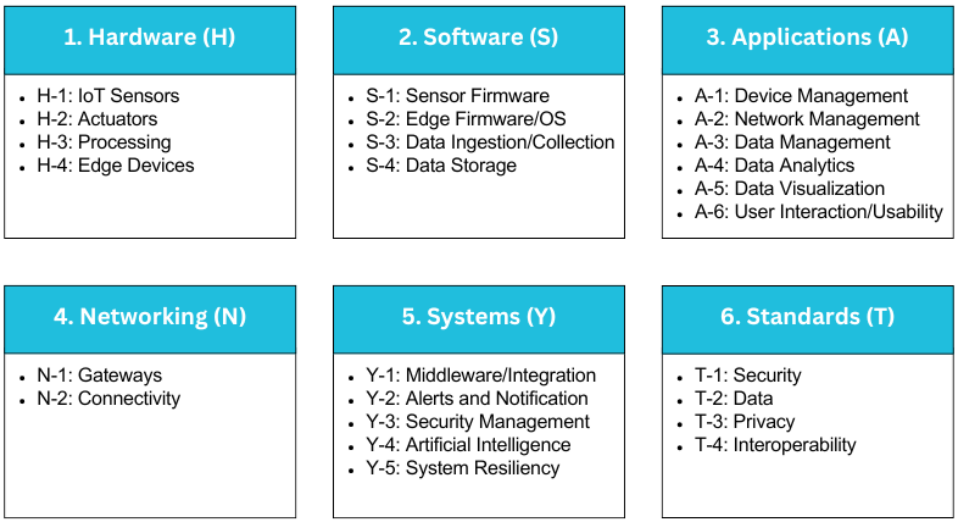


Figure 11-4: IoT Single Technical Component Taxonomy

- **Hardware** represents the physical components of an IoT solution. In this model, it covers IoT sensors, actuators, processing equipment such as servers and embedded systems, gateways and edge equipment.
- **Software** is the code and associated data intended to operate hardware within an IoT solution. It includes embedded systems firmware on devices, gateways and servers. It also includes software that manages data ingestion, collection and transformation and data storage.
- **Applications** are software that is designed to be used by people within an IoT solution. It includes device management, network management, data management, data analytics, data visualization and user interaction/usability.
- **Networking** is the collection of interconnected components that facilitate communication within an IoT solution and to other systems. It includes communications protocols, gateways and other connectivity.

[259] The six categories follow the taxonomy indicated in the grant documentation. See Page 7, 2019-NIST-TPO-IOT-0

© Strategy of Things, 2025. All rights reserved.

- **Systems** are software providing services to other software within an IoT solution or to other systems. It includes middleware/integration, alerts and notifications, security management, artificial intelligence and system resiliency.
- **Standards** are rules, conditions or documentation established by consensus and approved by a recognized body for IoT solutions. It includes security, data, privacy, communications and others.

© Strategy of Things, 2025. All rights reserved.

Appendix: Industry Appendices Structure

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

© Strategy of Things, 2025. All rights reserved.

12. Appendix: Appendices Structure

Sections 13 through 21 provide detailed information on IoT issues for the selected industries. Each of the industry appendices follows the same structure and contains the following:

- An overview providing key industry facts and challenges.
- The role of IoT in the industry and a description of some representative use cases.
- The top IoT technology challenges
- The top non-technology challenges

To arrive at the IoT technology challenges for each industry, the following process was used:

1. **Identify initial list of challenges.** An initial list was developed by asking "What are the IoT technology challenges hindering adoption in this industry?" Information was collected through desk research and interviews with key industry personnel.

   Some of these challenges were common across multiple industries (e.g., cybersecurity, interoperability), while others were relevant to a particular industry (sensors in retail). In addition, a set of non-technology challenges was documented for completeness.

2. **Identify strategic and relevant challenges.** The initial challenges list was pared down by considering those challenges that are strategic, critical and have a significant impact using the data sources to inform any judgment. These were then considered as strategic gaps.

   For example, one consideration was the number of times a particular challenge was mentioned which signified the extent to which it was a "top of mind" issue. Another consideration was the extent the challenge impacted the IoT evolution framework discussed in Section 22.

   Other considerations included the impact on scalability (i.e., how does this gap affect the future scalability of IoT), user adoption (i.e. how does this gap affect the users' ability to procure, integrate and use IoT) and value realization (i.e. how does this gap impact the benefits that the adopting organization is expected to receive).

   For example, connectivity is a strategic and important challenge in agriculture. Without connectivity, the use of IoT applications is not possible or severely constrained. In retail, however, connectivity is not an issue. While not all retail environments have robust connectivity, the connectivity challenge is addressable by current industry solutions and approaches.

   Similarly, artificial intelligence is emerging in importance. However, it is not a top challenge in smart cities because most cities have not yet implemented basic smart city

© Strategy of Things, 2025. All rights reserved.

technologies and solutions.

3. **Determine which challenges offer potential opportunities for government research.** While industry, government and academia address these gaps in various ways, these efforts are often limited and there are often opportunities for continued research. There may be gaps that industry is not addressing or may be addressing in traditional ways.

   For example, low-cost devices are important in retail. Current industry development efforts, however, are insufficient to bring the cost of sensors to a level comparable to RFID solutions. Research investments in more novel approaches, such as thin film technologies are needed.

   Assessments of what is currently not addressed are made by reviewing desk research, survey results and interviews.

4. **Other considerations:** To arrive at the final list, additional questions were applied. Some examples include:

   - Is this a challenge that hinders the evolution of IoT?[260] With few exceptions, many research sources informed the "here and now" IoT challenges and opportunities. For example, further investments in AI are necessary to support a future where some IoT applications operate autonomously

   - Are there factors that could significantly impact current industry efforts? For example, privacy regulations and policies are evolving and may render existing privacy approaches obsolete. Research in privacy enhancing technologies is essential for the development of IoT solutions that comply with possible future regulations.

   - Is this challenge an area that can be accelerated by research investments? For example, AI is evolving and presents an opportunity for federal research investments to supplement current industry research efforts.

For the remaining appendices:

- Section 22 provides information on the evolution of IoT
- Section 23 provides the cross industry gap analysis
- Section 24 provides information on government opportunities to address the consolidated cross industry infrastructure gaps
- Section 25 provides details on the quantification methods and the technology classification selections from survey participants, desk research and interviews for each of the 9 industries

[260] As described in in Appendix 22.

© Strategy of Things, 2025. All rights reserved.

- Section 26 provides the summary results, a sensitivity analysis and the impact of a nominal public sector investment
- Section 27 provides a list of initialisms and acronyms

© Strategy of Things, 2025. All rights reserved.

Appendix: Agriculture

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

© Strategy of Things, 2025. All rights reserved.

13. Appendix: Agriculture

This section describes the research findings for IoT technology infrastructure in the U.S. agriculture industry. The topics discussed here include:

- Industry overview
- Use of IoT in agriculture
- IoT challenges in agriculture

13.1. Industry overview

This section presents some key facts about the agriculture industry, as well as the most significant industry challenges.

13.1.1. Key facts

Agriculture plays an important role in the United States economy. Key sectors include agricultural chemicals, crop production, aquaculture, forestry, logging and livestock. In 2023, agriculture and related industries contributed $1.537 trillion, or 5.5% to national GDP.[261]

Farm outputs generated $222.3 billion, or 0.8% of the national GDP.[262] In 2023, the industry generated commodity cash receipts of $521 billion for crops, animals and animal products.[263] Of that number, crops, including crops grown for animal feed, represented 52.1%.[264]

The agricultural and food sectors employed 22.1 million people, or 10.5% of the U.S. employment in 2022. Ranching and farming provided 2.6 million jobs, or 1.2% of all U.S. employment.[265] Another 1 million jobs, or 0.5% came from forestry, fishing and related activities.[266] Agriculture outputs, including food, beverage and tobacco manufacturing; food and beverage stores; food service, eating and drinking places; and textile, apparel and leather manufacturing lead to another 18.5 million positions, representing 8.8% of all U.S. employment.[267]

The United States is the second largest agricultural exporter after the European Union. With U.S. agricultural output growing faster than domestic demand for many products, export markets have

[261] "Ag and Food Sectors and the Economy", USDA. Economic Research Service, December 19, 2024. Link

[262] ibid.

[263] "Annual Cash Receipts by Commodity", USDA, Economic Research Service, December 3, 2024. Link

[264] ibid.

[265] See note 261

[266] ibid.

[267] ibid.

© Strategy of Things, 2025. All rights reserved.

enabled farmers and ranchers to sustain prices and revenues. As a result, U.S. agricultural exports have grown steadily from $52 billion in 1994[268] to $174 billion in 2023.[269]

In 2023, the top markets for agricultural exports are China, Mexico, Canada, the European Union and Japan.[270] The top exported products are food grains, grain and oilseed milling products, oilseeds and fruit and tree nuts. A majority, 90 percent of total agricultural exports, come from just four categories. These include grains and feeds; oilseeds and products; animals (e.g. livestock and poultry), meats, and products; and horticultural products.[271] China is the largest importer of soybeans taking 52% of the exports.[272]

There were 2.05 million farms in operation in 2017, a decrease from a peak of 6.8 million farms in 1935.[273] The average farm size rose from 155 acres to 444 acres during the same period. Family farms accounted for 98% of all U.S. farms in 2018.[274] Small family farms, with a gross cash farm income (GCFI) of $350K, account for 90% of farms and 21% of production.[275] Large-scale family farms, having a GCFI of $1 million or more, accounted for about 3 percent of farms and 46 percent of production.[276]

A total of 1,045 million acres of land[277], or 20% of the lower contiguous 48 states of the United States, is used for agricultural purposes. Of this total, 38% or 392 million acres are for growing crops.

Only 77 million acres (20%) of this crop land is used for growing the food that Americans consume. Half of the crop land (49%) is used for growing livestock feed or for grain exports. One-third, or 654 million acres[278], of the land in the lower contiguous 48 states of the United States is used for livestock and grazing. Considering the 127 million acres of land used to grow feed for livestock, approximately 43% of land in the United States is used to support livestock.

13.1.2. Industry challenges

The U.S. agriculture industry faces several challenges that constrain the growth and advance of the industry. Four key challenges, which are relevant to the Internet of Things in agriculture are:

- Changing climate patterns

---

[268] "U.S. Agricultural Trade at a Glance", USDA, Economic Research Service, April 2023. Link

[269] "Agricultural Trade", USDA, Economic Research Service, February 16, 2024. Link

[270] ibid.

[271] ibid.

[272] "China: Top Market for U.S. Ag Exports", Department of Agriculture. Link

[273] "Farming and Farm Income", USDA, Economic Research Service, August 2023. Link

[274] ibid.

[275] ibid.

[276] ibid.

[277] "Here's How America Uses its land", July 2018. Link

[278] ibid.

© Strategy of Things, 2025. All rights reserved.

- Labor shortages
- Agriculture and scale
- Global food shortages

Each of these is discussed below.

13.1.2.1. Changing climate patterns

Shifting climate patterns pose a challenge to U.S. agricultural producers. Increasing temperatures and changing precipitation patterns affect plant life cycles and decrease crop productivity. Exposure to higher and lower temperatures increases stress in livestock and affects their health, reproduction and the production of milk and eggs.

These changes also affect pests and beneficial insects, including plant pollinators which affect weed growth, plant and livestock health and productivity yields. Extreme weather events, from heatwaves, droughts to excessive rainfall and flooding, are likely to become more frequent and last longer and will impact growing conditions and result in increased damages and lower yields.[279]

For example, previous studies of temperature changes found that "corn yields declined 3.8% and wheat declined 5.5% compared to the yields without climate trends."[280]

To maintain productivity, agricultural producers will be required to adapt to changing climate patterns by adjusting inputs and the types of inputs, use of new disease and drought tolerant crop species, crop rotations and a variety of new harvesting strategies.

13.1.2.2. Labor shortages

U.S. agricultural producers have difficulty attracting, recruiting and retaining workers. In a 2017 California Farm Bureau Federation survey, 55% of the 762 respondents experienced staffing shortages. For those respondents that employ a seasonal workforce, 69% reported employee shortages, with some unable to hire up to 50% of the workers needed.[281]

The *Ag Barometer*, a monthly survey published by Purdue University/CME Group, indicated that 66% of its respondents reported "some" or a "lot of difficulty" hiring adequate labor in 2021, compared with 30% in 2020.[282] This is consistent with a 2019 Farm Journal Ag Labor study

[279] "Climate Change and Agriculture In The United States: Effects and Adaptation", USDA Technical Bulletin 1935, February 2013. Link

[280] "Agriculture In the Midwest", White Paper Prepared For The U.S. Global Change Research Program National Climate Assessment Midwest Technical Input Report, J. Winkler, J. Andresen, J. Hatfield, D. Bidwell and D. Brown, coordinators, Hatfield, J., 2012. Link

[281] "Searching for Solutions: California Farmers Continue to Struggle with Employee Shortages Agricultural Labor Availability Survey Results—2017", California Farm Bureau Federation, October 2017. Link

[282] "Five Facts About the Ag Labor Shortage", J. Shaffstall, AgWeb, July 27, 2021. Link

© Strategy of Things, 2025. All rights reserved.

which reported 68% of respondents' biggest challenges were finding qualified workers and temporary labor.[283]

The shortage is a combination of many factors, including declining interest in agriculture among young people, competition from higher paying and less physical jobs in other industries, decline in the numbers of undocumented workers due to immigration policies and inefficiencies in the H-2A program for temporary agriculture workers.[284]

The impact of this labor shortage is seen in several ways. A study estimated a production loss of an additional $3.1 billion in fruits and produce, $2.8 billion in additional spending in services utilized by agricultural producers such as transportation and 41,000 more supporting jobs in non-farm sectors.[285]

13.1.2.3. Small farm profitability

Small family farms, defined as having a gross cash farm income (GCFI) of less than $350,000, represented 89.6% of all farms, 48.8% of all farmland and 21.1% of all production in 2019. Large family farms, with GCFI of $1,000,000 or greater, represented 2.7% of all farms, 20.7% of all farmland and 43.8% of all production.

Most small family farms, between 62% to 81%, depending on the specific farm type, have a less than 10% operating profit margins. As farming is capital intensive, these farms are operating with high financial risk with little margin for error.

Chapter 12 bankruptcy filings rose from 361 filings in 2014 to 599 in 2019 before dipping slightly to 560 filings in 2020. Chapter 12 filings dropped by half to 276 in 2021, helped in part by rising commodity prices though this was against an increase in production expenses and costs of 18% in 2022. Farm income was expected to decline 0.6% over the year.

Small family farms had higher incomes from non-farming activities than from farming. For example, low sales family farms, with GCFI of less than $150K, had a negative income of $1,427 from farming while generating an off-farm income of $65,482. Similarly, family farms with GCFI between $150K and $350K, reported an average non-farm income of $56,135 and an average farm income of $42,170. Mid-size family farms, having a GCFI between $350K and $1 million, generated 35% of their total income from non-farming activities.

Finally, federal government payments contribute to a portion of the farmers net income, ranging from an average of 11% in 2014 to 48% in 2020. The government payments include pandemic assistance, market facilitation programs, crop insurance and disaster assistance programs.

13.1.2.4. Global food shortage

As the cost of necessities rises, experts in global health have warned that food shortages could cause the next global health crisis. According to the World Food Programme ("WFP"), 345

[283] ibid.

[284] "The U.S. Farm Labor Shortage", June 28, 2022. Ag America. Link

[285] "Agriculture", New American Economy. Link

© Strategy of Things, 2025. All rights reserved.

million people are in immediate danger from acute food insecurity and 828 million people go to bed hungry every night.[286] Four of the main causes for world hunger include[287]:

- Conflict, with 60% of the world's hungry living in areas afflicted by war and violence
- Climate Shocks that destroy lives, crops and livelihoods
- COVID-19 pandemic economic consequences
- WFP's monthly operating costs, which are $73.6 million above their 2019 average

The sudden change in global food and fertilizer prices added $9 billion to the import bills of the 48 most affected countries in 2022 and 2023.[288] According to the IMF, an additional $5–7 billion would need to be budgeted for vulnerable households in the 48 countries to be protected from increased food prices.

The world grows enough food to feed 12 billion people, yet more than one billion people are underfed.[289] The UN estimates that by 2050 we will reach a tipping point and there will be a global food crisis if we continue our current path of food consumption and waste.[290] The current process has created a consumer expectation of blemish-free goods at specific sizes. Food purveyors have responded and built a market predicated on waste.[291] With these expectations, the cost of managing suppliers to ensure product consistency and safety makes it difficult to embrace new, innovative providers.[292]

13.2. IoT in the agriculture industry

Agriculture is undergoing a transformation driven by the integration of information and digital communications technologies, the Internet of Things (IoT), data analytics, automation and robotics and other emerging technologies.[293] This transformation offers the potential to increase agricultural productivity, operational efficiency, facilitate adaptation to climate changes and enhance overall competitiveness.

This transformation, sometimes called Agriculture 4.0 or "smart Agriculture", represents the 4th agricultural revolution. The first agricultural revolution occurred with the transition from nomadic hunting and gathering to farming and herding. The second revolution occurred with the

---

[286] "Global Food Crisis Demands Support for People, Open Trade, Bigger Local Harvests", IMF Blog, September 2022. Link

[287] "A Global Food Crisis", WFP. Link

[288] "Tackling the Global Food Crisis: Impact, Policy Response and the Role of the IMF", IMF, Rother B. et al, September 2022. Link

[289] "Is the Internet of Things the Answer to the Global Food Crisis?", GlobalData,Thematic Intelligence, September 14, 2021. Link

[290] ibid.

[291] ibid.

[292] ibid.

[293] "Agriculture 4.0: Broadening Responsible Innovation in an Era of Smart Farming", D. Rose and J. Chilvers, Frontiers in Sustainable Food Systems, Dec 21, 2018. Link

© Strategy of Things, 2025. All rights reserved.

use of mechanization and the development of scientific methods and practices for livestock breeding and farming. The third revolution occurred with the hybridization and genetic engineering of products, the use of pesticides and fertilizers and new technologies, such as controlled irrigation and new mechanization methods.

The Internet of Things is one of the technologies that enables Agriculture 4.0 and the most current transformation of Agriculture. The "smart" in "smart Agriculture" is enabled by the application of sensors, data and analytics to enhance agricultural operations and outcomes.

One source of real time data is from IoT sensors and devices that monitor traditional agricultural equipment, such as combine harvesters and tractors, operational machinery and livestock. In some cases, the sensors collect information that was not previously available or collected. Other sources of data come from existing operations and equipment, as well as third party business and government organizations.

While agricultural producers are accustomed to using data to make key planting decisions, most of the data used are static or historical. IoT technologies and applications will generate real time data and insights to provide new ways to address many of the quotidian challenges faced by agricultural producers.

For example, sensors placed into the soil measure the moisture level and inform the irrigation system which parts of the growing area need watering and direct water to those areas of the field most in need. A 2019 USDA analysis estimated that a smart irrigation application for specialty crops can contribute a potential annual gross benefit of $801.9 million to the industry.[294] Another IoT example is the use of drones to fly over vast fields to monitor crop health and inform farmers where further attention is needed.

Similarly, sensors placed on livestock measure vital health signs and proactively alert ranchers when the animals are sick, facilitating earlier diagnosis of illnesses and detection of disease outbreaks. This frees up ranch workers who would otherwise have to check on the individual animals daily. The same USDA analysis estimated that general health monitoring of livestock can produce an annual gross economic benefit of $8.8 billion.[295]

IoT helps agricultural producers address machinery breakages and unplanned downtime, inefficient operations, poor input management, plant and animal health, limited supply chain visibility and reactive field support. Equally important, IoT helps agricultural producers lessen the impact of labor shortages and augment existing labor resources.

A 2018 study estimated 250,000 farms across the United States were using IoT solutions, with most of these in livestock and crop management. The study also found that up to half of all U.S. farms were interested in purchasing IoT solutions, representing 1.1 million farmers and a potential agricultural IoT solution market opportunity of $4 billion dollars.[296]

---

[294] "A Case for Rural Broadband: Insights on Rural Broadband Infrastructure and Next Generation Precision Agriculture Technologies", USDA, Page. 22, April 2019. Link

[295] Ibid. Page 23

[296] "Nearly 250,000 U.S. Farmers Already Using IoT Technology, Study Finds", J. Tomas, May 16, 2018. Enterprise IoT Insights. Link

© Strategy of Things, 2025. All rights reserved.

A 2021 survey conducted by Purdue University and Croplife magazine found that 17% of crop input dealerships are offering wired and wireless sensor networks and IoT, up from 14% in 2019. The number of dealerships offering these technologies is projected to grow to 28% by 2024.[297]

Finally, new business models, such as "yield as a service", building upon the contract agriculture[298] model, emerge when networks of agricultural producers offer their land, expertise and smart agriculture capabilities to each other or other businesses. These models may be well suited for the emerging indoor farming or vertical farming businesses. This eventually leads to autonomous agriculture, which builds upon all the Agriculture 4.0 capabilities, connected industry ecosystems and new business models.

13.2.1. IoT use cases

Figure 13-1 shows a representative set of agriculture use cases organized into five categories.

- **Precision Farming.** Precision farming seeks to increase crop yields and profitability while lowering the levels of traditional inputs such as land, water, fertilizer, herbicides and insecticides.
- **Livestock Management.** Livestock monitoring collects information on animals and their health, their environment and their movements and other patterns. Monitoring ensures proper animal health, reproduction and growth. The integration with sensors, databases, mathematical models and knowledge bases enables proper animal health and care.
- **Greenhouse Monitoring.** Greenhouse and indoor farm monitoring ensure the proper environmental conditions, including temperature, humidity, soil, water and light for optimal plant growth and health.
- **Supply Chain and Logistics.** The IoT applications in the agriculture supply chain include those that monitor the way goods are transported from suppliers and producers to processors, buyers and to market.
- **Equipment, tools and machinery.** There is a range of use cases, ranging from machinery operation to maintenance. These use cases are not unique to agriculture.

[297] "2021 Precision Agriculture Dealership Survey", B. Erickson and J. Lowenberg-DeBoer, December 2021, Purdue University Departments of Agricultural Economics and Agronomy, Page 8. Link

[298] Contract Farming, Wikipedia. Link

© Strategy of Things, 2025. All rights reserved.

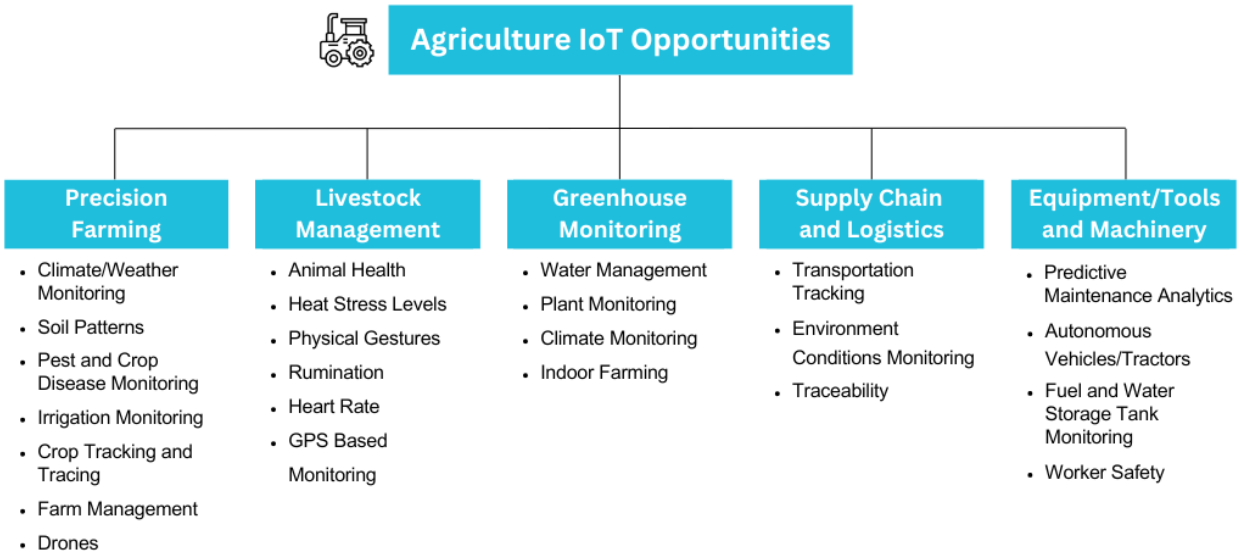


Figure 13-1: Agriculture: Use Case Categories and Representative Use Cases

IoT monitors the day-to-day operations in agriculture. For example, soil moisture sensors help inform on irrigation decisions. Drones fly over fields to monitor crop health and detect areas for early intervention. Computer vision sensors mounted on spraying booms detect the presence of pests and weeds and apply treatments to the target area. Sensors on livestock monitor animal health to identify and treat problems early and to proactively prevent disease outbreaks. The information collected helps farm and ranch managers optimize use of labor, equipment, resources and time, improve production operations and outputs and minimizes waste and environmental impacts.

While IoT will enhance and directly improve agricultural outcomes and day-to-day operations, value is also created in improving the indirect activities associated with farm or ranch operations. For example, predictive maintenance is not directly involved in agricultural operations, but it ensures that the machinery involved will be serviced before it breaks down. This prevents fields from going unworked while the machinery is down for weeks during the critical planting and harvest seasons. For equipment dealers and original equipment manufacturers (OEM), support of equipment deployed in the field is a major activity. Remote monitoring and management of field machinery and equipment allows dealer technicians to be proactive and agile in servicing their customers.

13.2.1.1. Use case and industry challenges alignment

The agriculture industry faces several challenges, some of which are described in Section 13.1.2. Figure 13-2 below shows the alignment of some representative IoT use cases to these industry challenges.

© Strategy of Things, 2025. All rights reserved.

Challenge	Role of IoT	Examples
Changing climate patterns	Minimize the impact of droughts, heat waves, flooding and other conditions caused by changing climate patterns. Facilitate adaptation to changing climate patterns will lead to improved plant and animal health, resilience and production yields.	• Climate/weather monitoring • Soil moisture monitoring • Smart irrigation • Livestock health monitoring • Water management
Labor shortages	Optimize workforce productivity, efficiency and effectiveness through operations planning, task automation, resource optimization and data informed actions. IoT technology helps producers do more with fewer resources and to be more effective doing it.	• Autonomous tractors and machines • Drones • Worker safety • Predictive maintenance
Small farm profitability	Small farms have limited resources and capabilities. IoT use helps optimize resources and capabilities, increase production yields and operational efficiencies and minimize operational costs. IoT helps small farmers become more resilient, competitive and profitable.	• Farm management • Soil moisture monitoring • Smart irrigation • Drones • Water management • Predictive maintenance
Global food shortage	Increase production yields, reduce waste and spoilage to meet growing demand in domestic and international markets.	• Pest and crop disease monitoring • Animal health monitoring • Climate/weather monitoring • Soil patterns • Pesticide application • Fertilizer application

Figure 13-2: Agriculture: Use Case and Industry Challenges Alignment

© Strategy of Things, 2025. All rights reserved.

13.2.1.2. IoT use case details

Figure 13-3 below provides additional details on the use cases shown in Figure 13-1.

Category	Use case	Definition
Precision Farming	Climate monitoring	Monitor and forecast environmental conditions across fields, planting, harvesting, plant health and pest management.
	Soil patterns	Monitor and measure soil humidity, moisture, fertilization and temperature.
	Pest and Crop Disease Monitoring	Detect and deter pests. Early and automated detection of plant diseases through sensors and cameras.
	Irrigation monitoring	Optimize irrigation systems by monitoring weather conditions and soil moisture conditions.
	Crop tracking and tracing	Track crop growth from seeding to harvest to market.
	Farm management	Integrates business, market and sensor information. Assists in profitability, market pricing planting and optimizing decisions.
	Drones[299]	Unmanned aerial vehicles for pesticide spraying, soil/field analysis, planting, crop monitoring, field moisture, crop health assessments.

[299] "Six Ways Drones Are Revolutionizing Agriculture", MIT Technology Review, July 202. Link

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Definition
Livestock Management	Animal health	Monitor animal health, activity, temperature and nutrition.
	Heat stress levels[300]	Monitor and calculate temperature-humidity index, heat load index, accumulated heat load units.
	Physical gestures recognition and patterns[301]	Track animal health through monitoring of behavior and gestures such as running and grazing, sitting, sleeping and standing.
	Rumination	Monitor food digestion and regurgitation.
	Heart rate	Monitor livestock heart rate health for agitation and stress.
	GPS based monitoring	Monitor livestock movement and grazing patterns, feed and water placement and behavior change detection.
Greenhouse Monitoring	Water management	Optimize irrigation systems by monitoring weather conditions and soil conditions.
	Plant monitoring	Monitor plant conditions, use images for disease detection, etc.
	Climate monitoring	Monitor and measure soil humidity, moisture, fertilization and temperature.
	Indoor farming	Monitor and optimize proper combination of temperature, humidity, water and light.

[300] "What is Cattle Heat Stress?", Kestrel Instrument. Link

[301] "Understanding How Cows Feel Using AI?", Tokyo Institute of Technology. Link

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Definition
Supply Chain and Logistics	Transportation tracking	Asset tracking of the vehicles, as well as the individual containers/shipping units of the food as it leaves the farm or the processing plant.
	Environment conditions monitoring	Temperature and humidity levels within the trucks as produce is transported.
	Traceability	Trace food supply back to source of supply or production.
Equipment/ Tools and Machinery	Predictive maintenance analytics	Sensors and algorithms detect and determine maintenance issues and service needs before failure.
	Autonomous vehicles/tractors	Sensors and algorithms, combined with GPS or other location tracking technology enable robot vehicles and machinery to operate in the fields.
	Storage tank monitoring – fuel, water	Monitor levels automatically and alerts staff when levels are low.
	Worker safety	Wearables, sensors, algorithms, location and movement tracking monitor workers, especially those involved in hazardous operations, or lone workers in fields, to prevent potential injuries and to respond to emergencies.

Figure 13-3: Agriculture: Use Case Details

© Strategy of Things, 2025. All rights reserved.

13.2.2. Market views of IoT in agriculture

To understand market views on IoT and to inform on our gaps discovery and analysis, our research team conducted a survey of 450 people, from adopters to solution providers, across the nine industries studied. The survey respondents were asked their opinion on the importance of IoT for the agricultural industry over the next 5 to 10 years. Despite the transformative potential of IoT, Figure 13-4 below shows that respondents expected a relative medium to low impact of IoT in agriculture, compared to other industries. Adoption resistance challenges, discussed in the gaps section of this appendix, may partially explain this result.

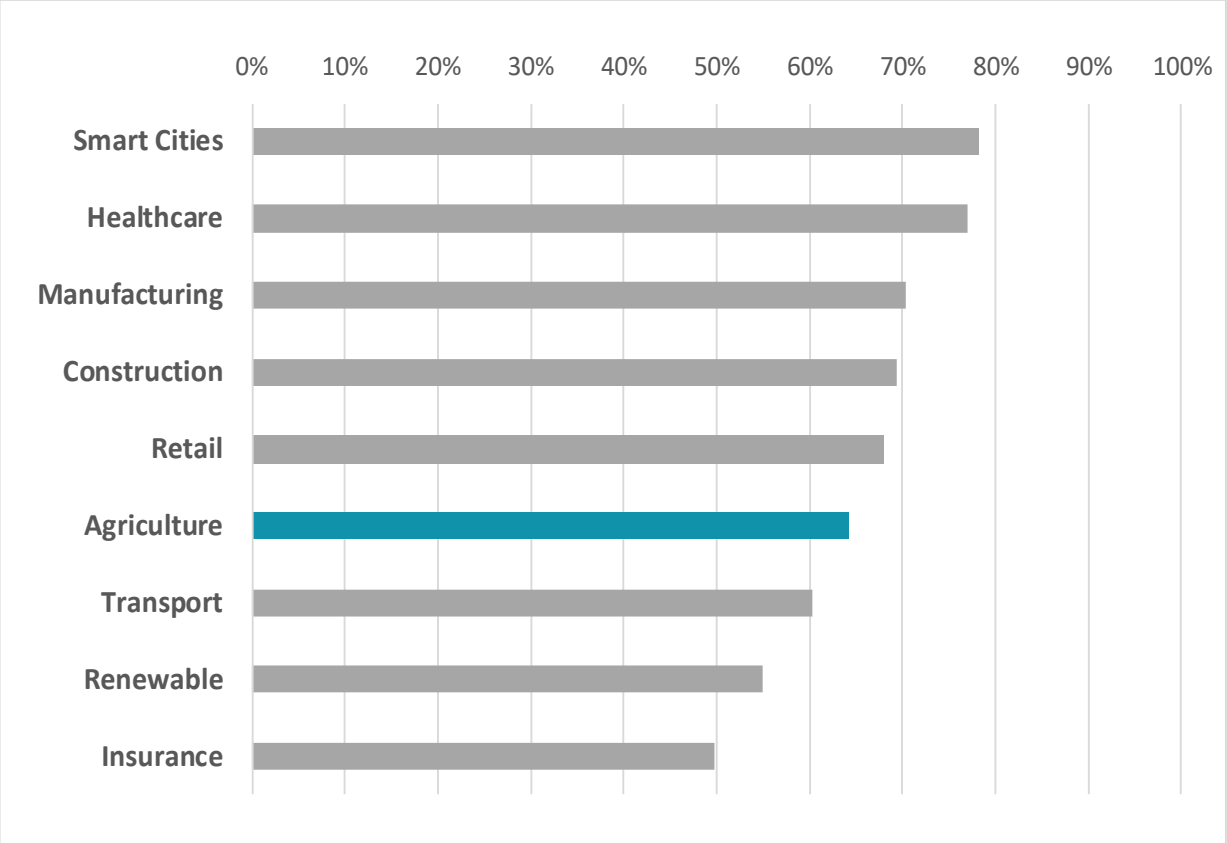


Figure 13-4: Agriculture: Importance of IoT

Survey respondents were also asked to rate the impact of the use cases categories on the agricultural industry.[302] Figure 13-5 below shows the percentage of responses in each impact category for each use case category. Overall, this shows a bias to a moderate to high impact of the use case categories in agriculture. This result indicates that within the agricultural industry, those who are familiar with and may have adopted IoT, believe that IoT provides value.

[302] In your view, what will be the impact of these use cases in agriculture over the next 5-10 years?

© Strategy of Things, 2025. All rights reserved.

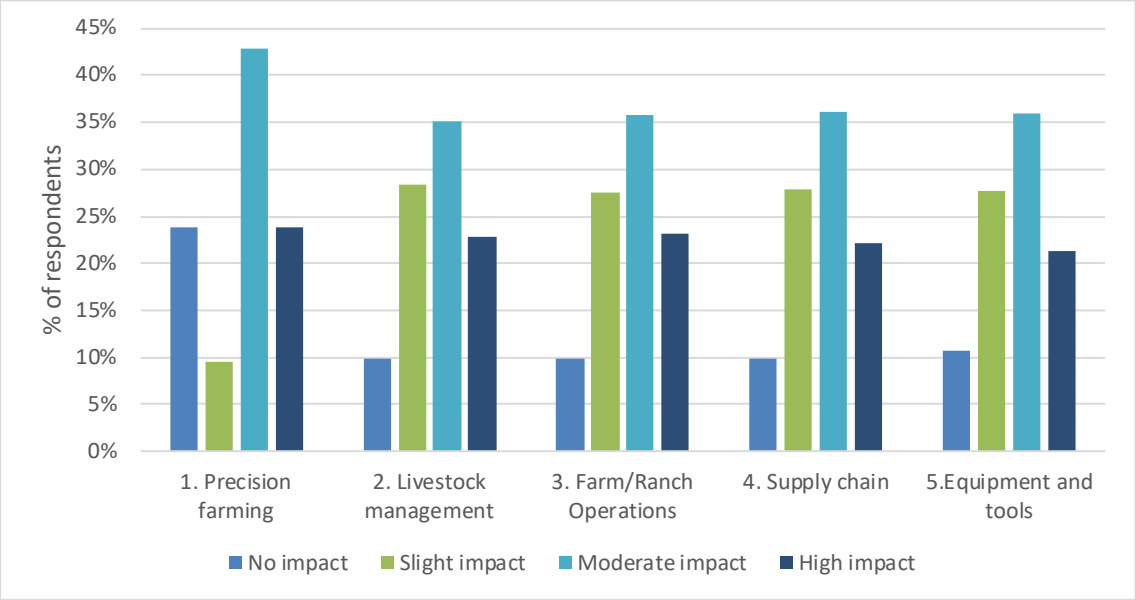
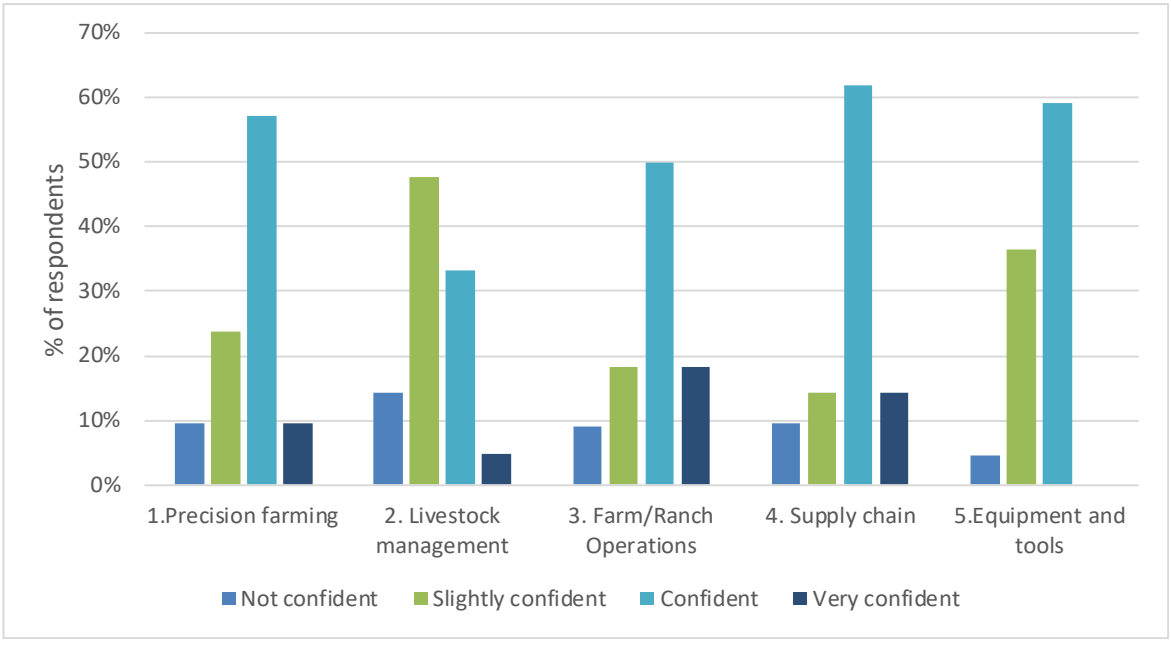


Figure 13-5: Agriculture: Use Case Category Impact

In addition, respondents were asked about their confidence in suppliers delivering the services required to operationalize these use case categories.[303] Figure 13-6 below shows the percentage of responses in each confidence category for each use case category. Overall, this indicates some confidence in the ability of suppliers to deliver the necessary services.



[303] How confident are you that suppliers will deliver the services that agricultural organizations need from these technologies over the next 5-10 years?

© Strategy of Things, 2025. All rights reserved.

Figure 13-6: Agriculture: Confidence in Suppliers Delivering

13.3. IoT gaps and findings in agriculture

A combination of interviews, secondary research and surveys was conducted to identify and understand the opportunities and challenges to the development and adoption of IoT. Each research method approached the challenges from a different perspective.

For example, the survey targeted a large audience but asked specific questions that supported the economic analysis. The interviews targeted a small number of people who provided deeper insight and context to supplement the information already collected. Finally, the desk research, consisting of a review of online news articles, published research reports, vendor and government white papers, blogs, webinars, videos and other content, provided a broad overview of the application of IoT in the industry.

In our survey, respondents were asked to choose the most important technology areas to operationalize IoT in their industry. Figure 13-7 below shows the respondent's selections of the top 10 IoT technologies and the percentage of respondents who chose that technology.[304] The survey results are not seen as a technology gaps list, but rather an indication of what is important to the respondents. This information partially informs the gap selection process.

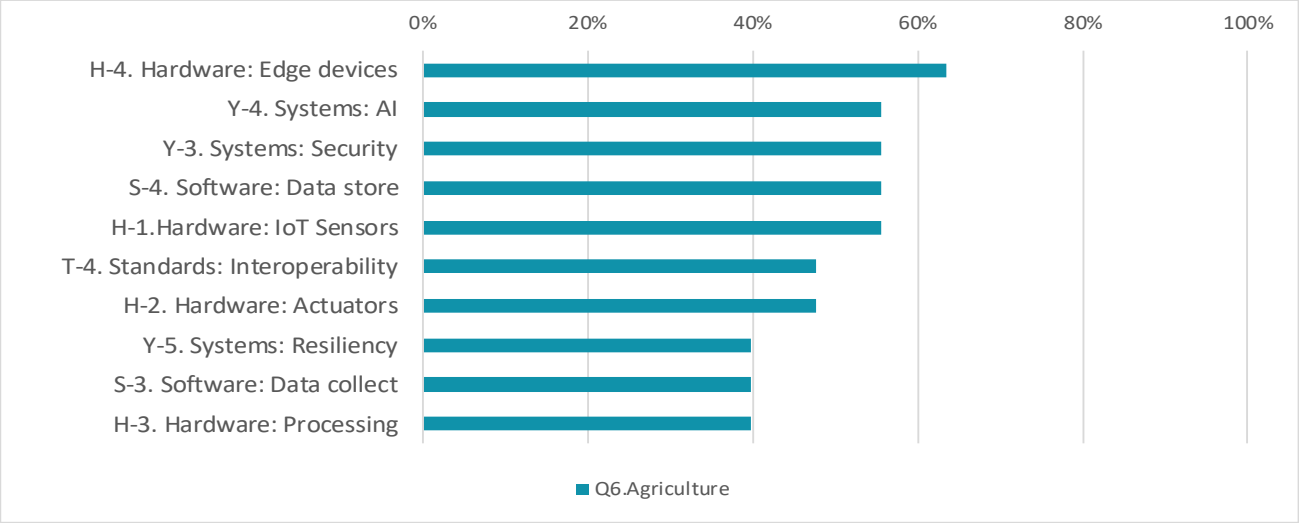


Figure 13-7: Agriculture: Top 10 Most Important Single Technologies

13.3.1. Top technology challenges

Based on the approach described above, three IoT technology challenges were identified. These are:

- Connectivity
- Edge computing and processing

[304] Respondents were asked to choose up to 5 out of the 25 technologies listed.

© Strategy of Things, 2025. All rights reserved.

- Interoperability

13.3.1.1. Challenge # 1: Connectivity

The ranked technology gaps methodology and survey did not identify connectivity as a gap. Our analysis attributed this result to survey respondents assuming that the connectivity gap was not a research and technology challenge, but an infrastructure investment and funding challenge.

Our overall broader analysis, however, identified connectivity as one of the largest barriers to IoT adoption and precision agriculture. Without connectivity, IoT sensors and other "precision agriculture" equipment are unable to send their data to remote data centers in the cloud for processing and storage.

The connectivity gaps are apparent in several ways, including availability of broadband service to the farm, connecting to the field and future needs. The benefits of overcoming these challenges are significant. A USDA report estimated that realizing the full potential of rural broadband and next generation precision agriculture technologies, could lead to "$47–$65 billion annually in additional gross benefit for the U.S. economy."[305]

> *For many farmers today, employing a drone means downloading the data on a thumb drive, uploading it off site, waiting three to five days for processing of the data and compiling a report before action can be taken in the field.*[306]

Lack of broadband to the farm. Agricultural producers are in rural areas where there is limited broadband infrastructure and Internet service. The FCC considers 25/3[307] service to be the broadband benchmark capable of providing the "advanced telecommunications capability" that enables users to "originate and receive high-quality voice, data, graphics and video telecommunications."[308]

This asymmetric level of performance, however, is insufficient for precision agriculture needs which sends large amounts of data, such as drone imagery and mapping data, to cloud data centers for processing to support critical decision-making in a timely manner.

The U.S. Federal Communications Commission (FCC) 2020 Broadband Deployment Report, estimated that 22.3% of the 50 million people who live and work in rural areas, have no coverage for 25/3 Internet service at the end of 2018.[309]

The actual number of people in rural areas without broadband Internet service is likely higher than reported. Although the FCC broadband report states that 77.7% of the rural population have

---

[305] "A Case for Rural Broadband", USDA, April 2019. Link

[306] "Examining Current and Future Connectivity Demand for Precision Agriculture, Interim Report December 2, 2022." Link

[307] 25 Mbps download and 3 Mbps upload speeds. On March 14, 2024, the FCC has updated its definition of broadband service from 25/3 to 100/20 Mbps. Source: "FCC increases broadband speed benchmark," FCC News Press Release, Federal Communications Commission, March 14, 2024. Link

[308] "2020 Broadband Deployment Report", FCC 20-50, April 24, 2020, Page 6. Link

[309] "2020 Broadband Deployment Report", FCC 20-50, April 24, 2020, Page 19. Link

© Strategy of Things, 2025. All rights reserved.

25/3 coverage available, that does not imply that they have subscribed to service in their homes or businesses.

In addition, the FCC relies on self-reported data, through form 477, provided by the telecommunications carriers and Internet service providers to build their broadband coverage maps. These data, however, have been found to overstate the actual broadband coverage. One study found that instead of 24.7 million people not having access to 25/3 Internet service, as many as 160 million people do not have access to this level of service.[310]

Mobile LTE connectivity service, from wireless telecommunications providers, is used by residents and businesses as an alternative to fixed terrestrial services. While 10/3[311] service does not meet the benchmark for "advanced telecommunications capability," the FCC broadband report found that 16.7% of people living and working in rural areas do not even have 10/3 coverage availability.[312]

Several initiatives are available to help close the rural connectivity gap. The Bipartisan Infrastructure Law (BIL) provided $65 billion for broadband infrastructure investments and lowering Internet service costs for consumers.[313]

And the United States Department of Agriculture (USDA) continues to award grants and loans for rural broadband projects through several programs, including the ReConnect[314] and Community Connect.[315] For example, the USDA announced in October 2022, that it is providing $759 million in grants and loans to bring broadband Internet to residents and businesses in 24 states, Puerto Rico, Guam and Palau.[316]

In addition to government investments, the private sector is planning to deliver Internet services in innovative ways. For example, several companies have launched or are planning to launch low earth orbit (LEO) satellite low latency broadband service.[317]

Limited connectivity in the field. While there is emphasis on bringing connectivity to the farm, or the "last mile", IoT for agriculture requires that connectivity be brought to sensors in the field, or the "last acre."[318] This connectivity can be from the field to the farmhouse or from the field to the cloud. Connecting the "last acre", however, is challenging.

---

[310] "Microsoft: FCC's Broadband Coverage Maps Are Way Off", C. Mihalcik, CNET, April 19, 2019. Link

[311] 10 Mbps down, 3 Mbps up

[312] "2020 Broadband Deployment Report", FCC 20-50, April 24, 2020, Figure 2b. Link

[313] "Fact Sheet: The Bipartisan Infrastructure Deal", White House Statement and Releases, November 6, 2021. Link

[314] "ReConnect Loan and Grant Program", USDA. Link

[315] "Community Connect Grants" , USDA, June 2023. Link

[316] "Biden-Harris Administration Provides $759 Million to Bring High-Speed Internet Access to Communities Across Rural America", USDA Press Release 0230.22, October 27, 2022. Link

[317] "LEO Satellite Networks – Fast Rural Internet at Reasonable Cost?", R. Renner, Frontier Centre for Public Policy, December 20, 2020. Link

[318] "Examining Current and Future Connectivity Demand for Precision Agriculture", Interim Report FCC, Precision Agriculture Connectivity Task Force, December 2022, Page 2. Link

© Strategy of Things, 2025. All rights reserved.

American farms vary in size. While the average size of the American farm in 2021 was 445 acres, the average size of farms generating over $1,000,000 in revenue was 2,920 acres, while those generating between $500,000 and $1,000,000 were slightly smaller at 1,942 acres.[319] The largest farm in the United States spans 190,000 acres[320], while the largest ranch spans 825,000 acres.[321]

Wireless technologies provide a scalable and economical way of covering vast areas of land. Commercial wireless telecommunications services are absent, however, in some areas because the providers are reluctant to build new or additional radio towers and infrastructure due to unfavorable economics, construction challenges and inability to secure suitable "right of ways."[322] Private wireless networks are financially unfeasible to all but the largest farms that have the capital and access to resources to operate this network.

Finally, signal attenuation and blockage can also impact "last acre" connectivity. Some areas cannot be covered due to geography and topographic challenges. One common problem is signal attenuation due to hills and tree foliage.[323] For example, wireless signals from soil moisture sensors placed underneath the tree canopies in an orchard, have difficulty communicating with gateways or with distant cell towers. One technology solution provider interviewed for this research reported that soil moisture sensors placed underneath leafy vegetables had experienced difficulties communicating with the gateway.

In addition, environmental conditions such as heavy rain, high humidity and heat weaken wireless signals and further reduce signal propagation.

Some emerging options to address these "last acre" challenges include IoT connectivity provided by next generation low earth orbit satellites, as well as the utilization of TV white space frequency bands.

The allocation of lower frequency bands, which travel farther and can penetrate trees and canopies, should be examined to understand how they interoperate and integrate into a multi-connectivity distributed architecture environment.

Evolving connectivity capabilities with future needs. The Connectivity Working Group of the FCC Precision Agriculture Connectivity Task Force identified two initial connectivity service profiles[324]:

- "Low speed, broad coverage" for transmission of sensor data from the fields, systems automation and monitoring and mobile access of systems and data for workers and

[319] "Farms and Land in Farms, 2021 Summary", USDA National Agricultural Statistics Service, February 2022. Link

[320] "Top 5 Farms with the Largest Acreage in the U.S.", E. O'Keefe, Successful Farming, September 28, 2019. Link

[321] "King Ranch", Wikipedia. Link

[322] "Rural Broadband Access in the United States", Center Forward, February 2021. Link

[323] "Factors That Affect Lora Propagation in Foliage Medium", R. Anzum, The 18th Learning and Technology Conference, Procedia Computer Science, Volume 194 (2021), Page 149-155

[324] "Task Force for Reviewing the Connectivity and Technology Needs of Precision Agriculture in the United States", FCC Precision Agriculture Connectivity Task Force, November 10, 2021. Link

© Strategy of Things, 2025. All rights reserved.

decision makers. Connectivity service is low speed, asymmetric upload and download and non-latency sensitive.

- "High speed centralized" for transmission of farm-level data aggregation and modeling, raw data uploads for processing and remote training and systems support. Connectivity service is from a centralized location and is high speed, low latency and has symmetric upload and download speeds.

Today's connectivity models are, however, insufficient and will need to evolve to support future use cases that involve autonomy, robotics, computer vision and large amounts of sensor data. The amount of information and communication in the field requires a stable and continuous connection, higher bandwidth and symmetric upload and download speeds. For example, in row crop farming, machines equipped with GPS, computer vision, sensors and connectivity, operate autonomously to perform a variety of farming tasks, from soil preparation, seed planting to weeding and harvesting.

These smart machines communicate and coordinate with other nearby machines for offloading, refueling and tracking. In addition, the machines collect information, which is sent to the farm operations center, in real time for monitoring, processing and action.

Similarly, innovative new types of robotics are emerging in livestock farming. For example, mobile autonomous cattle feeders[325] which deliver feed to the fields and drones[326] which track cattle and monitor animal health, can cover large areas of land without human intervention. To support these types of high bandwidth needs, the future standard for upload speed is expected to be 1 Gbps from the current upload standard of 3 Mbps.[327]

As the fields become more connected and new connectivity methods, such as satellite services are used, allocation of additional radio frequencies and spectrum management will play a key role to support future bandwidth, speed and coverage needs while minimizing interference. The Connectivity Working Group has identified spectrum policies, management and allocation as critical considerations.[328]

13.3.1.2. Challenge # 2: Edge computing and processing

Agriculture is an information business. Agricultural producers have long used data to make decisions to maintain animal and crop health, maximize yields of produce, fruit and animal products and minimize operational costs. IoT provides new data sets not possible before and that new data set enables agricultural producers to make decisions in real time and act, as well as optimize and plan for the next seasons.

---

[325] "Robot Feeder Caters to Cattle", W. Vogt, Western Farm Press, March 14, 2022. Link

[326] "The Drones Watching Over Cattle Where Cowboys Cannot Reach." D. Singer, BBC. Link

[327] "Task Force for Reviewing the Connectivity and Technology Needs of Precision Agriculture in the United States", FCC Precision Agriculture Connectivity Task Force, November 10, 2021, Page. 60. Link A 300 fold increase.

[328] "Task Force for Reviewing the Connectivity and Technology Needs of Precision Agriculture in the United States", FCC Precision Agriculture Connectivity Task Force, November 10, 2021, Page 57. Link

© Strategy of Things, 2025. All rights reserved.

Processing all this data in the cloud is not feasible as moving large amounts of data to the cloud for processing and storage is expensive. Further, not all data collected needs to be stored or processed in the cloud. To enable and sustain smart agriculture, some of these data must be processed on the farm. By processing IoT data locally, timely analysis can be performed to yield key insights that support real time decision making. For example, smart machines employ computer vision to identify ripe fruit to be picked, then send the collected data to servers on the machines or in the farmhouse to be analyzed. Fruit picking robots follow the machine and pick the fruit immediately.

Farms of the near future will integrate sensors, drones, robotics and autonomous machines in many aspects of their daily operations. To support these applications, farms will employ enabling edge and cloud infrastructure and technologies.

Edge computing in agriculture is, however, still nascent and several challenges must be addressed. A survey of recent research in edge computing in agriculture found research papers focused in the areas of latency sensitive analytics, edge mining for data compression, computation offloading, reducing data traffic, reducing latency and distributed data collection.[329]

Some examples of the challenges of edge computing, synthesized from a research literature search,[330] [331] to be addressed include:

- **How, where and when should processing be best performed?** Processing can be performed on IoT devices, edge servers on drones and mobile machines, farmhouse servers and the cloud. Key considerations include processing latency, communications latency, processing resources and capacity available, type of processing to be performed, energy consumption, cybersecurity, scalability, reliability of the communications network and the use case.

  Processing can be predefined or assigned dynamically or offloaded based on various parameters. Continued study and development of distributed architectures, resource assignment algorithms and interaction models is required to address this topic.
- **How can edge devices support advanced data processing?** There are multiple approaches being pursued. One approach uses the development of machine learning codes that run on resource constrained devices. Another approach focuses on the development of AI capable microprocessors and microcontrollers on IoT devices. A third approach would be to dynamically split the process into tasks and divide the processing into multiple devices and servers based on resource availability considerations.

  There is no single model and the future farm will likely incorporate all three models. As the adoption of smart agriculture and new applications and device types emerge,

[329] "Edge Computing: A Tractable Model for Smart Agriculture?", M.J. O'Grady et al, Artificial Intelligence in Agriculture, Volume 3, 2019, Pages 42-51, ISSN 2589-7217. Link

[330] "Overview of Edge Computing in the Agricultural Internet of Things: Key Technologies, Applications, Challenges," in IEEE Access, vol. 8, pp. 141748-141761, 2020, doi: 10.1109/ACCESS.2020.3013005, X. Zhang, Z. Cao and W. Dong. Link

[331] "Edge Computing Challenges and Their Solutions", GreyB blog. Link

© Strategy of Things, 2025. All rights reserved.

however, continued research and development of the approaches is necessary to sustain and maximize the outcomes and benefits.

- **How can edge processing on mobile devices (mobile edge computing), such as drones, moving machines and equipment swarms be operationalized at scale?** Mobile devices present new challenges, such as variable signal coverage and communication latencies, moving frames of reference, identification, authentication and access to nearby devices and services based on location and data exchange with the edge and cloud networks. Continued research and development into operating modes, algorithms, models and interoperability requirements is required for seamless integration into farm networks and operations.
- **How to ensure maximum cybersecurity and privacy protection for edge devices in a large network where devices are often changed?** The placement of edge servers and processors on machines and devices in the field poses physical security concerns. Each device type and model may, however, have unique vulnerabilities and characteristics and the ability to manage, update or remove those devices from the network at scale is challenging.

  In addition, the devices collect data which may be stored locally and must be managed, protected and deleted. Finally, access to the devices, whether from humans or other machines, must be managed. IT centric management models and policies are not compatible with the agricultural IoT networks because of issues like device mobility, heterogeneity and accessibility.
- **How should data collected for edge processing be managed?** While IoT sensors collect vast amounts of data, only a small set of it is analyzed at the edge. For example, video sensors on a machine may capture pictures of ripe and unripe fruit to determine what should be picked, but only the pictures of the ripe fruit are analyzed and sent to the robot for picking.

  Farm managers are faced with what to do with the data that is used and unused, where that data should be stored, for how long and who and what other devices should have access to the data. To support edge processing at scale on the farm, new architectures and algorithms are needed that account for the distributed nature of the compute resources and its unique set of requirements.
- **How should IoT edge devices and servers be integrated into a farm's operations?** The introduction of edge devices and processors in a farm adds additional complexity. In addition to the maintenance of farm equipment, farm operations must also support the maintenance and management of these devices. With the potential of thousands of sensors on a farm, new operational, troubleshooting and maintenance models, tools and resources must be developed.

13.3.1.3. Challenge # 3: Interoperability

Farms have a variety of machines and equipment, from the "latest and greatest" equipment with current technology to 30- to 40-year-old legacy equipment with limited technology and no connectivity.

© Strategy of Things, 2025. All rights reserved.

Because of the high capital costs for new equipment, "right to repair" issues and operating costs, farmers are buying old equipment. In farm auctions in the Midwest, tractors manufactured in the late 1970s and 1980s are some of the fastest selling items.[332] The most recent USDA Census of Agriculture, conducted in 2017, reported that tractors less than five years old represented only 9.9% of farm tractors less than 40 hp, 9.8% of tractors between 40 and 99 hp and 14.5% of tractors greater than 100 hp.[333]

Interoperability challenges are a major barrier to IoT adoption and value realization in agriculture where old and new equipment work together. Many of the machines employ a variety of proprietary and incompatible protocols that make sharing information with each other, as well as with farm operations software difficult or impossible.

For example, some equipment may incorporate incompatible physical connections and require the use of adapters to communicate with other equipment. Others may have different formats or syntaxes for the same data, while others have different meanings for the same data. Old equipment may not work with newer equipment, despite coming from the same manufacturer. In addition, the data may be encrypted and not accessible to other users.

> *... the agriculture industry's default model, pioneered by machinery manufacturers, is to develop and market software and devices in proprietary formats. This has created a situation where thousands of devices and systems operate in their own ecosystem with different data formats and languages. As a result, the industry is full of single point solutions that get data elements from point A to point B, with no standardized way to connect and exchange data between these points.[334] Farm Foundation*

> *CAN-Bus standard has been around for a long time… manufacturers use the data carried through CAN-Bus for themselves, but some of that data is of value for others. However, while CAN-Bus is somewhat open and an industry standard, the messages it carries are encoded in proprietary ways [by the manufacturer] and not available to the farmers or users.[335] Dennis Buckmaster, Purdue University*

There are several reasons for the lack of interoperability. The key reason is a lack of industry wide structural and semantic interoperability.[336]

Structural interoperability focuses on a common data structure and format between the exchanging parties. Semantic interoperability focuses on a common definition of the data being exchanged between the parties.

---

[332] "For Tech-Weary Midwest Farmers, 40-Year-Old Tractors Now a Hot Commodity", A. Belz, Minneapolis Star-Tribune, January 5, 2020. Link

[333] "2017 Census of Agriculture", United States Summary and State Data, Volume 1, AC-17-A-51, April 2019, USDA, Table 45. Link

[334] "Data Interoperability in Agriculture", Farm Foundation Issue Report, September 2021. Link

[335] Interview notes - D. Buckmaster, Professor, Purdue University, August 17, 2020.

[336] "Data Interoperability in Agriculture", Farm Foundation Issue Report, September 2021, Page 4. Link

© Strategy of Things, 2025. All rights reserved.

Many companies are reluctant to share because they view other services as competitors.[337] Others believe that their technology approach is superior and that aligning with open standards, will result in commoditizing their solutions.

A venture capital backed agriculture IoT start-up company volunteered that the reason their investors invested was because of the potential for above average revenue growth opportunities.[338]

Finally, development of standards is well suited for mature and established applications and processes, but less so in "actively innovating" areas where knowledge is rapidly being obtained.[339]

The FCC Precision Agriculture Connectivity Task Force, in its report, listed several factors that hinder the industry from reaching interoperability. These include[340]:

- Large numbers of diverse stakeholders from the agriculture ecosystem need to be involved, such as farmers, manufacturers, input providers, service providers, consultants, government agencies, technology companies
- Both public and non-public data, created and used by the various stakeholders, are stored across multiple cloud platforms
- Nascent market for data in agriculture with few standards
- Inherent complexity between individual product solutions and those from manufacturers interoperating toward a common task

There are several organizations working on various aspects of the interoperability challenge. Representative efforts and projects include:

- **AgGateway's ADAPT.** This open-source framework and toolkit facilitates interoperability between different software and hardware applications. The framework maps multiple data formats into a common agriculture model.[341]
- **The Agricultural Industry Electronics Foundation.** This foundation is developing the Agriculture Interoperability Network (AgIN), focusing on guidelines for data formats to facilitate data sharing for end users, growers and operators[342]

[337] "Interoperability – Why It's Essential for the Future of Digital Agriculture." Link

[338] Various interviews conducted as part of this research with IoT ag startups.

[339] "Data Interoperability in Agriculture", Farm Foundation Issue Report, September 2021. Link

[340] "Task Force for Reviewing the Connectivity and Technology Needs of Precision Agriculture in the United States", FCC Precision Agriculture Connectivity Task Force, November 10, 2021, Page 81. Link

[341] ADAPT Standard Development, AgGateway. Link

[342] "Agriculture Interoperability Network to Simplify Data Sharing", B. Schultz, Diesel Progress, July 18, 2022. Link

© Strategy of Things, 2025. All rights reserved.

- **Demeter.** Supported by the European Union, is an "overarching solution that integrates various heterogeneous hardware and software resources and enables the seamless sharing of data and knowledge throughout the agri-food chain."[343]
- **The Open Ag Data Alliance.** Led by the Open Ag Technology and Systems (OATS) group at Purdue University, is developing an open-source standard API framework for automated data exchange with the cloud.[344]
- **The DataConnect platform.** Developed by a partnership of several large agricultural manufacturers and service providers, is a manufacturer independent, cloud to cloud solution that was designed to simplify data sharing.[345]

Interoperability is a prerequisite for large scale, cross-boundary, cross-system data sharing—the necessary infrastructure of a traceable, sustainable and innovative 21st century supply chain.[346]

13.3.2. Other challenges

In addition to the technology challenges for further consideration, our research has identified other challenges that impact IoT adoption. These challenges did not meet the criteria for research consideration because they were either not a technology challenges or a technology related challenge that can be addressed by current marketplace offerings or capabilities.

These include:

- Service and repair of smart equipment
- Digital skills
- Adoption resistance
- Data ownership and sharing

13.3.2.1. Service and repair of smart equipment

Modern agricultural equipment, such as tractors, combine harvesters and precision farming equipment, employs computers, electronics, sensors and software systems. Unlike older equipment which can be repaired by farmers, only authorized dealers can repair the new equipment. These repairs are expensive and may take days or weeks before dealer technicians complete the work. This delays time-critical planting and harvesting activities and jeopardizes farm revenues. Due to these concerns, some farmers are turning to hacked software from

[343] Empowering Farmers, EU, demeter. Link

[344] Open Ag Data Alliance, 2021. Link

[345] "DataConnect Platform to be Unveiled at Agritechnica", Precision Farming Dealer, October 4, 2019. Link

[346] "Data Interoperability in Agriculture", Farm Foundation Issue Report, September 2021. Link

© Strategy of Things, 2025. All rights reserved.

Ukraine,[347] while others are purchasing older equipment that they can service and repair themselves. [348]

Several farming organizations and independent repair shops have been advocating for the "right to repair" legislation that would allow farmers and other equipment owners to access the information, software and tools needed to repair their own equipment.[349]

Such laws require manufacturers to provide repair manuals, diagnostic tools, software and other information to equipment owners, as well as making it illegal for manufacturers to use digital locks and other technologies to prevent equipment owners from making repairs.

As of April 2022, twenty-seven U.S. states have introduced "right to repair" legislation although not all are concerned with agriculture equipment.[350] In addition, a federal Agricultural Right to Repair Act bill was introduced in February 2022 and is undergoing consideration.[351]

In response to growing pressure, one of the agricultural equipment manufacturers, Deere & Company signed a memorandum of understanding (MOU) with the American Farm Bureau Federation (AFBF) to formalize the availability and access to parts, tools, software and documentation for repairs and maintenance at independent repair facilities.[352] The "right to repair" issue, however, is an industrywide concern as agricultural equipment and other supporting equipment increasingly incorporate digital elements.

13.3.2.2. Digital skills

As digital and emerging technologies are increasingly integrated into agricultural equipment and operations, the skills that agriculture workers need to be successful will change. For example, as smart machines increasingly automate previously manual activities, agriculture jobs will evolve from being low skill, repetitive physical work to medium to high skill, non-repetitive digital work.

Automation will shift the focus to critical human centric tasks, such as creativity, leadership, complex information processing and interpretation. The future agricultural workforce will need technical, cognitive and advanced people skills.[353]

---

[347] "Farmers Are Having to Hack Their Own Tractors Just to Make Repairs", S. Schrader, The Drive, February 9, 2021. Link

[348] "Senate Introduces Bill to Allow Farmers to Fix Their Own Equipment", L. Matsakis and O. Solon, NBC News, February 1, 2022. Link

[349] "Farmers Deserve the Right to Repair Their Tractors", H. Packman, National Farmers Union, May 24, 2021. Link

[350] "Half of U.S. States Looking to Give Americans the Right to Repair", N. Proctor, PIRG, April 22, 2022. Link

[351] "TFB: Agricultural Right to Repair Act introduced", G. Joiner, Morning Ag Clips, February 1, 2022. Link

[352] "NAEDA Comments on John Deere Right to Repair MOU.", Farm Equipment, September 2023. Link

[353] "What Will Be the Capabilities and Skills Needed to Manage the Farm of the Future?", Farmdoc Daily, April 2021. Link

© Strategy of Things, 2025. All rights reserved.

The advances of agriculture technology have put pressure on farm workers to have higher skills and technical understandings than that of previous generations. Some of the technical skill sets required for the future farmer will include:

- **Data analysis and management.** This includes the ability to collect, analyze and interpret large amounts of data from various sources, such as sensor networks, drones and satellite imagery.[354]
- **Precision agriculture.** This involves the use of technology, such as GPS, to increase the efficiency and precision of farming operations, such as planting and harvesting.[355]
- **Robotics and automation.** This includes the ability to design and program robots and autonomous systems for tasks such as planting, harvesting and soil analysis.
- **Computer vision.** This involves the use of computer algorithms to interpret and make sense of images and videos, such as those captured by drones.
- **IoT and connectivity.** This includes the ability to connect different technologies and systems, such as sensors and machines, to enable the collection and sharing of data.[356]
- **Networking.** The understanding of available networks, how they are set up, operated, secured and how they support IoT connectivity.
- **Systems Integration.** The ability to bring together different technologies, systems and data to operate as a single system, increasing the value of systems to the farmer.
- **Cloud computing.** This involves the use of remote servers for data storage, processing and analysis and machine learning.
- **Cybersecurity.** Understanding how to protect systems, networks and data from malicious attacks is also important.[357] [358]

Technology adoption tends to be more widely embraced by younger generations often called "digital natives." Currently, the average age of the American farmer is 60[359], which means the aging farmer must adapt and work to attract the younger generation of future farmers through careers involving technology and innovation.

The digital skill gap is likely to remain an issue however, as competition for technical skills will grow with increasing demand. Some of the reasons behind the skills gap besides age include:

- **Lack of funding.** Some farmers and agricultural workers, especially small sized farms may not have the financial resources to invest in training and new technology.[360] Small farms have shown a lower level of technology adoption compared to medium and large

[354] "Modern Farming is as Much About Data as Digging…", World Economic Forum, June 2021. Link

[355] "The Skills Needed to Manage a Farm in the Future", AG Daily, April 2021. Link

[356] "Agriculture's Connected Future: How Technology Can Yield New growth", McKinsey, October 2020. Link

[357] "Cybersecurity Skills Are Vital for the Forth Agricultural Revolution", Digital Tories. Link

[358] "The Importance of Cybersecurity in Modern Agriculture", Research Gate, June 2021. Link

[359] "Technology Holds Key to Agriculture's Aging Problem.", Precision Farming Dealer, April 2022. Link

[360] "The U.S. Farm Labor Shortage", Ag America, June 2022. Link

© Strategy of Things, 2025. All rights reserved.

farms, pointing towards a lack of skills and resources to effectively deploy agricultural technology.[361]

- **Resistance to change.** Some farmers and agricultural workers may be resistant to adopting new technology, which can make it difficult for them to acquire the necessary skills.[362]
- **Lack of education and training opportunities.** Many farmers and agricultural workers may not have access to the education and training needed to develop the digital skills required for modern agriculture.

With the advent of emerging digital technologies such as AI, IoT, robotics and other automation technologies, the gap will likely become even more pronounced.

13.3.2.3. Adoption resistance

Despite the benefits of IoT and precision agriculture technologies and solutions, uptake of these solutions has been uneven and may take as long as 15 years for the technology to reach a critical mass.[363] Large producers are more likely to adopt these technologies compared to smaller farms because they have access to a skilled workforce, are less wary of technology and have economies of scale.[364]

For example, a USDA Economic Research Report found that the adoption rates for GPS soil/yield mapping, guidance systems and Variable Rate Technology (VRT) were 80%, 84% and 40% respectively for corn farms over 3800 acres. In contrast, for corn farms less than 600 acres, the adoption rates for the same precision agriculture technologies were all at 12%.[365]

While all farmers want to increase production yields, there are several reasons that may slow adoption. Some of these reasons, including the limited availability of broadband and connectivity in rural areas and "right to repair", have been discussed in previous sections. Our research and select interviews uncovered several other reasons for the uneven adoption.

Nature vs Technology. Many agricultural producers have been farming for a long time, with "tried and true" knowledge, expertise and practices handed down from generation to generation. Much of this had been informed by historical understanding of weather patterns, hands-on experiences and knowledge exchanges with other farmers, input providers and suppliers. Even when crops benefit from agriculture innovation, the farmer may be skeptical to attribute the benefits to the technology, instead crediting what they know, such as good weather patterns or a change in the fertilizer mix.

---

[361] "Voice of the U.S. farmer in 2022: Innovating Through Uncertainty", McKinsey, September 2022. Link

[362] "Digital Skills in Farming for a Digital Future in Agriculture." National Rural Network, August 2018. Link

[363] "Adoption of Farming Technology, Or Precision Ag, Varies Across Generations", KTTN News, December 20, 2020. Link

[364] "Adoption of Precision Agriculture", USDA NIFA. Link

[365] "Farm Profits and Adoption of Precision Agriculture", D. Schimmelpfennig, USDA Economic Research Report ERR-217, October 2016. Link

© Strategy of Things, 2025. All rights reserved.

> *It is a seven-year adoption cycle. If they get good results in the first year, farmers will say 'how do you know it's not nature?'. Then you wait a second year and they say, 'how do you know it's not something I did?'. And this goes on until they believe it's the technology. Bret Beringer, Chief Engineer, Fybr*[366]

> *I could spend $50,000 on this, or I could spend the same $50,000 on more inputs where I know exactly what results I will get.*
>
> *Ron Hiller, Founder/CEO, blx.io*[367]

Poor previous experiences with technology. Other farmers who have deployed agriculture technologies have suffered from reliability and usability issues and cannot afford trial and error on their crops. Many companies have also over promised and under delivered on actionable steps derived from the data, losing farmers' trust and building new barriers that are hard to address for the next possible use case.

> *Visiting farms these days, it's not uncommon to see the ghosts of agtech promises scattering the fields. Abandoned weather stations stretch out like metal scarecrows. Forgotten soil moisture meters are nothing more than tripping hazards. The companies that installed them are long gone and the tools remain as a reminder of a failed investment.* [368]

> *Farmers hate being 'nickeled and dimed'. They just spent $200,000 for a tractor, but they hate the idea of paying $20 to $30 a month for data. They are used to buying capital, not services. Ron Hiller, Founder/CEO, blx.io*[369]

13.3.2.4. Data ownership and sharing

Producers have been perfecting their techniques for generations. Planting times, input mixes, feed formulations and crop and livestock management practices are some of their most closely guarded proprietary information that they may share with their neighbors and members of cooperatives.

One interviewee recounted an incident in which an input company came out to conduct an analysis to improve the crop performance and made some specific recommendations with a new product. The product was tried and it was a success, which yielded the farmer additional revenues. Seeing the success of the product, however, the input company raised the prices, thereby reducing the value share for the farmer.[370]

---

[366] Research interview with Bret Beringer, Chief Engineer, Fybr. March 6, 2020.

[367] Research interview with Ron Hiller, Founder, blx.io. April 10, 2020.

[368] "Farmers Have Been Burned by Agtech Too Often. Here's How to Win Back Their Trust.", AFN, November 2021. Link

[369] See note 367

[370] See note 367

© Strategy of Things, 2025. All rights reserved.

While sensors and the collected data are integral parts of precision agriculture, there is the issue of data ownership and access. This issue was reflected in a 2016 American Farm Bureau Federation survey of 400 farmers and ranchers that reported they want to control the information collected from their equipment.

Specifically, 77% are concerned with who accesses their data and whether it could be used for regulatory purposes. Two-thirds, or 67%, stated they will consider how outside parties use and treat their data when deciding which technology or service provider to use. Similarly, 61% were concerned that companies can use the farm data to influence market decisions.[371]

In a 2020 survey of 393 farmers across 44 states, when asked the question "Do you trust the following entities with the security and use of your farm's data?", 60% of the respondents did not trust "federal/state/county level government offices" and 59% did not trust private companies.[372]

> *The farmer doesn't like the idea of … who is going to use my information to make more money. Robert Tse, USDA*[373]

> *Farmers were very concerned about how that data may be used. Would it come into the hands of environmental agencies? Would it come into the hands of somebody who might use it for something other than what they paid for?. Brad Reins, USDA*[374]

[371] "Farm Bureau Survey: Farmers Want to Control Their Own Data", Precision Farming Dealer, May 12, 2016. Link

[372] "Farmer Perspectives on Data", Trust in Food research report, 2020. Link

[373] Research interview with Robert Tze, USDA. June 30, 2020.

[374] Research interview with Bradley Reins, USDA. March 26, 2020.

© Strategy of Things, 2025. All rights reserved.

Appendix: Manufacturing

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

© Strategy of Things, 2025. All rights reserved.

14. Appendix: Manufacturing

This section describes the research findings for IoT technology infrastructure in the U.S. manufacturing industry. The topics discussed are:

- Industry overview
- Use of IoT in manufacturing
- IoT challenges in manufacturing

14.1. Industry overview

Manufacturing is one of the largest industries in the United States. This section presents some core facts about the manufacturing industry as well as some key industry challenges.

14.1.1. Key facts

In 2020, U.S. manufacturing contributed $2.27 trillion to the American economy, representing 10.8% of the Gross Domestic Product (GDP). When its indirect contributions are factored in, U.S. manufacturing contributed 24.1% of the overall U.S. GDP.[375]

According to the United Nations Statistics Division, the United States accounts for 16.6% of global manufacturing by value. This makes the U.S. the second largest manufacturing nation in the world after China which accounts for 29.4%. Manufacturing in the United States is significantly larger than Japan (7.1%), Germany (5.1%) and South Korea (3.1%).[376]

US manufacturing grew at a compound annual growth of 1.9% in the five years between 2014 and 2019. In contrast, the compound real annual growth for the 25-year period between 1994 and 2019 was 2.4 %.[377] Relative to the rest of the world, these rates place the U.S. in the 2nd quartile.

The largest subsectors within manufacturing are chemicals ($398.6 B, 17% of total manufacturing value added (TMVA)), computer and electronics ($328.1 B, 14% TMVA), food and beverage and tobacco ($296.2 B, 12.6% TMVA), motor vehicles, bodies and trailers and parts ($183.6 B, 7.8% TMVA) and machinery ($161.2 B, 6.9% TMVA).

Durable goods accounted for 56.3% of the value added by manufacturing.[378] Relative to the rest of the world, the U.S. is the largest manufacturer in:[379]

- Chemicals and pharmaceuticals
- Computers, electronics and optical products
- Motor vehicles, trailers and semi-trailers
- Fabricated metal products

---

[375] "NIST Advanced Manufacturing Series 100-42, 2021. Link

[376] ibid.

[377] ibid.

[378] "2020 Q4 Seasonally Adjusted Valued Added Statistics", Bureau of Economic Analysis. Link

[379] See note 375

© Strategy of Things, 2025. All rights reserved.

- Coke and refined petroleum products
- Paper products and printing
- Other transport equipment

The U.S. exported $1.17 trillion in manufactured goods in 2020. This is a decline from $1.4 trillion in 2018 and $1.36 trillion in 2019. This decline was attributed to the impacts of developing trade policy and COVID-19.[380]

The U.S. manufacturing industry is the fifth largest employer of Americans.[381] U.S. manufacturers employed 12.8 million people in May 2022 with 57.9% of manufacturing workers employed at firms with 500 or more people. The top three sectors employing the most Americans in 2019 are transportation equipment (1.55 million), food (1.49 million) and fabricated metal products (1.38 million).[382]

In 2019 there were 243,687 manufacturing companies in the United States. Small businesses, employing 500 people or less, represent 98.3% of these manufacturers. In addition, 87.7% of the firms employ less than 50 people with 74.3% having 20 employees or less.[383]

14.1.2. Industry challenges

The U.S. manufacturing industry faces several challenges that constrain the growth of the industry. These challenges were exacerbated by the COVID-19 pandemic. Four of the most important challenges are:

- Vulnerable supply chains
- Declining labor productivity
- Labor shortages
- Future skills gap

Each of these is discussed below.

14.1.2.1. Vulnerable supply chains

The pandemic disrupted the U.S. manufacturing industry with supply chain challenges and increased raw material costs among the top business challenges.[384] While most businesses expect

[380] "Facts About Manufacturing", National Association of Manufacturers. Link

[381] "Manufacturing in America: 2021", U.S. Census Bureau. Link

[382] ibid.

[383] ibid.

[384] "Manufacturers' Outlook Survey First Quarter 2022", National Association of Manufacturers, March 17, 2022. Figure 9. Link

© Strategy of Things, 2025. All rights reserved.

these disruptions to ease, manufacturers are re-evaluating their supply chains and some are considering onshoring some parts of their manufacturing operations.[385] [386]

At the federal level, several measures to mitigate future disruptions and remake the supply chain are appearing. In February 2021, President Biden issued an executive order (E.O. 14017) to conduct a review of and address vulnerabilities in America's critical supply chains.[387]

Bipartisan legislation is undergoing consideration in both the Senate[388] and the House of Representatives.[389] This bill, known as the CHIPS for America Act, contains a provision that would provide up to $10 billion in federal grants to match state subsidies to encourage companies to build semiconductor fabs and foundries in the U.S. [390] [391]

14.1.2.2. Declining labor productivity

Labor productivity in U.S. manufacturing fell 4% over the period from 2010 to 2019. In contrast, U.S. manufacturing labor productivity increased 41% during the previous period 2001 to 2010.[392] A decline in labor productivity means that more people, or more labor hours, are required to produce the same product. This both increases the cost of the product and can lead to lower workforce wages.

The net effect of decreasing labor productivity is decreased competitiveness of U.S. manufacturers. Possible explanations for declining labor productivity include not reallocating or hiring additional resources to take advantage of productivity enhancements and innovations, decreased competition, growing income inequality, drag from the global financial crisis and recession of 2008 and slowdown in new capital investments.[393]

> *... as companies have grown, they don't necessarily reimagine what their factory floor looks like. They just bolt on different equipment or different processes. It becomes more challenging to efficiently run their machines to make whatever they're making in the factory. Joe Work, Senior Growth Advisor, MAGNET*[394]

---

[385] "Supply Chain Woes Prompt a New Push to Revive U.S. Factories", Schwartz, Nelson D., January 5, 2022. New York Times. Link

[386] "2021 State of Manufacturing Report", Fictiv-Dimensional Research Report, 2021. Link

[387] "Executive Order on America's Supply Chains", Executive Order 14017, February 24, 2021. Link

[388] S.3933 - CHIPS for America Act, June 2020. Link

[389] H.R.7178 - CHIPS for America Act, June 2020. Link

[390] The bill passed in July 2022.

[391] At the time of report submission, the CHIPS and Science Act has been signed into law on August 9, 2022.

[392] "US Manufacturing Productivity is Falling and it's Cause for Alarm", Robert Atkinson, July 12, 2021, Industry Week. Link

[393] "The U.S. Productivity Slowdown: An Economy-Wide and Industry-Level Analysis", Monthly Labor Review, U.S. Bureau of Labor Statistics, April 2021. Link

[394] Research interview with Joe Work, Senior Growth Advisor, MAGNET. March 31, 2022.

© Strategy of Things, 2025. All rights reserved.

14.1.2.3. Labor shortages

American manufacturing employed 12.8 million people in June 2022 and hired 242,000 employees between January and June 2022. There were 809,000 new job openings over this period.[395]

The labor shortage continues to be a challenge for U.S. manufacturers, with 89.4% of manufacturers indicating they had unfilled positions and were struggling to find qualified applicants.[396]

The shortage is a result of growth in new jobs as U.S. manufacturing grows, retirement of the "baby-boomers" workforce, lack of interest in manufacturing careers, different job and career expectations between manufacturers and jobseekers, insufficiency in U.S. education system and STEM talent development and a lack of job training programs.[397]

> *… before the pandemic started, the U.S. was almost at full employment. And the same thing that we're facing now was going on just before the pandemic where companies were battling each other in the neighborhoods for the same resources, the same staff. And it's even worse now because before there were always people looking for jobs. And now there's seems to be less people looking for jobs… companies can't find the people or they would expand their businesses right now. We walk in and companies tell us, we'll hire 10 people tomorrow, if we could. Joe Work, Senior Growth Advisor, MAGNET*[398]

14.1.2.4. Future skills gap

Digital technologies are transforming how manufacturing is performed. Automation will likely soon be integrated into almost all manufacturing operations and people will work alongside robots and machines.[399] As a result, manufacturing jobs are increasingly requiring more advanced skills.

The top five skill sets required are expected to increase significantly due to automation and advanced technologies include technology and computer skills, digital skills, robots and automation programming, working with tools and technology and critical thinking.

These shortages and skill gaps are projected to leave 2.4 million unfilled positions between 2018 and 2028, resulting in a loss of $454 billion of manufacturing value in 2028.[400]

---

[395] See note 380

[396] See note 384

[397] "Creating Pathways for Tomorrow's Workforce Today: Beyond Reskilling in Manufacturing", Deloitte Insights and The Manufacturing Institute. Link

[398] See Note 394

[399] "The Jobs Are Here, But Where Are the People?", Deloitte Insights, November 14, 2018. Link

[400] ibid.

© Strategy of Things, 2025. All rights reserved.

> *Manufacturing companies are struggling to fill existing job positions and retain workers.*[401] *The inability to bring in these skills not only has an impact on the business, but it also prevents the manufacturers from implementing IoT, developing and operating smart manufacturing processes.*
>
> *... misconceptions in manufacturing are that it's kind of a low skill type opportunity, but it's not really the case… With the advent of more automatic control equipment, the operators have to be better qualified in some instances to work with those machines because now they're doing programming of those machines to make those parts. Joe Work, Senior Growth Advisor, MAGNET*[402]

In addition, smart manufacturing will create a new set of jobs that require new skills. Some examples include:[403]

- Predictive supply network analyst
- Manufacturing cybersecurity strategist
- Smart factory manager
- Digital twin architect
- Smart Quality Assurance (QA) manager
- Collaborative Robotics technician

Many companies lack the new digital skills necessary to operate and succeed in a smart manufacturing environment. Over the past twenty years, many manufacturing companies have outsourced their in-house engineering teams who may have some of the programming and integration skills.[404]

The 2022 CESMII survey found that lack of skilled talent and lack of technical expertise was reported by 59% and 46% of the respondents, respectively. Those same two challenges were reported to have had a severe/major impact by 63% and 61% of the respondents, respectively.[405]

A Deloitte and the Manufacturing Institute research report[406] surveyed 800 manufacturers on the impact of not being able to fill these new jobs. The analysis showed that:

- 82% reported an impact to growing their business and revenues
- 81% reported an impact to maintaining production levels to satisfy customer demand

---

[401] See note 396

[402] See Note 394

[403] "The Manufacturing Skills Gap: What is it?", Manufacturing.net, August 25, 2021. Link

[404] Interview notes with Jon Weiss, VP of IoT and Analytics, SoftwareAG, February 17, 2021

[405] "The Manufacturing Institute–BKD Small and Medium-Sized Manufacturers Survey", The Manufacturing Institute, September 2021. P. 6. Link

[406] See note 397.

© Strategy of Things, 2025. All rights reserved.

- 79% reported an impact to responding to new market opportunities
- 79% reported an impact to implementing new technology in the business
- 79% reported an impact to new product development and innovation

14.2. IoT in the manufacturing industry

The concept of Industry 4.0 originated in 2011 in Germany.[407] Since then, the global manufacturing industry has been undergoing a transformation to "smart manufacturing" brought about by the convergence of manufacturing and operations technology with information and digital communications technologies, systems integration, Internet of Things and data analytics. This transformation offers the potential to increase manufacturer productivity, efficiency, agility and overall competitiveness.

IoT is one of a set of technologies that enable Industry 4.0 and the transformation of manufacturing. The "smart" in "smart manufacturing" is enabled by the application of data and analytics to enhance manufacturing operations. One source of data is from IoT sensors and devices that monitor the manufacturing equipment, operations and other assets.

In many cases, the sensors collect information that was not available before (e.g., machine vibration levels, etc.). In other cases, operations technology devices, such as Programmable Logic Controllers (PLC), collect data that were not easily extracted or shared.

IoT technologies and applications provide new ways to address many of the day-to-day challenges faced by manufacturers. These include unplanned downtime, inefficient operations, poor production quality, limited supply chain visibility and reactive field support. Equally important, IoT helps manufacturers lessen the impact of labor shortages and declining labor productivity.

Among manufacturers with less than 500 employees, the top three reasons for investing in disruptive technologies are performance improvement of operational processes, achieving production cost efficiencies and filling labor shortages.[408] A 2022 survey[409] conducted by CESMII found that the top five smart manufacturing goals by manufacturers were better manufacturing capacity utilization (65%), lower production costs (63%), improving on-time delivery (62%), operational excellence (61%) and improving quality/reducing quality risks (60%).

14.2.1. IoT use cases

Figure 14-1 below shows a representative set of 5 manufacturing use case categories and their associated use cases.

[407] "Short History of Manufacturing: From Industry 1.0 to Industry 4.0", Adrian Dima, January 25, 2021. Link

[408] See note 405

[409] "2022 Smart Manufacturing Market Survey Executive Summary", CESMII, May 2022, Page 4. Link

© Strategy of Things, 2025. All rights reserved.

- **Production and Operations.** These use cases support the activities involved directly in the production of goods covering the conversion from raw materials or inputs to finished product. The category covers both discrete and process manufacturing.
- **Production Support.** These use cases are concerned with the set of activities that support the production of goods such as worker safety.
- **Field Support.** This category of use cases supports the use, maintenance and operation of customer or company equipment that is located outside the manufacturer's facilities. This covers products that have already been sold to the customer as well as those owned by the manufacturer for their own use outside of the manufacturer's facilities.
- **Supply chain and logistics.** These use cases support the activities involved with the movement of raw materials and finished products. The goods can be within the manufacturer's facilities as well as those in supplier and distributor facilities and in transit between locations.
- **Equipment, tools and machinery.** These use cases support the equipment, machinery and tools that are used to produce the goods. The category covers both discrete and process manufacturing.

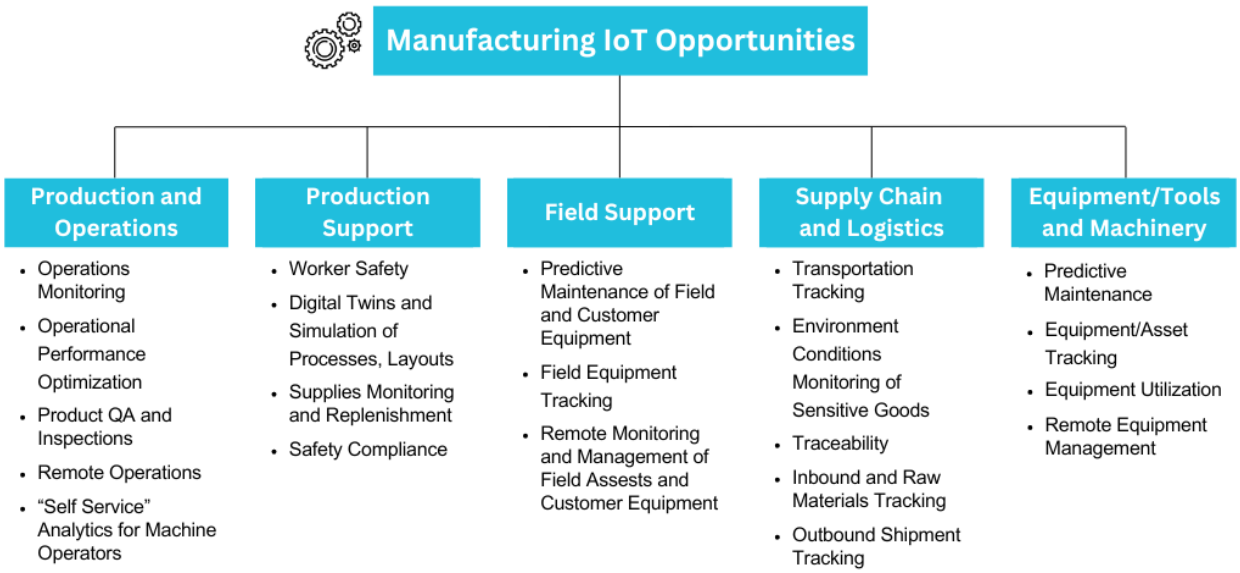


Figure 14-1: Manufacturing: Use Cases and Selected Use Cases

IoT monitors the operations used to produce products. For example, sensors monitor if a machine is operating and at what levels of utilization. The sensors monitor the processes and the production parameters, the quality of the products produced and detects product defects and production issues. The information collected helps operators and managers optimize use of equipment and resources, improve production operations and outputs and minimizes quality issues and scrap.

© Strategy of Things, 2025. All rights reserved.

While IoT will enhance and improve day-to-day manufacturing processes and operations, value is created in improving the indirect activities associated with manufacturing. For example, predictive maintenance is not directly involved in manufacturing products, but it ensures that the machinery involved in manufacturing the products will be serviced before it breaks down. This eliminates unplanned downtime while maintaining production rates and capacity.

For machine builders and original equipment manufacturers (OEM), customer support of equipment deployed in the field is a major activity. Remote monitoring and management of field machinery and equipment allows manufacturers to be proactive and agile in servicing their customers.

> *What are manufacturers actually interested in today?*
>
> *Unplanned outages. Why did it happen? How do I use data and analytics to get that machine or asset back up and running immediately?*
>
> *Increasing efficiency. How do I become more efficient in my process? When are my machines not running when they should be running?*
>
> *Supply chain visibility. How do we become more resilient in our supply chain?*
>
> *OEM and equipment builders. How do we enable very effective remote asset management for field services purposes, for understanding user behavior on those assets?*
>
> *Jon Weiss, VP IoT and Analytics, Software AG*[410]
>
> *The simplest use case is basic asset utilization. Is the machine running or is it not running?... The other use case that companies would like to be able to do is machine maintenance prediction… lots of sensors you put on a machine to indicate when a spindle is going bad on a cutting tool. Joe Work, Senior Growth Advsior, MAGNET*[411]

14.2.1.1. Use case and industry challenges alignment

The manufacturing industry faces several challenges, some of which are described in Section 14.1.2. Figure 14-2 below shows the fit between the proposed use case subcategories and the documented industry challenges.

[410] Research interview notes, Jon Weiss, Software AG, February 17, 2021

[411] Research interview with Joe Work, Senior Growth Advisor, MAGNET. March 31, 2022.

© Strategy of Things, 2025. All rights reserved.

Challenge	Role of IoT	Use case examples
Vulnerable Supply Chain	Track, monitor and optimize incoming parts and materials shipments needed for manufacturing. Track and monitor finished product shipments.	• Transportation tracking • Traceability • Inbound and raw materials tracking • Outbound shipment tracking • Supplies monitoring and replenishment
Declining Productivity	Increase productivity, efficiency and effectiveness through operations monitoring, improved resource utilization and optimization, automation, minimized unplanned downtime and waste and data informed targeted actions. IoT helps manufacturers be more resilient, competitive and profitable.	• Operations monitoring • Operational performance optimization • Product QA and inspections • Digital twin production simulations • Remote monitoring • Predictive maintenance
Labor Shortages	Optimize workforce productivity, efficiency and effectiveness through operations planning, task automation, resource optimization and data informed actions. IoT technology helps manufacturers do more with fewer resources and to be more effective doing it.	• Remote operations • Worker safety and safety compliance • Remote equipment management • Remote monitoring and management of field assets and customer equipment • Process automation
Future Skills Gap	IoT reduces reliance on hard-to-find resources through intelligent algorithms and process automation.	• Self-service analytics • Robotics • Predictive maintenance • Process automation

Figure 14-2: Manufacturing: Use Case and Industry Challenges Fit

14.2.1.2. IoT use case details

Additional details on the use case subcategories shown in Figure 14-1 are provided below in Figure 14-3

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Description
Production and Operations	Operations monitoring	Monitors the status and key parameters of the production process and equipment. Identify equipment and operations that are not working properly.
	Operational performance optimization	Monitor and adjust processes to improve quality, enhance efficiency and reduce waste.
	Product QA and inspections	Inspect products at various stages of the process to verify parts or batches are within specifications.
	Remote operations	Monitor, operate and control machinery and operational processes from a location different from where the operations are running.
	"Self-service" analytics for machine operators	Operators monitor operational parameters during batch runs, use analytics at the machine station to identify trends and adjust the next batch.
Production Support	Worker safety	Monitor behaviors, activities and conditions that may put workers at risk.
	Digital twins and simulation of processes, layouts	Digital models of manufacturing assets, processes and operating conditions. These models can be used to simulate different conditions, new assets, layouts and processes.
	Supplies monitoring and replenishment	Monitors inventory levels of parts and inputs used in the production process and place order to replenish supplies based on actual quality, production runs, etc.

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Description
	Safety compliance	Monitors key parameters during production operations to ensure practices are followed, parameters within specification and compliance with regulations.
Field Support	Predictive maintenance of field and customer assets	Monitors key parameters on field and customer equipment. Detects out of spec conditions early and alerts technicians to service equipment before failure.
	Field equipment tracking	Monitor location, condition and status of company and customer assets in the field
	Remote monitoring and management of field assets and customer equipment	Manage, configure and administer manufacturer and customer equipment. Examples include remote software updates, troubleshooting, configuration changes.
Supply Chain and logistics	Transportation tracking	Track location and condition of delivery vehicles. Estimated time of arrival, transportation planning, logistics management.
	Environment Conditions Monitoring of sensitive goods	Monitors the conditions that sensitive shipments requiring controlled environment during transport, including pharmaceuticals, vaccines, produce and other food products.
	Traceability	Tracks the provenance of products. For example, the specific batch of chemicals used in production of other chemical or pharmaceutical products.

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Description
Equipment/ Tools and Machinery	Predictive maintenance	Monitors key parameters on production equipment. Detects out of spec conditions early and alerts technicians to service equipment before failure.
	Equipment Asset tracking	Monitor location, condition and status of company assets and equipment, Work in Progress (WIP) and inventory in the factory, warehouses and staging areas
	Equipment utilization	Monitor equipment usage to determine if machines are operating, over and underutilized. Assists in production and capacity planning.
	Remote equipment management	Manage, configure and administer production equipment. Such as remote software updates, troubleshooting and configuration changes of equipment

Figure 14-3: Manufacturing: Use Case Details

© Strategy of Things, 2025. All rights reserved.

14.2.2. Market views of IoT in manufacturing

To understand market views on IoT and to inform on our gaps discovery and analysis, our research team conducted a survey of 450 people, from adopters to solution providers, across the nine industries studied. The survey respondents were asked their opinion on the importance of IoT for the manufacturing industry over the next 5 to 10 years. Figure 14-4 below shows an expected relative medium to high impact of IoT, as compared to other industries. Despite this, several factors hinder the adoption and use of IoT in manufacturing. These will be discussed in the following section.

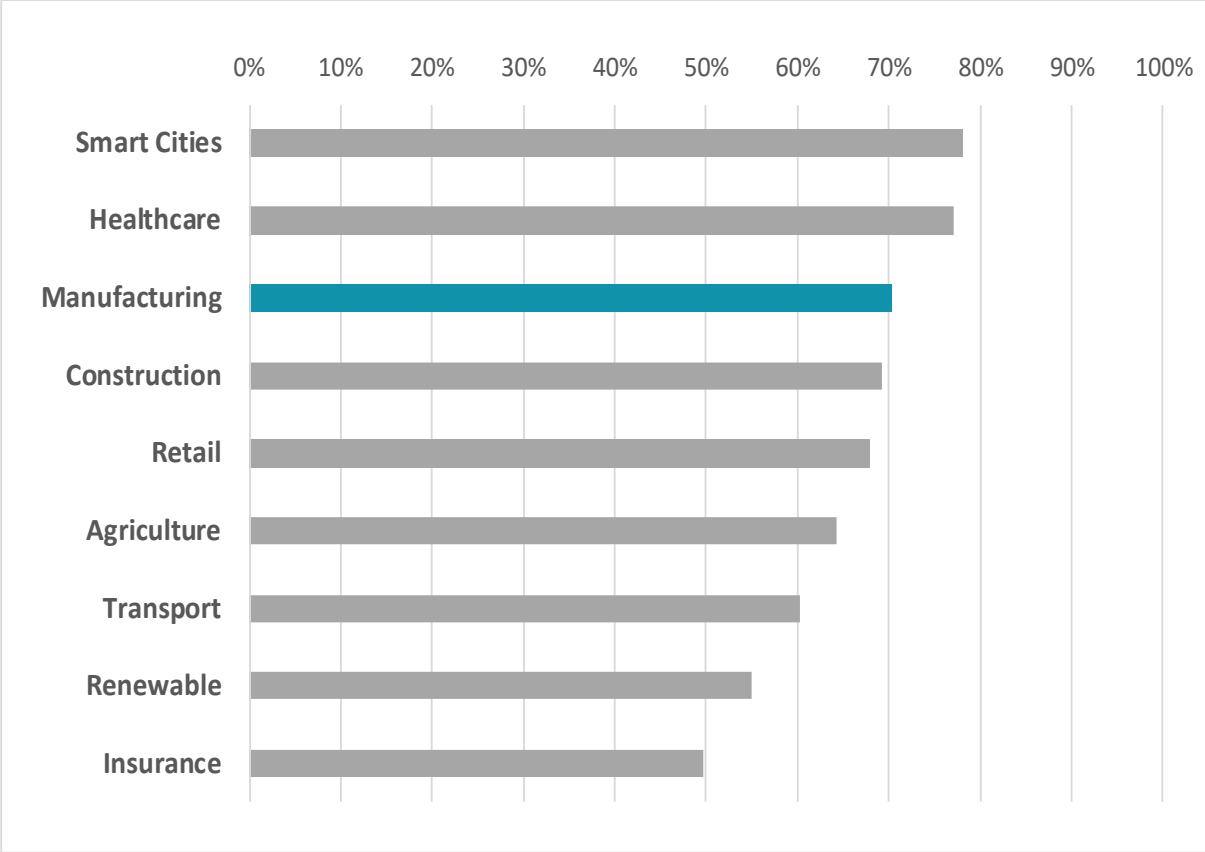


Figure 14-4: Manufacturing: Importance of IoT

Survey respondents were asked to rate the impact of these use case categories on the manufacturing industry.[412] During the survey collection process, the use case categories provided to respondents became more detailed based on information collected through interviews. Adjustments were made to responses to map to the new use case categories. Figure 14-5 below shows the impact of different use case categories based on this mapping. Despite the transformative potential of smart manufacturing, the survey results show respondents rated the impact as medium. Some of the reasons for these beliefs are discussed in the following section.

[412] In your view, what will be the impact of these use cases in manufacturing over the next 5-10 years?

© Strategy of Things, 2025. All rights reserved.

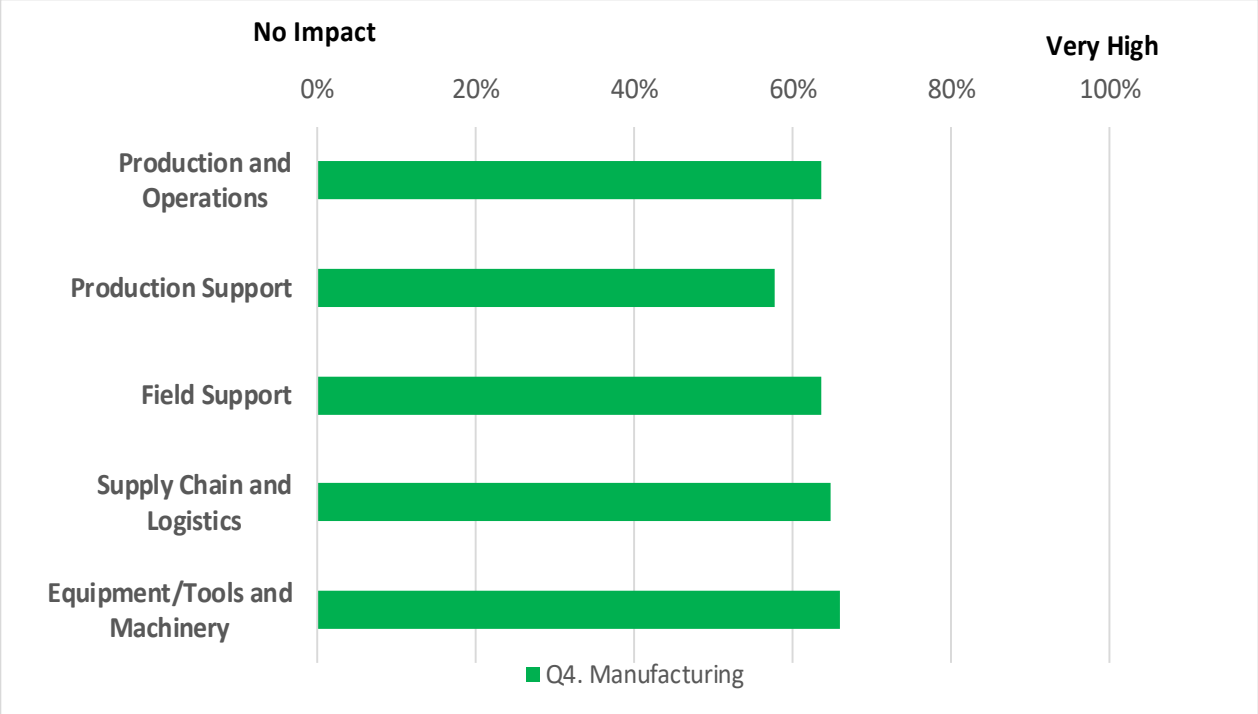


Figure 14-5: Manufacturing: Use Case Category Impact

14.3. IoT gaps and findings in manufacturing

A combination of interviews, secondary research and surveys was conducted to identify and understand the opportunities and challenges to the development and adoption of IoT. Each research method approached the challenges from a different perspective.

For example, the survey targeted a large audience but asked specific questions that supported the economic analysis. The interviews targeted a small number of people who provided deeper insight and context to supplement the information already collected. Finally, the desk research, consisting of a review of online news articles, published research reports, vendor and government white papers, blogs, webinars, videos and other content, provided a broad overview of the application of IoT in the industry.

In our survey, respondents were asked to choose the most important technology areas to operationalize IoT in their industry. Figure 14-6 below shows the top 10 IoT technologies and the percentage of respondents who chose that technology.[413] The survey results are not seen as a technology gaps list, but rather an indication of what is important to the respondents. This information partially informs the gap selection process.

[413] Respondents were asked to choose up to 5 out of the 25 listed single technology components.

© Strategy of Things, 2025. All rights reserved.

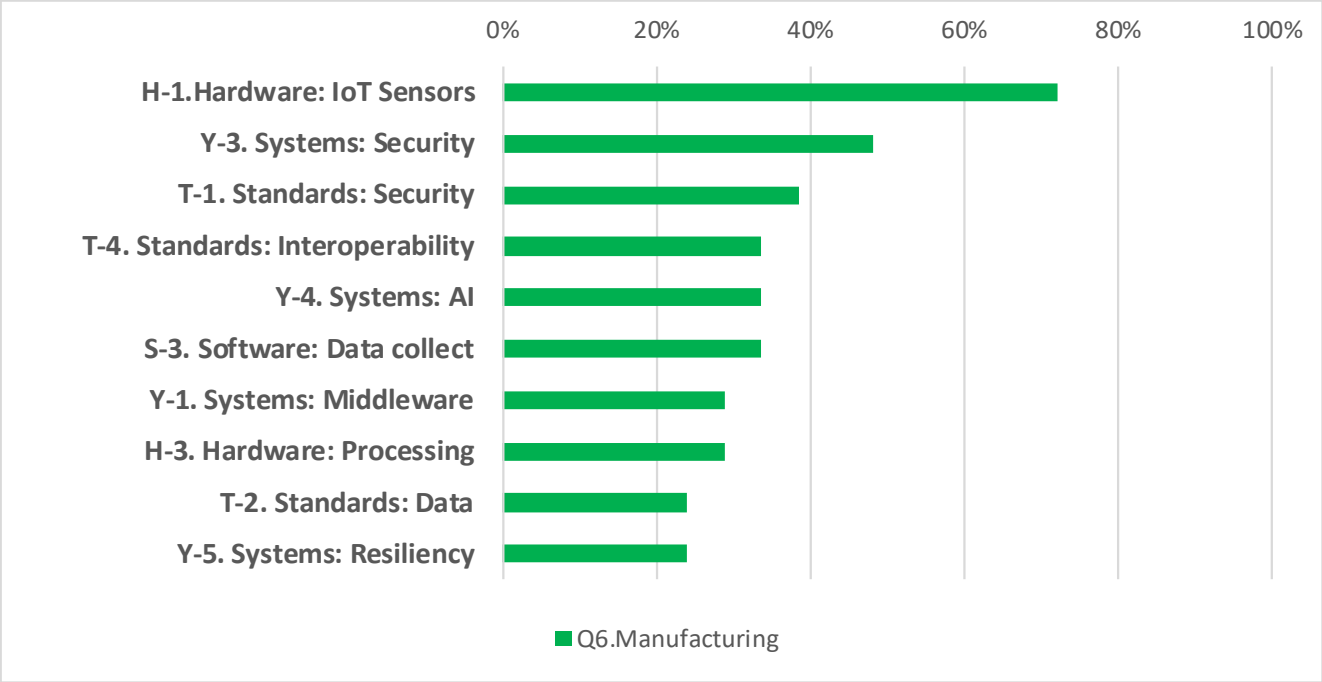


Figure 14-6: Manufacturing: Top 10 Most Important Single Technologies

14.3.1. Top technology challenges

Based on the approach described above, four IoT technology challenges were identified as shown below:

- Interoperability
- Cybersecurity
- Sensors and devices
- Connectivity

14.3.1.1. Challenge #1: Interoperability

Interoperability challenges are a major barrier to IoT adoption and value realization in manufacturing. Factories have a variety of existing industrial and operations technology (OT) systems, from new industrial equipment with current technology to legacy equipment with limited technology and connectivity.

Many of the machines employ a variety of proprietary and incompatible protocols that make sharing information from Manufacturing Execution Systems (MES), Enterprise Resource Planning (ERP) systems, Supervisory Control and Data Acquisition (SCADA) and Distributed Control Systems (DCS) difficult or impossible. This inability to share information and services

© Strategy of Things, 2025. All rights reserved.

between disparate systems creates operational inefficiencies. A 1999 study estimated that imperfect data interoperability cost the U.S. automotive chain a billion dollars each year.[414]

Data sharing, communicating and integration of disparate devices and systems in this environment is difficult. For example, PLCs on a particular set of machines may be connected directly to a specific MES application, Historian or SCADA system. In addition, some control devices, such as PLCs, may collect data but as they are not connected there is no easy way of data extraction.[415] Interoperability issues that may occur include:[416]

- Exchanging data between commercially similar or dissimilar systems
- Exchanging data between machines having different versions of software from the same vendor
- Compatibility between newer and older software versions
- Misinterpreting definitions or the meaning of terms used to structure data exchange and differences in data dictionaries
- Not using a recognized normative documentary standard upon which exchange data are formatted and based
- No means of consistently testing self-declared conformant applications to ensure correct communication between systems

Lack of interoperability is a long running challenge that pre-dates IoT, Industry 4.0 and smart factories. Smart manufacturing simply added another set of technology that is required to interoperate with existing equipment, machinery and systems.

> *... islands of interoperability where some things work with others in the same vendor, but not across vendor brand. Doug Sandy, VP of Technology/CTO, PCI Industrial Computer Manufacturers Group (PICMG)*[417]

> *You may go into two factories that create the exact same product for the exact same company and have different machines communicating over different protocols measuring KPIs differently. That gets really challenging when it comes to enterprise scaling of these implementations. Jon Weiss, VP of IoT and Analytics, Software AG*[418]

> *There's a lot of very old equipment that's still being used and it works… those machines are more difficult to tap into, to pull information or pull data out of it*

[414] "Interoperability Cost Analysis of the U.S. Automotive Supply Chain", Smita B. Brunnermeier and Sheila A. Martin, RTI Report 7007-03, March 1999. Link

[415] Research interview notes, Jon Weiss, Software AG, February 17, 2021

[416] "Manufacturing Interoperability Program, a Synopsis", NIST Interagency/Internal Report (NISTIR), National Institute of Standards and Technology, Gaithersburg, MD, Kemmerer, S. February 24, 2009. Link

[417] Research interview with Doug Sandy, PICMG, October 11, 2021.

[418] Research interview notes, Jon Weiss, Software AG, February 17, 2021

© Strategy of Things, 2025. All rights reserved.

> *because they're antiquated control systems. So it takes more effort to try to get whatever that company is looking for from that machine from a data generation perspective. Joe Work, Senior Growth Advisor, Manufacturing Advocacy and Growth Network (MAGNET)*[419]

There are several organizations working on various aspects of the interoperability challenge. For example, the Open Manufacturing Platform (OPM) was formed in 2019 to "harness the power of collaboration and openness so that raw equipment data can be collected, aggregated across multiple data sources, consolidated) and analyzed to create information."[420] In addition to the OPM, a partial list of other organizations working independently to develop standards for information models and interoperability include:

- the MTConnect Institute (protocol designed for "the exchange of data between shop floor equipment and software applications used for monitoring and data analysis")[421]
- the OPC Foundation which developed the OPC-UA standard that allows devices from different vendors to communicate with each other
- PICMG data models for sensors used in manufacturing applications[422]

The interoperability challenge is difficult to overcome for a variety of reasons. Technology is evolving and standards must adapt. For example:

- Many existing organizations, standards bodies and consortiums, focus on specific interoperability gaps, industries and functional areas.
- Some solution providers promote proprietary protocols because they believe it to be technically superior, gives them a customer "lock in" advantage and above average profit margins.[423]
- Standards may vary geographically, in compliance with country or regional approaches, policies and regulations.

14.3.1.2. Challenge #2: Cybersecurity

While IoT is a critical enabler of smart manufacturing and factories, it also introduces potential technical vulnerabilities that can be exploited to disrupt manufacturing and supply chain operations. With the convergence of IT and Operational Technology (OT) systems, along with the integration of IoT devices, formerly "air gapped" OT systems are now accessible from the internet.[424]

---

[419] Research interview with Joe Work, Senior Growth Advisor, MAGNET. March 31, 2022.

[420] "Crossing the Interoperability Chasm", David Greenfield, Automation World, December 17, 2020. Link

[421] "MTConnect", Wikipedia entry. Link

[422] Research interview with Doug Sandy, CTO at PICMG, October 11, 2021

[423] Research interview, Chief Engineering Officer, smart city IoT solutions company

[424] "2022 State of Operational Technology and Cybersecurity Report", Fortinet report, 2022. Link

© Strategy of Things, 2025. All rights reserved.

Hackers can gain access to the manufacturer's network through vulnerabilities in improperly configured or secured IoT devices. Once in the network, they can access sensitive information, such as intellectual property and data, execute ransomware or disrupt business and manufacturing operations. Cybersecurity risks were identified as one of the top three project risks that hinder companies from adopting IoT.[425]

Field data supports these concerns. IBM reported that manufacturing was the number one industry targeted in 2021, accounting for 23.2% of the attacks that they remediated. Of the organizations with operations technology attacked, 61% were manufacturing companies. Oil and gas companies were next at 11%, followed by transportation and utilities, both reporting in at 10% each. The report also showed a high volume of IoT malware attacks in 2019, including a 3,000% surge between Q3 2019 and Q4 2020. Manufacturing was the number one targeted industry in North America with 28% of the attacks, compared with 25% in Europe and 29% in Asia.[426]

Manufacturers are particularly vulnerable for a range of reasons. Most manufacturing environments were not designed to address cybersecurity issues. In many factories, as much as 40% of equipment and assets are not connected to each other or to the network.[427] A blog article about process sensors used in industrial environments stated that these sensors "have direct and indirect connectivity to the Internet but without cyber security capabilities." and that "there is a need for industry and standards organizations to address the lack of cyber security and authentication in legacy process sensors and IIOT devices."[428]

The shift to smart manufacturing is driving the convergence of OT with Information Technology and connecting these previously unconnected systems and assets to the internet. This, however, creates new cybersecurity challenges, including:

- The creation of new attack surfaces instead of a former "protection by air gap" environment
- The integration of resource constrained IoT devices with limited cybersecurity capabilities
- The availability of machine time for security updates
- The impact on production, machine uptime and reliability and latency from cybersecurity measures to OT systems and processes

The disruption potential is high, as unplanned downtimes are amplified across the supply chain. The U.S. Cybersecurity and Infrastructure Security Agency has identified manufacturing as one of 55 national critical functions that are "so vital to the United States that their disruption,

---

[425] "Three Main Risks That Prevent Companies From Adopting Iiot Solutions", IIoT World, November 24, 2021. Link

[426] "X-Force Threat Intelligence Index 2022", IBM Security Report, February 2022. Link

[427] "Moves to Connected Manufacturing Hindered by Stranded Assets", L. Rosencrance, TechTarget, November 20, 2018. Link

[428] "Process sensors are different than IoT and IIoT devices," J. Weiss, Control, December 12, 2022. Link

© Strategy of Things, 2025. All rights reserved.

corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[429]

Small manufacturing companies are most vulnerable as they lack the digital infrastructure, resources and skills to fend off cybersecurity attacks. Despite the rising cybersecurity threats, adoption of cybersecurity measures remains low. This is supported by a study which found that only 25% of respondents reported it as a challenge.[430]

Cyberattacks have financial consequences. A 2023 Cybersecurity Risk analysis reported that the manufacturing industry has an average loss exposure (probable likelihood and probable financial impact) of $1.1 Million per attack scenario. These scenarios include insider misuse, web application attack, system intrusion, insider error, ransomware, social engineering and denial of service attack.[431]

14.3.1.3. Challenge #3: Sensors and Devices

IoT sensors and devices monitor a variety of objects and states including the state of production assets, operational processes, asset productivity, usage and locations. High hardware costs and the use of more powerful IoT devices to manage on-device processing slow the adoption of IoT. Each of these is discussed below.

High hardware costs. The high cost of devices poses a barrier to adoption for manufacturers who are considering IoT implementations in their factories.[432] [433] Although the average cost of sensors has dropped from $1.30 in 2004 to $0.38 in 2020,[434] the semiconductor cost in IoT devices in 2017 was $85.[435]

In addition, the specific application will dictate the IoT device cost. As an example, temperature sensors can range from $10 for a HVAC application to $2,000 for a high accuracy and high precision application.[436]

Solutions providers offering IoT devices for special applications are caught in the middle. The special applications they support mean higher device prices but the slow adoption of IoT limits demand and hinders them from leveraging scales of economy to reduce prices.[437]

---

[429] National Critical Functions Set, Cybersecurity and Infrastructure Security Agency. Link

[430] See note 409 Page 5

[431] "2023 Cybersecurity Risk Report," RiskLens, 2023. Link

[432] See note 449

[433] Interview notes with Senior Manager, Sales Development of Industrial IoT solutions company

[434] "The Average Cost of IoT Sensors is Falling", Goldman Sach BI Intelligence estimates, 2016. Link

[435] "Will Higher Production Costs Hamper IoT Growth?", Joanne Itow, Semiconductor Engineering, May 22, 2017. Link

[436] "How Much Do Temperature Sensors Cost?", Dave Dlugos, Ashcroft blog, July 26, 2021. Link

[437] See note 449

© Strategy of Things, 2025. All rights reserved.

A large manufacturer may operate multiple factories containing thousands to hundreds of thousands of machines and production equipment of varying types. The cost to fit all production equipment in these factories with various devices can be cost prohibitive.

The total IoT investment required is more than just devices, as hardware is usually around 30%[438] of the initial implementation cost. In some cases, the network infrastructure that the IoT devices need may require upgrading. There are additional professional services costs for implementation, systems integration, technical support and maintenance. Finally, recurring costs for cloud services, including storage, processing and analytics need also be considered.[439]

Small and medium size manufacturers, representing 98.3% of U.S. manufacturing businesses, face a similar problem.[440] While they have smaller factories with less production equipment, they also have reduced access to capital. These businesses operate with manual manufacturing and production steps, small lot sizes, a variety of older machinery with different communications protocols[441] and underutilized capacity.[442] In addition, they are likely to have outdated infrastructure that needs to be modernized prior to any IoT investment.

> *...industrial grade sensors that cost $200 to $225 a sensor, you have to have a hell of a ROI on your use case to invest that much money across thousands of pieces of equipment or assets. Jon Weiss, VP, IoT and Analytics, Software AG*[443]

For these reasons, the solution provider community is exploring "IoT as a Service" as an approach to "cut all upfront costs including that of hardware"[444] for the customer. This approach bundles in the hardware, software and services and offers it to the customer on a subscription basis. While this approach is attractive to manufacturers, it brings substantial financial risk to solutions provider who must purchase the devices upfront and then recover their investment over time.

"Open source IoT" is another approach that could lead to lower cost IoT solutions for manufacturers and other IoT adopters. In this approach, developers collaborate to develop solutions that are innovative, robust, up to date, secure and non-proprietary.

There are many collaboration groups, such as the Eclipse IoT Foundation, which are working on open source IoT projects. There are, however, obstacles that must be overcome first, such as "the ease-of-use, customer support, guarantees, regulatory compliance and certifications."[445]

---

[438] "How Much Will an IoT Device Cost Your Business?", Nabto blog, IDA HÜBSCHMANN, June 4, 2022. Link

[439] "6 Factors That Determine IoT Price for Manufacturers", Mark Stevens, Sept 14, 2021. Link

[440] See note 380.

[441] "Trends for Low-Cost and Open-Source IoT Solutions Development for Industry 4.0", Antti Martikkala, Joe David Andrei Lobov, Minna Lanz, Iñigo Flores Ituarte 7-10 Sept 2021, Athens, Greece. Link

[442] See note 449

[443] Research interview notes, Jon Weiss, Software AG, February 17, 2021

[444] "IoT as a Service – A Game Changer?", Zinnov blog, Ketan Vaid, August 21, 2017. Link

[445] See note 441

© Strategy of Things, 2025. All rights reserved.

More powerful IoT devices to manage on-device processing. The wireless environment within a factory is challenging. Factories are replete with machinery and metallic surfaces, concrete walls and steel structures that attenuate the propagation of wireless signals and create latency. Still other factories do not have a network infrastructure for connected operations.

Many manufacturing operations require real time data monitoring and processing. On-device or local gateway processing of sensor data is a feasible option in these situations. Depending on the specific application, this may require the use of AI capable microprocessors and microcontrollers that can be integrated into IoT devices or gateways and/or the development of analytics algorithms that can operate on resource constrained devices. These smart sensors and gateways, however, are more expensive than their "dumb" counterparts, which can slow adoption.

> *Where's data actually going to be processed? It goes right back to the distributed architectures and the importance of being able to deploy whatever it is that you're building anywhere, because it might not be on the internet anymore. Jon Weiss, VP, IoT and Analytics, Software AG*[446]

14.3.1.4. Challenge #4: Connectivity

Many manufacturers lack the appropriate connectivity infrastructure to support "smart operations" for tomorrow's factories. This is attributed to a lack of network standards and poor network infrastructure.[447,448]

Some factories do not have an adequate network infrastructure because their previous production operations did not require connectivity.[449] While some of their equipment may have collected data, there was no provision to extract or analyze the data.[450]

Other factories are in buildings with extensive metal racking and machinery which hinders wireless signal propagation and results in poor coverage and performance.[451] Still other factories employ SCADA systems with limited or proprietary connectivity options that cannot support the scale that IoT requires.

In other cases, factories in rural parts of the country with no high-speed broadband infrastructure[452] are effectively isolated from the internet, the cloud, other factories and their suppliers and distributors. This lack of connectivity precludes:

- Bandwidth heavy applications such as video-based quality inspections
- Remote management of production equipment and operations

---

[446] Research interview notes, Jon Weiss, Software AG, February 17, 2021

[447] "The Factory of the Future", Boston Consulting Group, December 16, 201. Link

[448] See note 449

[449] Interview notes with Jon Weiss, VP of IoT and Analytics, Software AG, February 17, 2021

[450] Interview notes with Joe Weiss, Senior Growth Advisor at NIST MEP, May 31, 2022

[451] "Technology Challenges Facing Manufacturers", Business Information Group. Link

[452] See note 449

© Strategy of Things, 2025. All rights reserved.

- Real time transportation and critical shipment tracking information.

A Michigan based economic development organization stated the lack of broadband access threatens the ability of its rural based manufacturing companies to compete with companies that employ industry 4.0 technologies.[453] Underscoring the importance of broadband for manufacturers, the National Association of Manufacturers urged in a letter to the Senate Committee on Commerce, Science and Transportation to "support investment in our broadband infrastructure system, maximize consumer choice in how they connect and reduce regulatory barriers that can slow manufacturers' ability to deploy current and next-generation broadband infrastructure."[454]

> *I've been in lots and lots of factories where there's no cell service, there's no Wi Fi and everything's kind of hardwired into a network. In today's environment, that's a bit crippling. Jon Weiss, VP, IoT and Analytics, Software AG*[455]

14.3.2. Other challenges

In addition to the technology challenges for further consideration, our research has identified other challenges that impact IoT adoption. These challenges did not meet the criteria for research consideration because they were either not a technology challenge or a technology related challenge that cannot be addressed by current marketplace offerings or capabilities. These include:

- Slow adoption of Industry 4.0
- ROI Skepticism
- Resistance to change

14.3.2.1. Slow adoption of Industry 4.0

In a 2019 survey, 39% of U.S. manufacturers had not adopted "smart factory" technologies, while another 14% were starting to experiment with them.[456] Although the pandemic has accelerated digital transformation investment and initiatives, U.S. manufacturers still lag Europe and China.

Less than half (44%) of U.S. manufacturers are implementing IoT solutions according to a strategic plan, compared with 65% and 92% of European and Chinese manufacturers. Only 22% of U.S. manufacturers have adopted the use of cobots, compared with 52% and 77% in Europe

[453] "Lack of Broadband Access Threatens Rural Manufacturers' Ability to Compete", MiBiz, January 20, 2019. Link

[454] "The U.S. Needs Better Broadband Access", August 11, 2020. Link

[455] Research interview notes, Jon Weiss, Software AG, February 17, 2021

[456] "Navigating the Fourth Industrial Revolution to the Bottom Line", The Manufacturing Institute research report, 2019. Link

© Strategy of Things, 2025. All rights reserved.

and China respectively. Similarly, 26% of U.S. manufacturers use machine learning, compared with 61% and 78% of European and Chinese manufacturers respectively.[457]

> *The vast majority of manufacturers in the United States are small companies. They got 20 to 30 people on staff. And that definitely poses problems when it comes to embracing technology that is a little bit more on the cutting edge of innovation. These folks don't have the money to invest typically or they're not under the impression they need to get connected and retrieve data because they have an operation so small. They believe that they know how their performances are. Most small manufacturers believe that they're operating on pretty optimal levels because they've been in business for so long. … And so culturally, there's pushback on embracing new technologies. Jon Weiss, VP, IoT and Analytics, Software AG*[458]

> *It's not as easy as the technology guys make it sound. These companies have a mix of old and new machines, so you just can't go around to every machine and plug an Ethernet cable into it and hook it into a server to get the benefits. And if you can't connect to it, you can't add sensors to it and connect those. But you need to get some engineering support to do this… And a lot of times, IT has to be involved. Do you have a cloud-based system? Or if you worry about cybersecurity, do you have an on-premise server? You really need to have an IT role for that. Nothing keeps running. So it's not as easy as everybody makes it out to be for these guys. They're working on their business and they got to take the time and effort away to dip their toe in the water... And it's a big deal for them. Joe Work, Senior Growth Advisor, MAGNET*[459]

14.3.2.2. ROI skepticism

While IoT enables smart manufacturing and bring substantial benefits to the manufacturer, there is skepticism about the overall Return on Investment (ROI) for smart manufacturing. A 2021 industry survey reported that 68% of 500 respondents felt that their investments have not yet shown a positive return and 65% indicated that the costs to adopt smart manufacturing outweighed the benefits.[460] This is attributed to a lack of maturity and understanding of the RoI and business case for IoT.[461]

Many manufacturers have difficulty justifying the ROI as there is little clarity on what problem is addressed with IoT. This leads to a range of pilot projects, none of which lead to

---

[457] "Powering up the Connected Factory: The 2019 MPI Internet of Things Study", BDO USA LLP. Link

[458] Research interview notes, Jon Weiss, Software AG, February 17, 2021

[459] Research interview with Joe Work, Senior Growth Advisor, MAGNET. March 31, 2022.

[460] "Accelerating the Adoption of Smarter Manufacturing", Lift industry survey, 2021. Link

[461] See note 449

© Strategy of Things, 2025. All rights reserved.

deployments.[462] In other cases, some manufacturers are expecting to see a return on investment immediately and not in three to four years.[463]

While ROI is a common metric used by businesses to evaluate the feasibility of a solution or course of action, it is not enough to drive adoption in some cases. Success stories highlight what someone has done and the real-world benefits obtained facilitate adoption.

For example, the Manufacturing Advocacy and Growth Network (MAGNET), a Cleveland based NIST Manufacturing Extension Partner (MEP), is working with several small and medium sized manufacturers to share their experiences with other manufacturers to drive interest in IoT.[464]

> *There's still a lot of convincing that has to be done on the business side of the house when you're talking about what's it going to take to adopt this technology… It's just the importance of fleshing out the business cases and having a really clear understanding of the ROI. That's probably one of the largest maturity challenges today. I don't think it's really technology maturity challenges anymore in many respects. Many times they have a hard time justifying the ROI because they haven't even really clearly decided strategically what the problem is that they want to address. I was talking to a guy that had been doing POCs and pilots in the field for five or six years to determine what's even important to that contract and what technologies are going to work for them. Jon Weiss, VP, IoT and Analytics, Software AG*[465]

> *IoT has been a harder thing to sell to some companies because the math is not as easy … you have to either see somebody else has done it and see what benefits they've reaped, or you just take the jump and do pilot projects. A lot of smaller companies, medium sized companies… can only spend so much time and effort and money on these things. So what they put in as to be something that's going to impact them rather quickly and not just be something that in three or four years is going to help them out. I think that's kind of the mentality that we're dealing with. Joe Work, Senior Growth Advisor, MAGNET*[466]

14.3.2.3. Resistance to change

Despite the benefits that IoT provides, change resistance is a key barrier to adoption. For example, some organizations believe they are already operating at optimal levels because they can fill all their current orders. In other cases, they believe that their operation is too small to be connected. Finally, there are silos between Information Technology (IT) and Operations

---

[462] See note 449

[463] See note 450

[464] See note 450

[465] Research interview notes, Jon Weiss, Software AG, February 17, 2021

[466] Research interview with Joe Work, Senior Growth Advisor, MAGNET. March 31, 2022.

© Strategy of Things, 2025. All rights reserved.

Technology (OT) with opposing goals of innovation and cost management which leads to a slow adoption of innovative solutions.[467]

Another dimension is the impact of IoT on people. While much of the transformation focuses on the technology elements and what it can do[468], the people side of IoT is ignored. For example, IoT can result in how an operator's job will be performed. Accustomed to relying on their "gut feeling" or intuition from years of experience, many operators still do not trust the data from the sensors that are used to make decisions on the factory floor.[469]

This change resistance is supported by a 2019 Walden University research dissertation. Using data collected from 168 information technology U.S. manufacturing organizations, the research found that the top three indicators that predicted IoT adoption intention were technology readiness, top management support and competitive pressure.[470] The latter two factors have a significant impact on increasing or decreasing change resistance.

A CESMII study found that 82% of respondents indicated that lack of executive leadership support was a severe to major challenge.[471]

> *Why are they so far behind the curve? I think there are some cultural challenges in the industrial space. A lot of people believe that they are operating more efficiently than they actually are. I've spoken with hundreds of manufacturers. And a lot of the discussion starts by having to really convince folks to start looking at their data because they're probably not operating at 90% efficiency like they think they are. ... I think part of it is just apprehension, which means it's a change management problem. Jon Weiss, VP, IoT and Analytics, Software AG*[472]

> *The key is the culture of the company and making sure that the operators or the technicians and everybody else are on board with what's going on, because they can get the feeling that big brother is watching them now. And they're being held to a different account, relative to what they're responsible for. I would say it's more of a cultural issue than it is a them being able to interface with the technology. Joe Work, Senior Growth Advisor, MAGNET*[473]

---

[467] See note 449

[468] "In the Internet of Things, People Are Still the Most Important Component", Dusty Weis, AEM blog, June 18, 2017. Link

[469] See note 433

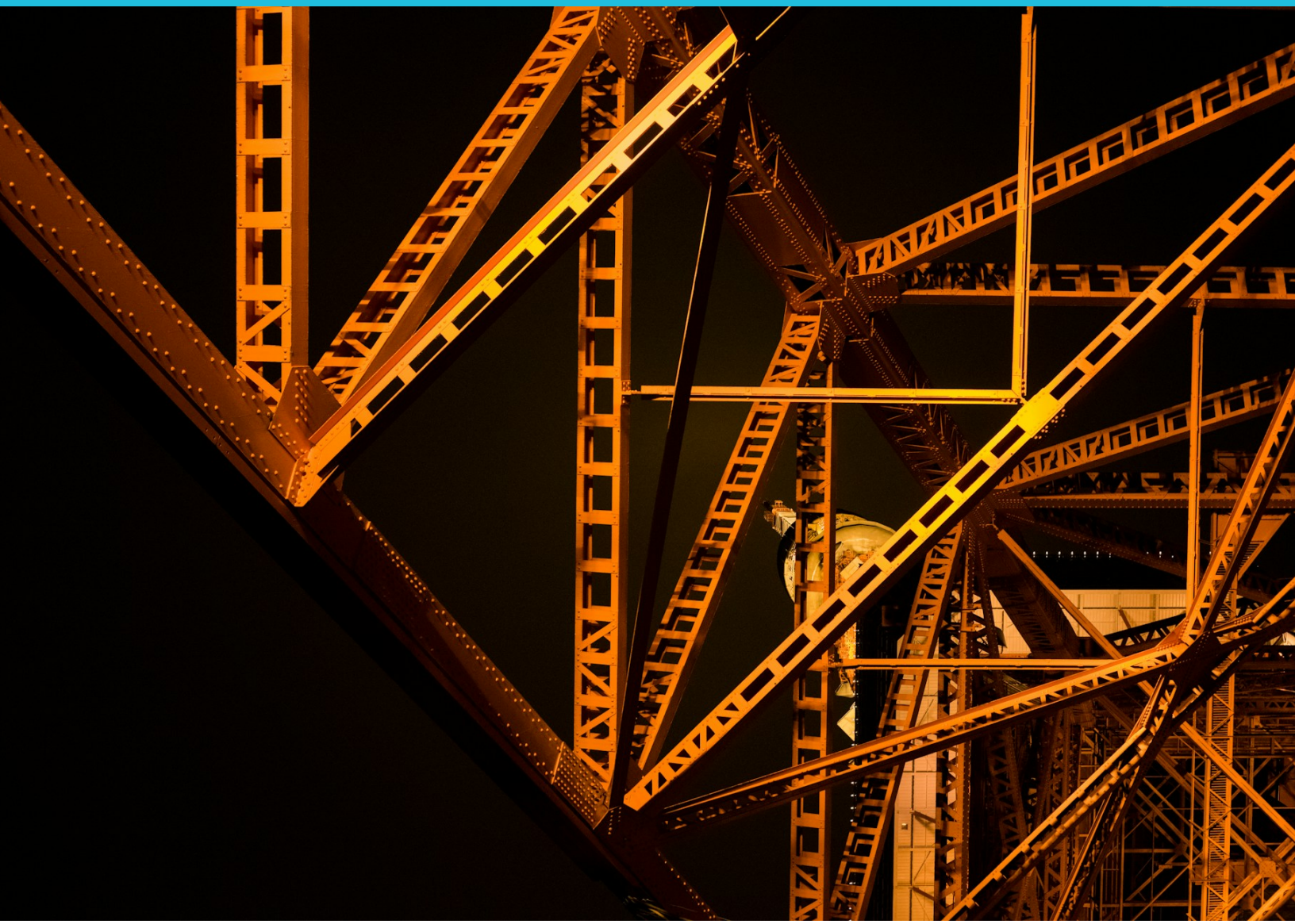
[470] "Influential Determinants of Internet of Things Adoption in the U.S. Manufacturing Sector", Ronville D. Savoury, Walden University research dissertation, 2019. Link

[471] See note 409 Page 6

[472] Research interview notes, Jon Weiss, Software AG, February 17, 2021

[473] Research interview with Joe Work, Senior Growth Advisor, MAGNET. March 31, 2022.

© Strategy of Things, 2025. All rights reserved.



Appendix: Construction

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

© Strategy of Things, 2025. All rights reserved.

15. Appendix: Construction

This section describes the research findings for IoT technology infrastructure in the U.S. construction industry. The topics discussed here include:

- Industry overview
- Use of IoT in construction
- IoT challenges in construction

15.1. Industry overview

The construction industry is one of the largest employers of Americans in the United States. This section presents some basic facts about the construction industry, as well as some key industry challenges.

15.1.1. Key facts

In Q1 of 2022, construction contributed $1.01 trillion USD[474] to the American economy, representing 4.13% of Gross Domestic Product (GDP).[475] The Architecture and Engineering industry is interdependent with the construction industry. Its services are integral to the planning, design, building and operations of construction projects. This industry contributed an additional $386 billion to GDP in 2019.[476]

The construction industry is a major employer of Americans with more than 753,000 employers and over 7.18 million employees in 2020.[477] The industry has a $458.9 billion annual payroll in 2020 and builds nearly $1.4 trillion worth of structures each year.

The construction industry consists of three subsectors: Construction of Buildings, Heavy and Civil Engineering Construction and Specialty Trade Contractors.[478] These sectors employed 1.495 million, 1.047 million and 4.640 million Americans respectively in 2020.[479]

The construction industry is dominated by small businesses. Two-thirds of the 753,000 establishments in the industry employ fewer than 5 people in 2020. Two-thirds of the 7.18 million employees work in businesses employing fewer than 100 people. There are 700 firms, or 0.1% of all construction firms, which employ more than 500 people.[480]

---

[474] "Interactive Access to Industry Economic Accounts Data ", U.S. Bureau of Economic Analysis. Link

[475] ibid.

[476] "New Study: Total Economic Contribution of Engineering an Architectural Services nearly $600 billion", ACEC Research Institute, Feb 2021. Link

[477] U.S. Census Bureau, 2000, CBP Tables 2020. Link

[478] "Construction: NAICS 23 ", U.S. Burean of Labor Statistic. Link

[479] U.S. Census Bureau, 2000, CBP Tables 2020. Link

[480] ibid.

© Strategy of Things, 2025. All rights reserved.

In May 2022, the seasonally adjusted annual rate of construction spending was $1.76 trillion.[481] Of that, $932.9 billion (52.9%) was for residential construction, while the remaining $829.4 billion was for non-residential construction such as commercial buildings, highways and utilities. Private construction accounted for $1.416 trillion (80.3%) of the total construction value, while public construction accounted for the remaining 345.9 billion (19.7%).[482]

The Architecture and Engineering industry is a major partner to the construction industry. The major categories of this industry include architectural, landscape architectural, engineering, drafting, building inspection, geophysical surveying and mapping, non-geophysical surveying and mapping and testing laboratories. This industry contributed $386 billion to GDP in 2019,[483] employed 1.6 million workers and generated $144 billion in annual payroll in 2020.[484] Half of the workers are employed in firms that range in size from 20 to 250 employees. These mid-size firms represented 6.6% of all architectural and engineering service firms and generated $73.3 billion in payroll (or 50.6%).

15.1.2. Industry challenges

The U.S. construction and engineering industry faces several challenges that constrain the growth of the industry. Five key challenges, which are relevant to IoT in construction and engineering are:

- Flat productivity
- Fragmented industry
- Labor shortage
- Slow adoption of digital technologies
- Low profit margins

Each of these is discussed below.

15.1.2.1. Flat productivity

Productivity in the construction industry has stalled, remaining unchanged for many years. From 2007 to 2020, productivity declined by -0.3% and -0.9% for residential and multifamily residential construction respectively and increased 1.0% and 0.2% for industrial buildings, highway, street and bridge construction.[485]

[481] "Monthly Construction Spending, August 2023 ", Census.gov. Link

[482] ibid.

[483] "New Study: Total Economic Contribution of Engineering an Architectural Services nearly $600 billion", ACEC Research Institute, Feb 2021. Link

[484] U.S. Census Bureau, 2000, CBP Tables 2020. Link

[485] Construction Labor Productivity, U.S. Bureau of Labor Statistics, September 21, 2021. Link

© Strategy of Things, 2025. All rights reserved.

Key reasons for stagnant productivity include poor organization, inadequate communication, flawed performance management, contractual misunderstandings, missed connections, poor short-term planning, insufficient risk management and limited talent management.[486]

15.1.2.2. Fragmented industry

Large-scale construction projects involve hundreds or thousands of individual businesses working together. The general contractor, or prime, is responsible for overall project management and coordination and risk management. The general contractor brings in subcontractors and specialists to perform specific work, such as electrical, plumbing, HVAC and other specialty work. In such a fragmented structure, staying aligned is challenging, miscommunication is common, and coordination is difficult.

Another consequence of the fragmented industry structure is that the contractor-subcontractor arrangement leads each business to work in a way to maximize their individual outcomes while minimizing their risks. This often results in adversarial contracting behaviors, leading to suboptimal working relationships and limits collaboration towards desired project outcomes.

15.1.2.3. Labor shortage

The construction industry has faced a shortage of skilled labor for several years. The number of job openings in the industry rose from an average of 95,000 in 2012 to 335,000 in 2021.[487] The Associated Builders and Contractors industry association estimated that the industry needs to hire an additional 650,000 workers above the normal hiring pace in 2022.[488] The infusion of $550B in approved federal spending is estimated to create a need for 3.2 million new workers.[489]

At the same time, the construction workforce is aging. The median age of construction workers is 42.3 years. Workers aged 55 and over, comprise 21.8% of the construction workforce in 2021,[490] and are nearing the average industry retirement age of 61.[491] Meanwhile, there are fewer workers between the ages of 16 to 24 entering the industry. In 2021, these workers comprise 9.5% of the total workforce.[492]

One immediate consequence of the labor shortage is the expected impact on the Infrastructure Investment Jobs Act.

---

[486] "The Construction Productivity Imperative", S. Changali, A. Mohammad, M. van Nieuwland, McKinsey & Company, July 1, 2015. Link

[487] "Industries at a Glance: Construction NACIS 23", Bureau of Labor Statistics. Link

[488] "ABC: Construction Industry Faces Workforce Shortage of 650,000 in 2022", Press release, Feb 23, 2022. Link

[489] "The Construction Labor Shortage is Set to Intensify Over Next 6 Months", P. Sission, Bisnow National, June 28, 2022. Link

[490] "Labor Force Statistics from the Current Population Survey", Bureau of Labor Statistics. Link

[491] "ABC: Construction Industry Faces Workforce Shortage of 650,000 in 2022", Press release, Feb 23, 2022. Link

[492] "Labor Force Statistics from the Current Population Survey", Bureau of Labor Statistics. Link

© Strategy of Things, 2025. All rights reserved.

15.1.2.4. Slow adoption of digital technologies

The adoption and use of digital technologies, including software for modeling, project delivery and collaboration are at low levels in the U.S. construction industry. For example, an industry survey found that 43% of U.S. civil engineers and contractors reported the use of digital tools and innovations compared with 66% of non-U.S. counterparts. The same survey found that 43% of U.S. civil contractors had low digital capabilities, compared with only 23% of non-U.S. construction companies. In contrast, 45% of non-U.S. construction and engineering companies reported high digital capabilities compared with just 20% for U.S. companies.[493]

Building Information Modeling (BIM) is a key digital technology. Only 16% of U.S. civil engineering and construction companies are well prepared to participate in projects using BIM, compared with 45% of non-U.S. companies.[494]

Owners, who contract with engineering and construction companies to design and build their projects, play an important role in driving digital adoption. In an owner survey, 54% of owners were highly engaged with digital workflow technology, compared with 42% of designers and contractors. Only 60% of owners, however, use those digital technologies for internal workflows, compared with 28% that extend that workflow to external companies.[495]

15.1.2.5. Low profit margins

Construction is a high risk, low margin business. A review of the net profit margins found that building construction general contractors, including operative builders, had a profit margin from 4.4% in 2016 to 6.7% in 2020.[496]

Similarly, heavy construction contractors had a profit margin of 2% in 2016 and 2.7% in 2020. Specialty trade contractors showed a similar performance at 2.1% in 2016 and 2.6% in 2020.

A review of the top 30 global construction and engineering companies, however, showed that the average Earnings Before Interest and Tax (EBIT) for the companies was 5.7% of sales.[497] For the U.S. companies in the group, the average EBIT was 11.3% in 2020 and 16.1% in 2021.

One of the reasons for this above average EBIT was attributed to the presence of construction companies whose primary activities were home construction, which has higher margins than civil construction projects. When the influence of homebuilders was excluded from the analysis, the global average EBIT was 5.0% of sales.

The key reason for these low profit margins is the rising cost of materials and equipment and supply chain disruptions that continue to reduce the industry's margins.[498] Other factors, such as

---

[493] "Digital Capabilities in U.S. Civil construction", Dodge Construction Network SmartMarket Brief

[494] ibid

[495] "Connected Construction: The Owners' Perspective", Dodge Construction Network SmartMarket Brief. Link

[496] "Profit Margin - Breakdown by Industry", Ready Ratios, 2022. Link

[497] "Global Powers of Construction, CPoC 2021", Deloitte, Figure 5.1., July 2022. Link

[498] "2022 Engineering and Construction Industry Outlook", Deloitte, 2022. Link

© Strategy of Things, 2025. All rights reserved.

labor shortages, supply chain delays, design errors, underutilization of equipment, jobsite accidents and change orders contribute to reduced profitability.[499]

15.2. IoT in the construction industry

The term industry 4.0 used in manufacturing has been adapted to create construction 4.0, which some classify as the digitalization of the construction industry and the digitalization of the construction process.[500]

Construction 4.0 is made possible through the convergence of construction and operations technology with information and digital communications technologies, IoT, data analytics, building information modeling (BIM), digital twins, additive manufacturing and Cyber Physical Systems. Construction 4.0 aims to automate the entire project lifecycle.[501]

The digital transformation of the construction industry offers the potential for better construction quality at lower prices with work completed in shorter periods of time along with significant improvements in safety and efficiency.[502]

Transformations can also lead to improved worker safety and site security, productivity improvements through scheduling and supply chain management, predictive maintenance to reduced downtime, streamlined collaboration and reduced waste. In addition, the digital transformation of the construction will address some of the current problems in the industry, including labor productivity, low profitability and worker shortages.

Traditional construction methods use physical copies of engineering drawings, markups and change orders to support an evolving construction project. These are shared between the contractors, subcontractors, consultants and other personnel. Due to the large number of parties involved, it is not uncommon for teams to be working with different versions of the engineering drawings, leading to procurement and construction errors along with schedule conflicts and delays.

At the heart of digital construction is building information modeling or management (BIM). BIM software technology is a 3D model that allows designers, planners and workers to work smarter and literally be on the same "page." The BIM software collects and stores all the information of the "parts" that is used in constructing a structure. Engineering changes are instantly propagated across the various drawings and teams are notified. Equally important, the use of BIM allows architects, contractors and engineers to plan, design, build and collaboratively manage the physical and functional characteristics of a building.[503]

Adding real-time information from worksite IoT sensors into the BIM forms a digital twin of the jobsite, linking the real-world jobsite progress to a continuously updated digital representation.

---

[499] "5 Reasons for Low Contractor Profit Margin", April 2021. Link

[500] "Construction 4.0", Encyclopedia. Link

[501] "Construction 4.0", Building Transformations. Link

[502] "Digital Transformation of Construction Organizations", IOP Science, 2019. Link

[503] "BIM and IoT: The Grandest of All Designs", World Construction Network, October 2019. Link

© Strategy of Things, 2025. All rights reserved.

AI is then used on these models or twins to detect, prevent, predict and optimize the physical environment.

GlobalData has predicted that construction companies will spend $1 billion on AI platforms by 2024[504] as advanced connected modeling proves its value to deliver significant improvements over the traditional CAD plans used in the field.

Even though Construction 4.0 offers many benefits, the construction and engineering industry has one of the lowest rates of digitalization adoption.[505] The low levels of digital transformation can be attributed to:

- The specific characteristics of the construction industry which include the custom nature of projects that lack repeatable activities
- Transient working interactions and teams
- The high levels of fragmentation across the value chain of contractors
- The decentralized nature of large firms which often acquire smaller firms and operate in silos.[506]
- The lack of budget and schedule accountability
- Risk aversion and skepticism due to reliance on traditional operation models
- Limited technical skills and talent retention.[507]

Despite these challenges, the construction industry is ready for technological change. The global IoT in construction industry market size was valued at $8.99 billion in 2021 and is expected to reach $29.72 billion by 2030.[508] In addition, construction projects are becoming increasingly sophisticated and complex, requiring firms to use new technologies to remain competitive.[509]

15.2.1. IoT use cases

Figure 15-1 shows a representative sample of construction related IoT use cases. The IoT use cases are organized into five categories. These are:

- **Engineering and Design.** These use cases support the activities involved in the design, planning and specification of the construction projects.
- **Construction.** These use cases are concerned with the support of the construction and management of the project.

---

[504] "Tech Spending in Construction to Rise As Activity Picks Up Again in the Industry", World Construction Network, June 10, 2021. Link

[505] "Digital America: A Tale of the Haves and Have-Mores", McKinsey Global Institute, December 2015. Link

[506] "Decoding Digital Transformation In Construction", McKinsey. Link

[507] "Beating the Low-Productivity Trap: How to Transform Construction Operations", McKinsey, July 2016. Link

[508] "IoT in Construction Market Size", Globe News Wire., September 2022. Link

[509] "Construction 4.0: A Roadmap to Shaping the Future of Construction", ResearchGate, October 2020. Link

© Strategy of Things, 2025. All rights reserved.

- **Site management.** This category of use cases supports the set of activities around the construction zone and facilities. This includes the materials, human resources, tools and structure to be constructed.
- **Supply chain and logistics.** These use cases support the activities involved with the movement of raw materials and finished products. The goods can be within the manufacturers and distributor's facilities, as well as those in supplier and distributor facilities and in transit between locations.
- **Equipment, tools and machinery.** These use cases support the equipment, machinery and tools that are used in the project.

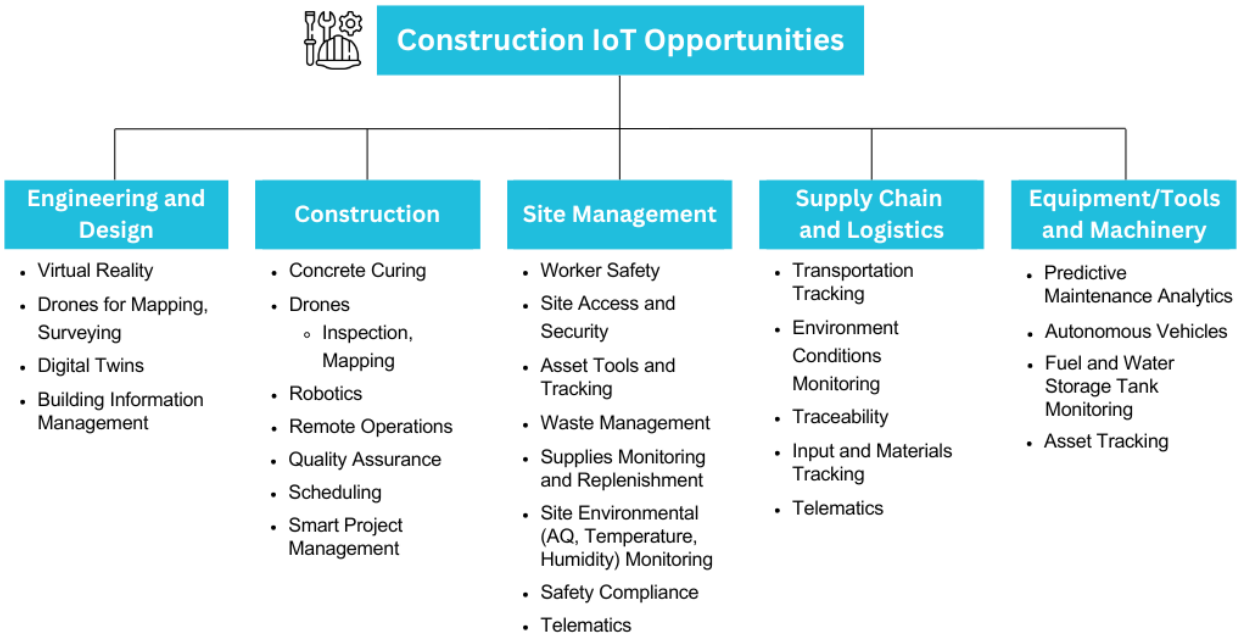


Figure 15-1: Construction: Use Case Categories and Selected Use Cases

There are many opportunities for IoT in construction, from operations related to the construction process, worker and site safety to compliance with government codes and regulations.

For example, imaging sensors and cameras can monitor construction progress and allow the early detection of conflicts or issues. Low cost IoT sensors added into freshly poured concrete provide managers with real-time status of the curing process, allowing schedule optimization and better workforce management. Workers on the jobsite could use wearable sensors to track their location, monitor site conditions and provide alerts if risky parameters are exceeded or dangerous locations are entered. These technologies can detect these conditions before or as they happen.[510] Wearables can also monitor heart rate for signs of stress, which can disrupt concentration and productivity and lead to injuries in critical activities. More futuristic applications include the use

[510] "IoT Applications in Construction", IoT for All, July 2020. Link

© Strategy of Things, 2025. All rights reserved.

of augmented reality (AR), virtual reality (VR) and mixed reality (MR) wearables that can allow users to plan and model sites and features prior to construction.

Modular construction and mass customization methods will continue as firms leverage production methods to lower costs and reduce waste. IoT is used in production lines to monitor environmental conditions, perform quality assurance inspections of in-progress and completed construction products, detect safety violations during production and track locations of outbound shipments to construction sites.

BIM and other modeling tools will continue to be adopted as digital plans become requirements for owners and project managers. Artificial intelligence will help architects so they can leverage historical design, building and construction data to save time.[511] AI can also help predict cost and timeline overruns and identify worker safety risks. IoT provides a variety of critical information that can be used by these software tools.

While IoT will enhance and improve various aspects of the construction processes, additional value is created in improving outcomes both before and after construction. For example, the use of drones equipped with cameras and sensors simplifies the survey of large project sites and facilitates project planning. Sensors on buildings and structures collect data that validate and refine the engineering design models, allowing these models to be extended to new projects. These same sensors can be used to monitor the structural integrity of a building or facility during its operational lifetime, providing building engineers and facility managers with an understanding of building health.

IoT also creates value in indirect activities associated with construction. For example, the construction industry is a heavy user of equipment and machinery. On a large construction site, asset tracking of equipment provides project managers with an understanding of their locations and facilitates the allocation, scheduling, mobilization, staging and demobilization of the machinery. Other IoT sensors monitor parameters, such as vibration and operating temperatures, which are used to proactively predict when the machinery needs to be serviced. This eliminates unplanned machinery downtime during construction and maintains project schedule. For original equipment manufacturers (OEM) dealers, providing support to equipment and machinery deployed in the field is a major activity. Remote monitoring and management of field machinery and equipment allows manufacturers to be proactive and agile in servicing their customers. Sensors around the jobsite could be used monitor noise and emissions levels to comply with local government regulations.

15.2.1.1. Use case and industry challenges alignment

The construction industry faces several challenges, some of which are described in Section 15.1.2. Figure 15-2 below shows the fit between the proposed use case subcategories and the documented industry challenges.

[511] "The Future of Construction – 2022 and Beyond", Blog, van Hooijdonk R. December 2021. Link

© Strategy of Things, 2025. All rights reserved.

Challenge	Role of IoT	Use case examples
Flat productivity	Boost productivity by enabling real-time tracking of equipment and materials, reducing downtime and waste.	• Input and materials tracking • Asset tracking • Telematics • Transportation tracking
Fragmented industry	Help integrate the industry by providing a unified platform for data sharing and collaboration among various stakeholders.	• Building information management • Digital twins
Labor shortage	Mitigate labor shortages by automating routine tasks, such as equipment inspection and inventory management, freeing up workers for more complex tasks.	• Worker safety • Safety compliance • Storage tank monitoring – fuel, water • Remote monitoring and operations
Slow adoption of digital technology	Drive digital transformation in the construction industry by demonstrating the tangible benefits of technology adoption such as cost savings and efficiency improvements.	• Robotics • Predictive maintenance analytics • Autonomous vehicles
Low profit margins	Improve construction quality and reduce rework and construction mistakes. Facilitate scheduling and project management to maximize utilization of general and specialized resources and timely delivery and availability of materials.	• Scheduling • Smart Project Management • Site access and security • Asset and tools tracking • Waste management • Supplies monitoring and replenishment • Traceability

© Strategy of Things, 2025. All rights reserved.

Figure 15-2: Construction: Use Case and Industry Challenges Alignment

15.2.1.2. IoT use case details

Additional details on the use case subcategories shown in Figure 15-1.are provided below in Figure 15-3.

Category	Use Case	Definition
Engineering and Design	Virtual reality	IoT data used to create real-time digital maps and digital twins of construction sites.
	Drones	Provide detailed information for planning, site inspections, design and mapping.
	Digital twins	IoT data, along with Building Information Management (BIM) output, create a real time version of the project or asset.
	Building information management	IoT devices provide input for BIMs to assist in creating real-time digital maps of Construction sites and operations and health data for post-construction buildings.
Construction process	Concrete curing	A wireless concrete sensor provides information on the state of concrete.
	Drones	Used for inspection of job sites, check work quality and construction progress.
	Robotics	Employed for repetitive low discretion jobs such as bricklaying, dry walls,
	Remote operations	Improved safety and compliance.
	Quality assurance	Information on the built status of assets.

© Strategy of Things, 2025. All rights reserved.

Category	Use Case	Definition
	Scheduling	Additional information for optimum scheduling.
	Project management	Management of contactors.
Site management	Worker safety	Location information or employees on site and other data from wearables improves worker safety.
	Site access and security	IoT can address issues of safety and site material shrinkage.
	Asset and tool tracking	Efficiency in the finding and using site assets and tools.
	Waste management	Reduced fines from inability to deal with waste appropriately
	Supplies monitoring and replenishment	Efficient management of supply and inventory levels.
	Site environmental monitoring	Examples include Air quality, humidity, temperature, supply, heat/humidity, fuel and concrete curing sensors.
	Safety compliance	Information to support safety requirements.
	Telematics	Identify vibrations, splits and states of necessary structure and common structures during and after development.

© Strategy of Things, 2025. All rights reserved.

Category	Use Case	Definition
Supply Chain and logistics	Transportation tracking	IoT in civil engineering gives the opportunity of improved labeling and trailing of materials or truck identification.
	Environment conditions monitoring	Some Construction elements and equipment have specific storage requirements. IoT devices can monitor metrics such as humidity, temperature and pressure.
	Traceability	Information on the provenance of assets.
	Input and materials tracking	Tag materials to reduce occurrences of theft and misplacement. These IoT-enabled tags can save time by making the Construction material easier to locate and monitor.
	Telematics	Information on asset status.
Equipment/ tools and machinery	Predictive maintenance	Monitors key parameters on machinery and equipment. Detects out of spec conditions early and alerts technicians to service equipment before failure.
	Autonomous vehicles	Precise positioning of transport assets.
	Storage tank monitoring – fuel, water	Information on storage status.
	Asset tracking	Information on asset location and status.

Figure 15-3: Construction: Use Case Details

© Strategy of Things, 2025. All rights reserved.

15.2.2. Market views of IoT in construction

To understand market views on IoT and to inform on our gaps discovery and analysis, our research team conducted a survey of 450 people, from adopters to solution providers, across the nine industries studied. The survey respondents were asked their opinion on the importance of IoT for the construction industry over the next 5 to 10 years. Figure 15-4 below shows an expected relative medium to high impact of IoT, as compared to other industries. Despite these views, IoT adoption in the industry is low. There are several factors hinder the adoption and use of IoT in construction. These will be discussed in the following section.

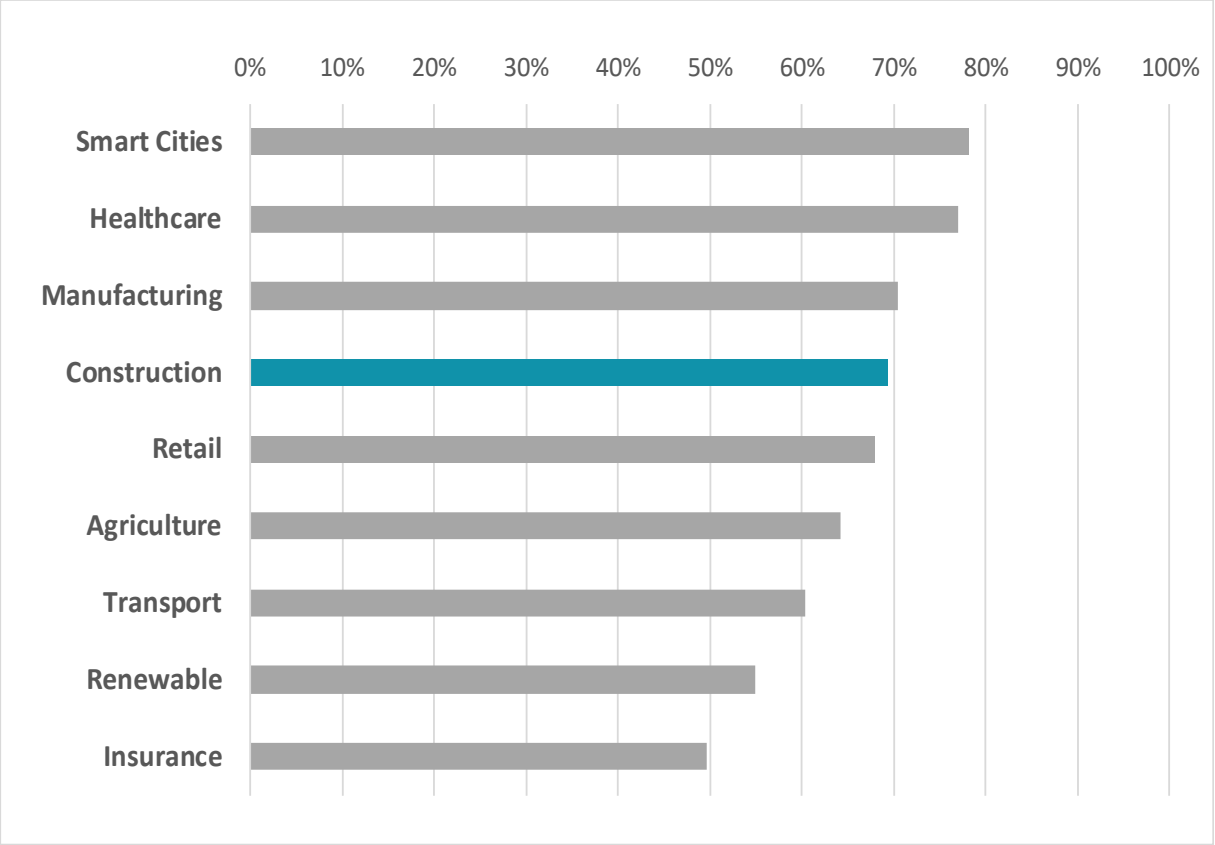


Figure 15-4: Construction: Importance of IoT

In support of the use case analysis, survey respondents were asked to rate the impact of these use case categories on the construction industry.[512] Figure 15-5 below shows the percentage of responses in each impact category for each use case category. Overall, this shows a bias to a high impact of the use case categories in construction.

[512] In your view, what will be the impact of these use cases in construction over the next 5-10 years?

© Strategy of Things, 2025. All rights reserved.

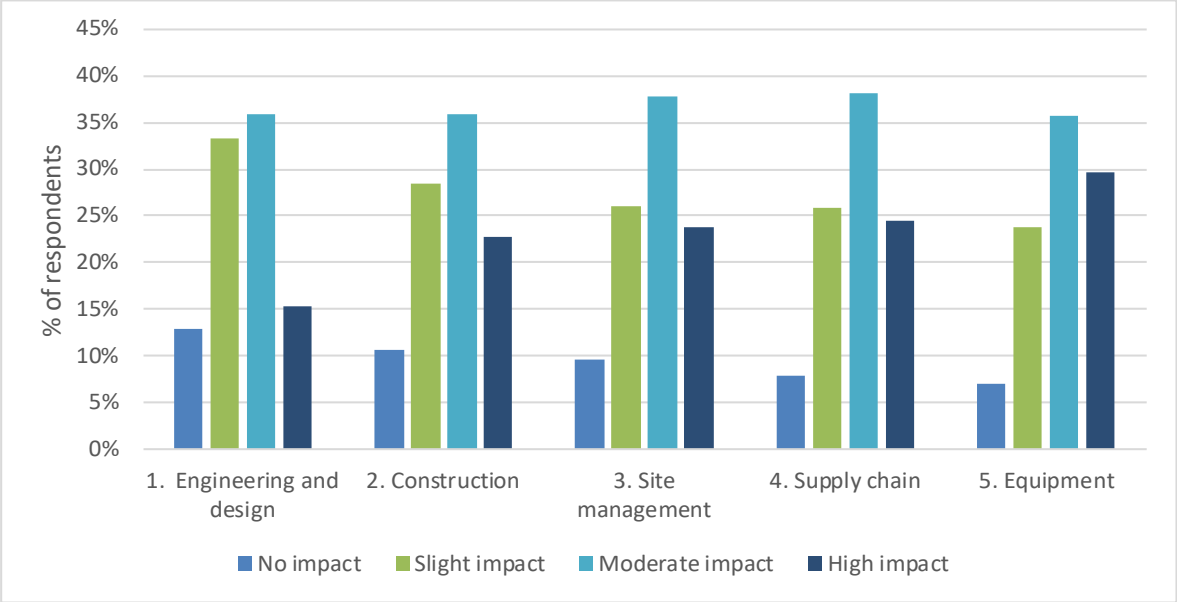


Figure 15-5: Construction: Use Case Category Impact

In addition, respondents were asked about their confidence in suppliers delivering the services required to operationalize these use case categories.[513] Figure 15-6 below shows the percentage of responses in each confidence category for each use case category. Overall, their responses indicate some confidence in the ability of suppliers to deliver the necessary services.

[513] How confident are you that suppliers will deliver the services that construction organizations need from these technologies over the next 5-10 years?

© Strategy of Things, 2025. All rights reserved.

Figure 15-6: Construction: Confidence in Delivering Use Case Categories

15.3. IoT gaps and findings in construction

A combination of interviews, secondary research and surveys was conducted to identify and understand the opportunities and challenges to the development and adoption of IoT. Each research method approached the challenges from a different perspective.

For example, the survey targeted a large audience but asked specific questions that supported the economic analysis. The interviews targeted a small number of people who provided deeper insight and context to supplement the information already collected. Finally, the desk research, consisting of a review of online news articles, published research reports, vendor and government white papers, blogs, webinars, videos and other content, provided a broad overview of the application of IoT in the industry.

In our survey, respondents were asked to choose the most important technology areas to operationalize IoT in their industry. Figure 15-7 below shows the top 10 IoT technologies and the percentage of respondents who chose that technology.[514] The survey results are not seen as a technology gaps list, but rather an indication of what is important to the respondents. This information partially informs the gap selection process.

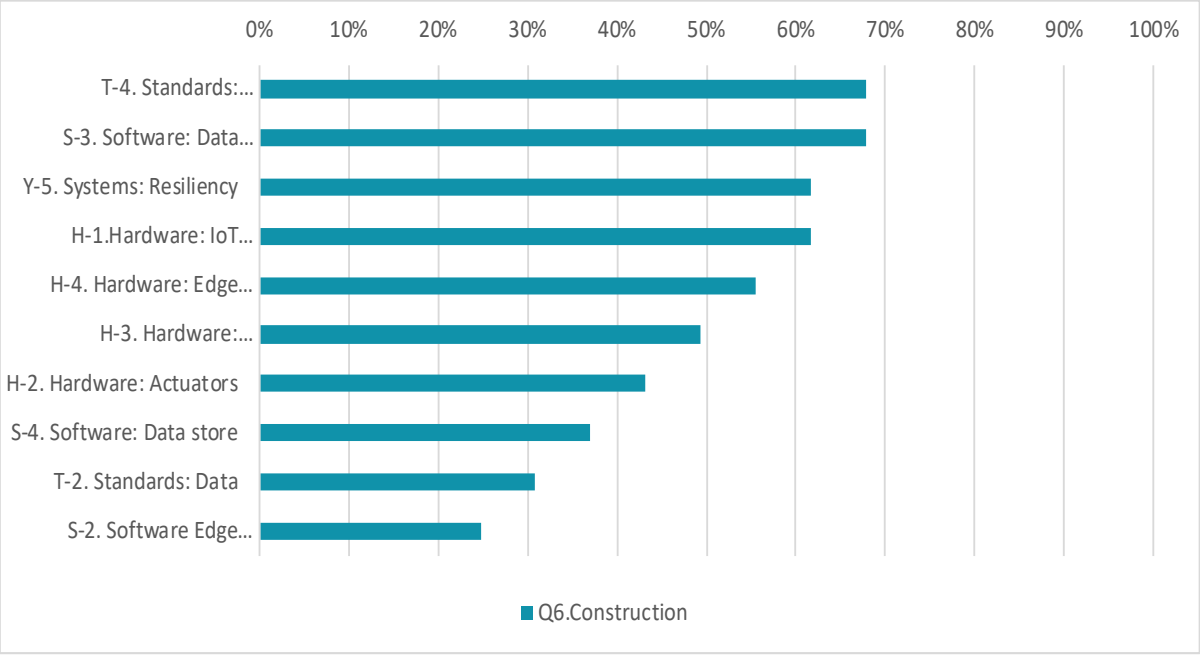


Figure 15-7: Construction: Top 10 Most Important Single Technologies

15.3.1. Top technology challenges

[514] Respondents were asked to choose up to 5 out of the 25 technologies listed.

© Strategy of Things, 2025. All rights reserved.

Based on the approach described above, the two IoT technology challenges were identified as below:

- BIM-IoT data integration
- Data standards and interoperability

15.3.1.1. Challenge #1: BIM-IoT data integration

Building Information Modeling (BIM) systems are foundational for the digital transformation of the construction industry. The integration of IoT with BIM provides owners, builders and facility operators with real time physical "perception" information to augment static data throughout the asset lifecycle, from planning, design, construction and operations.

For example, IoT sensors validate modeling assumptions during design, measure the progress and conflicts during construction and monitor and manage the constructed facility during its useful life. BIM-IoT integration is pertinent in four areas, construction operation and monitoring; health and safety management; construction logistics and management; and facility management.[515]

Integrating IoT with BIM faces several challenges including:[516]

- **Construction data are siloed and fragmented**. Different contractors and project teams may use different software, systems and tools. Using these data requires maintaining and integrating multiple data sources, versions and formats over its useful life cycle. IoT data, generated by a variety of heterogeneous devices presents large amounts of time varying data in different formats. These disparate data become significantly more complex with scale.
- **Ownership concerns inhibit data sharing**. The data provides developers and contractors with insights that can provide them with a competitive advantage. The original data owners, however, lose control of that data and leverage when integrated into a broader BIM database owned by the project owners and contractors.
- **Lack of trust in a fragmented value chain**. The construction industry requires many businesses to work together. Each business has a contractor-subcontractor arrangement and works to maximize its own business outcomes instead of the overall project outcomes. This arrangement precludes true transparency, communication and collaboration in integrating information and operations.
- **Security concerns about IoT.** Cybersecurity and data privacy concerns inhibit the adoption of IoT on construction projects or limit what applications are adopted or the number of devices employed.

---

[515] "Nexus Between Building Information Modeling and Internet of Things In the Construction Industries." Appl. Sci. 2022, 12, 10629, Mohammed, B.H.; Sallehuddin, H.; Yadegaridehkordi, E.; Safie Mohd Satar, N.; Hussain, A.H.B.; Abdelghanymohamed, S. Link

[516] "A Proposal to Harmonize BIM and IoT Data Silos using Blockchain Applications", Z. Bakar and M. Mathews, 5th CitA BIM Gathering Proceedings 2021, p129-141, September 21-23, 2021. Link

© Strategy of Things, 2025. All rights reserved.

Despite the benefits and the potential of BIM-IoT integration, current research is both nascent and limited. Initial research has identified areas to be explored including:

- **BIM-IoT integration.** Integrating these data streams to provide insights. For example, construction operation and monitoring measures build progress and performance while facilities management measures building operations performance such as energy management.
- **Open BIM platforms.** These can integrate with IoT applications and platforms as well as building management systems. An open standard approach can accelerate adoption in an industry where there is a wide variety of protocols and information exchange standards.[517]
- **Standards.** These address the interoperability gaps between the integration and the use of traditional file-based data stored in BIM with time series IoT data over the facility life cycle. In addition, data management models and approaches will need to be developed to support the integration over the data life cycle.

15.3.1.2. Challenge #2: Data standards and interoperability

The lack of interoperability is a major barrier to the digital construction and operations of the constructed asset. Project teams in construction are assembled from different businesses working together in a "one-off" way." Each business brings its own technologies and software tools to the project. These tools, however, often cannot communicate with each other. As a result, data are exchanged verbally, or through manual entry into disparate unconnected systems, or not at all.

In some cases, interoperability exists with a curated set of technologies within a vendor's ecosystem. Technologies within the "walled garden" can communicate with each other, while those outside are unable to communicate or must rely on a third-party middleware software to bridge the gap and become "compatible."

IoT applications and systems such as BIM, Project Management Information Systems (PMIS) and building management systems in completed buildings that operate in this environment may not be able to integrate into existing systems or require adapters or middleware.

> *... in the design and construction industry, we have seen decades and decades of resistance to non-proprietary standards by [solutions vendor] organizations that feel they have more to gain by blocking collaboration in that way than by forcing their own market share. That is slowly beginning to change.*
>
> *Tony Rinella, Strategic Building Innovation*

Building Smart International, a community for the built environment, has identified three areas for further data standards development.[518] These are:

---

[517] "A Framework for Integrating BIM and IoT Through Open Standards", B. Dave et al, Bhargav Dave, Andrea Buda, Antti Nurminen, Kary Främling, Automation in Construction, Volume 95,2018, Pages 35-45, ISSN 0926-5805. Link

[518] "Building an Ecosystem of Digital Twins", buildingsmart International Position Paper, 2020. Link

© Strategy of Things, 2025. All rights reserved.

- Extending interoperability between the various data model standards, such as geospatial information in planning applications, engineering models for construction and data models in building operations applications
- Standards for data management and integration, focusing on semantic interoperability and precision. That is, the data to be exchanged between the various applications have an unambiguous meaning that is mutually understood and accurately describes the intended meaning.
- Data security and privacy around the data created, collected, ownership and how it is used.

> *We can barely let the systems talk to each other, let them communicate, let them be interoperable, let alone take good intelligent actions. Certainly, we are nowhere near the vision that we all have of digital twins and IoT enabling us to become more autonomous…. We lack the data standards and more importantly, the ability to relate the data standards with the value proposition for the stakeholders and how to present that data in a way that will work commercially, financially and operationally.*
>
> *Dr. Calvin Kam, CEO, Strategic Building Innovation*

15.3.2. Other challenges

In addition to the technology challenges, our research has identified other challenges that impact IoT adoption. These challenges did not meet the criteria for research consideration because they were neither a technology challenge or a technology related challenge that can be addressed by current marketplace offerings or capabilities.

These are:

- Fragmented industry structure
- Lack of asset owner requirement
- Adoption resistance

Each of these is discussed below.

15.3.2.1. Fragmented industry structure

This industry business model brings together project teams of contractors, subcontractors and specialists from many different businesses. These contractor-subcontractor relationships, however, result in a lack of "connectivity" between the processes and the hundreds of firms involved. In this environment, IoT may be used by a subcontractor for their own benefit, but that benefit is not shared across the broader project team.

> *Let's say you want to build a hotel. And the way that process normally works is you give the project over to a general contractor. The GC is a different company and they say I can build this thing for 20 million and then they talk to an architect*

© Strategy of Things, 2025. All rights reserved.

who is a different company and then they hire maybe two to three hundred subcontracting firmsm that do different parts of it. It's highly fragmented and it's a bunch of mom-and-pop operations that put this hotel together. And because there's no connectivity between all the different players, none of them can think about optimizing the use of technology because they are very focused on a very narrow piece.

... the average margin for the GC is 4%. So, they're very focused on the big levers for getting the project done on time, which includes the scheduling, making sure there's no rework, all of that. But because they're stuck in this fragmented mess, they can't think about it holistically like 'How do I solve this problem of design rework?' which involves interacting with the architects in a more collaborative way, rather than acting as two separate entities. This is a different way of working for them as they don't understand that way. So structurally, they cannot fix the endemic problem because they're part of the problem.

RJ Mahadev, President, AIOTA

15.3.2.2. Lack of asset owner requirement

If the owner told the architect to put that stuff in the spec, then it gets in. An architect is not going to do it just because it's the right thing to do. And no contractor is going to do it just because it's the right thing to do. Somebody's got to be pulling it and that somebody needs to be the owner. Not enough owners know that they could or why they should.

Steve Jones, Senior Director, Industry Insights Research, Dodge Data & Analytics

Despite the benefits of digitalization and IoT in reducing risk and facilitating project success, the construction industry is "behind the curve" in digitalization and technology adoption. There are a variety of reasons, including a fragmented industry structure that leads to suboptimization of project processes, a lack of awareness of the value of technology and lack of owner requirement of the technology into the project.[519] [520] [521] This lack of owner requirement comes from a lack of awareness of the value of technology and prevents the use of IoT in construction projects and in the built asset.

Contractors are hired to build what's in the design firm's spec. That's their job and to do it as safely as they can so they don't incur liability there. And to meet

[519] Interview notes, Steve Jones, Steve Jones, Senior Director, Industry Insights Research, Dodge Data & Analytics, April 5, 2022

[520] Interview notes, RJ Mahadev, President, AIOTA, March 22, 2022

[521] Interview notes, Dr. Calvin Kam, Strategic Building Innovation, April 19, 2022

© Strategy of Things, 2025. All rights reserved.

their schedule and budget commitments so they don't get sued. That's it. There is no more than that. They're not trying to reinvent the industry. Nobody wants to reinvent this industry. They will do it when somebody tells them to do it and will pay for it.

The owners are never going to say 'I want IoT.' The owners are going to say 'Are you telling me I can operate my building at 9% less energy if I invest X in sensors and in systems to monitor my usage? And my payback is four years? I'm in!' Then the design firm gets told to design it in. The contractor gets told to buy it and install it.

Steve Jones, Senior Director, Industry Insights Research, Dodge Data & Analytics

Part of the driver is a short cycle profit constraint for designers and builders and a lack of well substantiated numerical evidence for the owners to understand that they will get a quick payback on investments in IoT. Unfortunately, it's only those who have a vision who are able to justify making investments in these areas.

Tony Rinella, Strategic Building Innovation

There is no forcing function across the fragmented way that things work [today]. The only thing you can address is 'how do I create policies that will push them in the direction that you're either forced to use it or they see the value of it'.

RJ Mahadev, President, AIOTA

There are examples of projects where owner mandates have driven adoption of adjacent digital technology. In the United Kingdom, public sector construction projects make up 40% of the construction industry's workload.[522]

The United Kingdom's Government Construction Strategy, published in 2011, requires all centrally procured public sector construction projects to be "fully collaborative 3D BIM with all project and asset information, documentation and data being electronic, as a minimum by 2016."[523]

In the 2016-2020 update of this strategy, the requirement was quantified as BIM Level 2.[524] This mandate is being adopted. A 2021 survey of 1,000 UK construction professionals reported BIM

[522] "Government Construction Strategy", Cabinet Office, Page 5, May 2011. Link

[523] ibid, Page 14

[524] "Government Construction Strategy 2016-20", Infrastructure and Projects Authority, Page 6, March 2016. Link

© Strategy of Things, 2025. All rights reserved.

adoption rates of 70%, with 99% of people at firms with 51 employees or more adopting BIM. At smaller firms 57% are using BIM.[525]

In the United States, the federal Government Services Administration (GSA) is responsible for the ownership, management and operation of all federal facilities. In 2003, the GSA set a goal to "require interoperable Building Information Models (BIM) on FY06 projects in support of improving design quality and construction delivery."

The GSA took a subset of BIM and starting in FY07 and mandated the use of Spatial BIM, focusing on spatial validation at an early design stage, for "prospectus level projects funded by Congress for design."[526]

Similarly, the U.S. Army Corps of Engineers mandated the use of BIM for its projects. This was driven by the requirement for contractors to build a particular set of identical buildings without developing new documentation for each new build.[527] There is no national level agency, however, that oversees the construction industry in the United States. Most of the regulation is done at the state and local levels.

> *It's the carrot, the stick and the tambourine…the carrot which is 'why you should do it' [benefits], the stick is 'why I have to do it' [compliance] and the tambourine is 'you got to make people know about it' [awareness]. The government actually has at least two and a half sticks - the stick and the tambourine. The GSA did a pretty decent job with BIM. Even though they're out to solve one little problem, they helped to grow BIM. The Army Corps helped to grow BIM too, even though they just wanted to solve a very specific problem of building out the prototype buildings without variation.*
>
> *Steve Jones, Senior Director, Industry Insights Research, Dodge Data & Analytics*

Outside of asset and project owner mandates, there are a small number of examples where digitalization and IoT are used in construction. Large construction projects, managed by the large and major general contractors, incorporate technology and digitalization in the day-to-day execution and management of their projects. This adoption is driven by sophisticated project and asset owners and the need to be competitive against other contractors when bidding on major projects.

> *... the big guys compete for the big projects with each other. And they have more sophisticated owners. So when the first big guy went in and said, 'I'm doing it this way and on my last three projects, I was able to improve this aspect of*

---

[525] "NBS Digital Construction Survey explores BIM uptake in 2021", A. Davis, Highways Today, January 10, 2022. Link

[526] "BIM: The GSA story", S. Hagen et al., Journal of Building Information Modeling (JBIM) National Institute of Building Sciences, April 1, 2009. Link

[527] Interview notes, Steve Jones, Steve Jones, Senior Director, Industry Insights Research, Dodge Data & Analytics, April 5, 2022

© Strategy of Things, 2025. All rights reserved.

performance, that aspect of performance and that aspect of performance. If you hire me, I'm bringing that knowledge, technology and whatever else, to you'. Then they win the job while everybody else [not doing the same things] has to scramble to get it. That's what happened with BIM with construction. Somebody had it and then everybody else had to have it. But that's because they all compete on projects with relatively sophisticated owners.

Steve Jones, Senior Director, Industry Insights Research, Dodge Data & Analytics

The adoption of technology on projects managed by the large construction firms and those specified by the U.S. government agencies represents a small fraction of all construction projects. Without the influence wielded by the UK government for digitalization, adoption of technology and digitalization in the United States will likely be limited.

Even if the federal government can do things really well, they [GSA] only represent one percent of the real estate portfolio across the United States even if they may have ten thousand buildings and five hundred million square feet. It is very difficult to diffuse change even with good federal government adoption. They can demonstrate, they can be a champion, but it still takes one owner at a time, one return on investment at a time

Dr. Calvin Kam, CEO, Strategic Building Innovation

15.3.2.3. Adoption resistance

Technology isn't the problem. What's needed to move the needle in construction isn't going and developing more technologies… It's how do we drive first adoption and then second implementation?

Steve Jones, Senior Director, Industry Insights Research, Dodge Data & Analytics

Adoption reluctance is slowing the use of technology in the construction industry. In the interviews, several themes were repeated. These themes included:

1. **"Things still got done with the status quo."** While technology can simplify and enhance some construction operations, the metric that "things still got done" continues to reinforce the reluctance to adopt technology on projects. Despite the value of technology, a lack of a "before and after" quantitative metric undermines an objective analysis of the benefits provided.

... the problem with construction is nobody measures what they did yesterday. Therefore, they don't have any idea how much better it could be. Or even really

© Strategy of Things, 2025. All rights reserved.

how bad it is because the buildings still get built and they still make their boat payments, they got their vacation house.

Steve Jones, Senior Director, Industry Insights Research, Dodge Data & Analytics

There is no LEED standard for any kind of tech at all. We've tried to introduce something like that in terms of maturity models. It's like 'so I'm at the 30% level, so what? I'm still getting the building built and paid.' There's nobody's not hiring my firm because I don't have a star on my door that says I'm one of the most technologically savvy firms.

Steve Jones, Senior Director, Industry Insights Research, Dodge Data & Analytics

2. **Risk aversion.** While the use of IoT and technology provides benefits during the construction process and to the operation of the constructed asset, a culture of risk avoidance limits adoption of new technologies.

General contractors don't build anything. They manage risk. That's their job. That's all they do. Therefore, they are by nature risk averse.

There's also a reluctance to adopt. The rule I use is everybody wants to be first or third. Why is that? Because they want you to adopt it first and get it all messed up. And then they want me to come in second and fix it and tell them how to do it. And then they're all in, because they want to beat all their competitors but they don't want to take any of the risk. The pioneers get the arrows, the settlers get the land. That's construction. Everybody wants to be first to be third. So it's extremely difficult to find the handful of people like the Mortons and the DPRs, that will actually be the leaders. And some of those guys are developing their own offerings and commercializing them to a small degree now. But it's a difficult industry to get adoption of things that are different.
Steve Jones, Senior Director, Industry Insights Research, Dodge Data & Analytics

In many cases, it's about mindset. It's about the mindset of our professionals being risk averse and staying with the old way business model… In some cases, it's about technology. The technology is not as reliable, mature, easy to use or where it should be. Or the technologies may not be totally fitting for the construction industry. We do need a lot of heroic efforts to make the technology work for our industry.
Dr. Calvin Kam, CEO, Strategic Building Innovation

© Strategy of Things, 2025. All rights reserved.

3. **The "right" problems are not addressed**. While there are many IoT solutions in the market that offer value in construction processes, the technology is not necessarily addressing a highly visible problem. Alignment of the solution with those day-to-day problems that cause the most difficulties, reduce risk or address compliance issues will motivate adoption.

   This industry has problems on projects all day long and they just need fewer problems on their projects… you only get traction, where there's the highest need. You have to look at what is it that is the most toxic [problems] and which trades caused the most problems for the general contractor. General contractors, at the end of the day, hold the insurance and answer to the owner. So the trades that cause the general contractor the most problems, the most unplanned work, gets addressed. You have to always follow the money. Look at where the highest risk is and where the biggest financial exposures are. That's where the bandages need to be applied. And that's where the technology needs to be applied and that's where it will likely get applied. … When you can point to either real money or improved safety, better schedule compliance. That's how you have to make things tangible for anything to get adopted. So none of these things were adopted because they're IoT. They happen to be IoT.

   Steve Jones, Senior Director, Industry Insights Research, Dodge Data & Analytics

4. **People readiness.** A common innovation adoption barrier is resistance to change. This barrier is common across multiple industries and is exacerbated by the extent and complexity of the change, the need for new skills, roles and responsibilities.

   One thing we encounter often is the need to make sure everyone sees their role, their value and their benefit in the new order that we are proposing. That happens on an individual level, where someone who is providing a service doesn't want to become obsolete. If they find a high barrier to adopting the new technology, then blocking the new technology becomes a very viable solution for them.
   Tony Rinella, Strategic Building Innovation

   Education is an important part for IoT adoption… It should be one direction that the industry should put more focus on to bring the education part to help the industry, to help different project stakeholders, to really understand it can bring value. And it won't be a difficult thing and we can start with simple steps to make it simple, better visuals, demos, simple use cases, to help the industry understand the value and benefit of IoT.
   Eva Yu, Strategic Building Innovation

© Strategy of Things, 2025. All rights reserved.

Appendix: Insurance

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

© Strategy of Things, 2025. All rights reserved.

16. Appendix: Insurance

This section describes the research findings for IoT technology infrastructure in the U.S. insurance industry. The topics covered are:

- Industry overview
- Use of IoT in insurance
- IoT challenges in insurance

16.1. Industry overview

The insurance industry facilitates the operation and resilience of the U.S. economy and its people. For example, credit insurance allows merchants, manufacturers and banks to extend credit to their customers by protecting them from losses or damages resulting from the nonpayment of debts.

The ability to extend credit is essential to businesses and the wider economy. Property and casualty insurance helps people, businesses and communities recover and rebuild from natural and human-caused hazards and disasters by defraying the financial costs. Health insurance enables Americans to receive healthcare by partially defraying the costs of care. Reinsurance, or insurance for insurers, enables insurance companies to operate, encourages new insurers to enter the market and provides the insurers access to global resources to expand and diversify risk.

16.1.1. Key facts

The insurance industry created $695.2 B dollars of value in Q1 2022, representing 2.85% of the national GDP of $24.39 trillion.[528] The insurance industry GDP contribution percentage has stayed constant between 2.8% to 2.9% during the period 2017 to 2021, except for 2020, when its contribution was at 3%.[529]

Insurance falls into one of three broad categories. These are property and casualty such as automobile, home and commercial insurance, life insurance and annuities and healthcare. The U.S. insurance industry underwrote $1.351 trillion in premiums in 2021. Of that, $715.9 billion or 53%, was for property and casualty and $635.7 billion or 47% was for life Insurance and annuities.[530]

The U.S. insurance industry employed 2.8 million Americans in 2021.[531] More than half, 56% or 1.57 million, were employed by the insurance providers or carriers. The remaining 44%, or 1.23 million, were employed at insurance agencies and brokers and other related service providers.

---

[528] "Insurance Carriers and Related Activities, Q1 2022, Value Added by Industry", Bureau of Economic Analysis. Link

[529] "Contribution to Gross Domestic Product", Insurance Information Institute. Link

[530] "Facts + Statistics: Industry Overview", Insurance Information Institute. 2022. Link

[531] ibid.

© Strategy of Things, 2025. All rights reserved.

Insurance brokers and agencies employed 881,500 people, representing 31.4% of those who work in the insurance industry.[532]

There were 181,309 insurance related business establishments in the United States in 2020. These businesses combined to pay $248.3 B in annual payroll. Most,150,380 or 82.9% were agencies, brokerages or those who provide insurance related services. They created $91.9 B (37%) in total annual payroll.[533] The remaining 30,929 businesses were insurance carriers, including reinsurers.[534] They created the bulk of the total annual payroll with $156.4 B (63%).

Insurance agencies, brokerages and other service provider firms tend to be smaller businesses. About three quarters, 108,460 or 72.1%, of these businesses employ less than 5 people. These small firms employed 195,103 people and paid $10.2 B in annual payroll in 2020, representing 11.1% of payroll from all agencies, brokerages and service providers. There are only 174 firms (0.12%) that employ 500 or more people. They employed 223,091 people and paid $16.36 B in annual payroll, representing 17.8% of payroll from all agencies, brokerages and service providers.

Insurance carriers tend to favor smaller scale entities. About half, 16,480 or 53.3%, of these business establishments employed less than 5 people. These smaller establishments employed a total of 27,242 people and paid $2.92 B in annual payroll in 2020, representing 1.9% of payroll from all carriers. There are only 652 firms (2.1%) that employ 500 or more people. They employed 853,615 people and paid $83.9 B in annual payroll, representing 53.7% of payroll from all insurance carrier establishments.[535]

16.1.2. Industry challenges

The American insurance industry faces several challenges that constrain the growth of the industry. Four key challenges, which are relevant to the Internet of Things in insurance are:

- Changing customer expectations accelerated by the pandemic.
- Growing underwriting risks in emerging areas.
- Commoditization of insurance products.
- Legacy infrastructure hinders digital transformation.

Each of these is discussed below.

[532] ibid.

[533] U.S. Census Bureau, 2000, CBP Tables 2020. Link

[534] ibid.

[535] ibid.

© Strategy of Things, 2025. All rights reserved.

16.1.2.1. Changing customer expectations accelerated by the pandemic

As customers turn to online channels to purchase goods and services, they expect to do the same for insurance products. From going online to learn, consider and purchase insurance products to filing claims and managing their policies, customers expect Amazon-like personalized "instant gratification" engagements and communications.

A survey conducted by global consultancy PwC in 2021 found a 45% and 77% increase in the number of customers who expected online support and the ability to submit claims through mobile devices respectively compared to the 2018 survey.[536] These expectations became more pronounced during the COVID-19 pandemic as in-person interactions moved online. The pandemic also changed the types of insurance products people wanted. For example, a survey conducted by the global consultancy EY found that 70% of consumers wanted usage-based car insurance since they were driving and commuting less.[537]

While insurance startups, "insuretechs", have offered innovative products and engaged online with policyholders for some time, traditional insurers are challenged to implement similar digital initiatives. The COVID-19 pandemic exacerbated this challenge and resulted in many traditional companies striving to provide digital services and experiences.[538]

Building on the EY survey, usage-based automobile insurance policies began to use telematics devices in vehicles to monitor miles driven and driving behaviors such as speeding and hard braking. This can provide customers with more control over their insurance premiums, incentivize safe driving and provide unique client touchpoints for insurers to add value.[539]

These new experiences and insurance products, however, require new business and operating models. A PwC survey found 53% and 48% of insurers identified "lean operations" and "customized products" respectively as disruptive industry trends to support these emerging market needs.[540]

Insurers that do not respond to changing customer needs run the risk of losing customers to competitors as there are low switching costs. A new customer acquisition costs around nine times that of retaining a customer.[541] A March 2022 survey, conducted by Prosper Insights and Analytics, reported 18% of millennials planned to switch auto insurance in the next six months.[542] A JD Power loyalty survey for the 4th quarter of 2022 reported 12.1% of auto insurance buyers were shopping for quotes.[543]

---

[536] "Next in Insurance: Top Insurance Industry Issues In 2022", PWC. Link

[537] "Are Your Insurance Solutions In Tune With New Consumer Needs?", B. Wassink, EY Insights, February 16, 2021. Link

[538] "2020 CIO Survey", KPMG. Link

[539] "Usage-Based Vehicle Insurance", IoT for All. Link

[540] "Insurers aim to become masters of risk management", PWC. 2022. Link

[541] "The Customer Experience Overhaul in Insurance", Forbes. April 2022. Link

[542] "The Customer Experience Overhaul in Insurance", Forbes. April 2022. Link

[543] "Auto Insurance Shopping – and Switching – Increases", C. Hemenway, Forbes, January 24, 2023. iLink

© Strategy of Things, 2025. All rights reserved.

16.1.2.2. Growing underwriting risks in emerging areas

Insurance companies are profitable and remain solvent when they can properly identify, quantify and manage underwriting risks. There is evidence that both risks and their impacts are increasing. In 2022, there were 18 separate billion-dollar weather and climate disaster events which totaled $165 billion in damage.[544]

In other risk areas, ransomware attacks increased by 151% in the first half of 2021, compared with the same period in 2020. There were 341 million attempted ransomware attacks in the first half of 2021, compared with 305 million for all of 2020.[545] The average ransomware payment rose to $570,000 in the first half of 2021, an 82% increase from $312,000 from the same period in 2020.[546] One report showed $1.8 billion in insured cyber losses in 2019, a 50% increase from the previous year.[547]

The increase in risk events and resulting payouts have led insurers to higher losses than expected, leading to lower profitability. Insurers are responding by increasing premiums, underwriting fewer policies or canceling policies for high-risk customers.

In California, there was a 31% increase in policy non-renewals for homeowners in 2019,[548] after the 2017 and 2018 wildfires led California insurers to pay out over $29 billion in claims while only collecting $15.6 billion in premiums.[549] It is also reported that homeowner policy premiums rose 12.1% on average between 2021 and 2022. In some states deemed riskier, rates rose even higher.[550] Similarly, cyber insurance rose by an average of 28% in the first quarter of 2022 compared to the same period a year ago.[551] At the same time, cyber insurance is more difficult to find, and insurers are imposing stricter requirements.

16.1.2.3. Commoditization of insurance products

Insurers operate in a competitive marketplace and have long been exposed to commoditization. Buyers of property and casualty insurance often cite price as the main reason for purchasing a

---

[544] "Billion-Dollar Weather and Climate Disasters", NCEI. October 2023. Link

[545] "Ransomware Volumes Hit Record Highs as 2021 Wears On", T. Seals, ThreatPost, August 3, 2021. Link

[546] "Average Ransomware Payment Hits $570,000 in H1 2021", Dark Reading staff, Dark Reading, August 9, 2021. Link

[547] "Cybersecurity Insurance Has a Big Problem", T. Johansmeyer, Harvard Business Review, January 11, 2021. Link

[548] "Risky Business, Climate Change Turns Up the Heat on Insurers, Policyholders", Reuters, November 2021. Link

[549] "Regulators Should Identify and Mitigate Climate Risks in the Insurance Industry", American Progress. June 2022. Link

[550] "Home Insurance Prices Are Rising Even Faster Than Inflation," Policy Genius, July 2022. Link

[551] "Rising Premiums, More Restricted Cyber Insurance Coverage Poses Big Risk for Companies", B. Violino, CNBC, October 11, 2022. Link

© Strategy of Things, 2025. All rights reserved.

policy.[552] Others purchase from brokers or aggregators instead from insurers and their agent representatives, which distances the buyer from the brand.

The shift to online channels and digital experiences to address customer demand contributes to the commoditization of insurance products. For example, many online sites provide price transparency and online price comparisons.[553] One company even provides personalized insurance recommendations based on driving habits monitored from your vehicle and alerts customers when their algorithm has found a better policy based on the collected driving data.[554]

In addition to traditional insurance carriers, insurers must also compete against insuretechs in the marketplace. These insuretechs have disrupted traditional business and operating models to offer innovative insurance products such as usage-based policies, streamlined online processes for underwriting and claims, while increasing accessibility and customer experience.

The global insuretech market is projected to grow at a Compounded Annual Growth Rate (CAGR) of 46.1% between 2022 and 2030.[555] In this market, it is increasingly difficult to differentiate and retain and attract customers. Ultimately, this places additional pressure on traditional insurers to innovate or suffer loss of customers and slimmer profitability.[556]

16.1.2.4. Legacy infrastructure hinders digital transformation

In response to changing customer needs for innovative products and new engagement methods, traditional insurers are transforming their business and operating models. Unlike the insuretechs whose disruptive business capabilities are typically built around lean digital operating models and technologies,[557] traditional insurance carriers are saddled with legacy technologies and an inability to modernize legacy infrastructures.

A 2019 Center for the Study of Financial Innovation survey of insurance providers reported that "the urgent need for business and technology modernization poses the greatest threat to the global insurance industry over the next 2 to 3 years."[558] Insurer legacy systems are a significant barrier in obtaining a single view of the customer, identified by 55% of respondents in a 2019 survey conducted by Research in Insurance.[559]

Updating legacy systems is not straightforward, especially in the often risk adverse insurance industry. The costs and risks involved in digital transformation play an important factor in the decision-making process for insurance firms. Choosing to upgrade parts of the existing legacy

---

[552] "Customer Behavior and Loyalty in Insurance: Global Edition 2017", H. Naujoks et al, Bain & Company Report, September 14, 2017. Link

[553] "The Productivity Imperative In Insurance", McKinsey, August 2019. Link

[554] "Insurtech-The Threat That Inspires", McKinsey, March 2017. Link

[555] "Insurtech Market is Expected…", Globe Newswire. June 2022. Link

[556] "Speed to Market", Deloitte. Link

[557] "Insurtech-The Threat That Inspires", McKinsey, March 201. Link

[558] "Insurance Banana Skins" 2019, PWC, 2019. Link

[559] "Insurance 360: The Current State of Big Data-Driven Transformation In the Insurance Industry", Research in Insurance, June 2019. Link

© Strategy of Things, 2025. All rights reserved.

system brings short-term benefits but lacks the additional benefits of the end-to-end transformation, which is a more expensive and riskier endeavor.[560] Upgrading only parts of the legacy system puts off larger issues associated with aging technology such as security risks, high IT costs, talent retention and introducing technical debt.[561]

Many insurance carriers have implemented front-end tools with a visible impact for customers but neglected their back-office systems. Of the 200 largest insurers worldwide, less than 25% have truly digitalized the value chain and half are still exploring how to apply digitalization in their business model.[562] These efforts to update parts of their processes have left inefficient and expensive legacy IT systems and processes in place that require an overhaul to realize the digital transformation benefits.

Often companies treat system transformations as IT projects instead of overall business transformation opportunities.[563] Lacking an end-to-end transformation view creates expensive redundancies and data silos that must be managed so customer data and insights can be leveraged across the enterprise.[564]

When implementing digital transformation, companies need to consider the human factor of change management and the ability for workers to adapt and learn new digital skills and processes. This includes closing the gap between talent supply and demand in organizations.[565] Change management is required to build the buy-in required to transform a business, but only if the transformation efforts align with employee values.[566]

16.2. IoT in the insurance industry

The insurance industry has been undergoing a technology driven transformation in response to changing marketplace conditions and customer expectations. Although the insurance industry has historically been slow to innovate, the merger and deeper integration of insurance and digital technology from insuretech firms have spurred innovation. These innovations have led to more personalized insurance products, online customer engagement and transactions, reduced fraud and lower underwriting risks.[567] Many of these outcomes are made possible by IoT, data science, mobile technology and artificial intelligence (AI).[568]

IoT is expected to make a significant impact on the insurance industry and contribute to its ongoing transformation. IoT sensors collect data, some of which have never been collected and

---

[560] "The Legacy Dilemma – Can Insurers Upgrade to Digital Without Losing Their Legacy Investments?", Financier Worldwide. April 2016. Link

[561] "Insurance Technology's Ugly Legacy", Insurance Thought Leadership. December 2022. Link

[562] "A Wake-up Call for Insurers", Insurance Thought Leadership. December 2022. Link

[563] "IT Modernization in Insurance: Three Paths to Transformation", McKinsey. November 2019. Link

[564] "Legacy IT Systems, Inefficient Processes Hold Back the Insurance Industry", Business Wire. June 2019. Link

[565] "Digital Transformation is About Talent, Not Technology", Harvard Business Review. May 2020. Link

[566] "The Role of Culture in Digital Transformation", WSJ. July 2019. Link

[567] "Overview of Insurtech & its Impact on the Insurance Industry", Investopedia. June 2023. Link

[568] "Insurtech", NAIC, February 2023. Link

© Strategy of Things, 2025. All rights reserved.

analyzed to create actionable insights and capabilities that mitigate some of the industry challenges.

For example, insurers have historically relied on a few broad factors such as age, location and creditworthiness for calculating risk premiums to underwrite insurance.[569] A driver living and working in a metropolitan area would pay more for insurance than one living in the suburbs, even if both have identical driving behaviors.

Data collected from IoT devices offer more relevant information to underwrite a policy that is aligned to the actual risk and priced accordingly. IoT devices, such as onboard car sensors and wearables can collect data on an individual's health and fitness, as well as their actual driving behavior such as speeding, mileage and hard braking. Insurers use these data to assess an individual's personal risk profile, offer behavior-based discounts and adjust their premiums accordingly. This helps insurers do their work of underwriting and managing risks more accurately.

As insurance products become more commoditized, IoT helps insurers create new offerings that better manage risks by reducing the magnitude of losses and improving customer experiences. For example, leak detection sensors notify insurers and customers of a leaky pipe so that it can be addressed quickly before it becomes a major issue. This enables insurers to act proactively and accurately, which minimizes disruptions to the customer, reduces claims costs and enhances customer interactions and experiences. In areas impacted by natural disasters, drones can help survey and assess damages over large areas more efficiently and effectively leading to claims processing in hours.

Finally, IoT helps insurers avoid commoditization by creating and underwriting more personalized policies. The collected IoT data from fitness trackers can be used to underwrite a customer specific life insurance policy, with discounts offered as incentives for those who undertake activities to meet their health and fitness goals. These personalized products and the ensuing interactions and experiences, provide insurers with opportunities to engage with their customers in new ways, leading to enhanced brand reputation and loyalty in an industry facing commoditization of policies and products.

Despite the many possibilities and benefits of IoT in the insurance industry, the adoption of IoT is not without challenges. Insurers are risk-adverse and have large and established technology infrastructure that cannot be easily or inexpensively changed, unlike startups which are starting with more agile and modern architectures.

Another challenge for insurers is how to address customer information privacy concerns, especially as companies promote personalized policies based on health and driver behavior data. Customers may be hesitant to share this personal data and insurers have a responsibility to comply with relevant regulations and have robust security measures in place to protect their customer data. Additionally, insurance companies must have the technical ability and skilled staff to manage and analyze the collected data to derive actionable insights.

---

[569] "Digital Ecosystems for Insurers: Opportunities Through the Internet of Things", McKinsey, February 2019. Link

© Strategy of Things, 2025. All rights reserved.

Even with the current challenges, the insurance industry has an opportunity to adopt IoT to make improvements and better meet customer expectations. Forecasts of the IoT in insurance market expect a CAGR of 56.2% reaching $317.31 Billion by 2023.[570]

16.2.1. IoT use cases

Figure 16-1 below shows a representative set of insurance use cases organized into two categories. These categories are:

- **Property and Casualty.** IoT applications addresses the activities and risks related to the underwriting and claims management and administration of loss or damage of property.[571]
- **Life/Annuity.** IoT applications address the activities and risks related to the administration and support of life insurance and annuity products.[572]

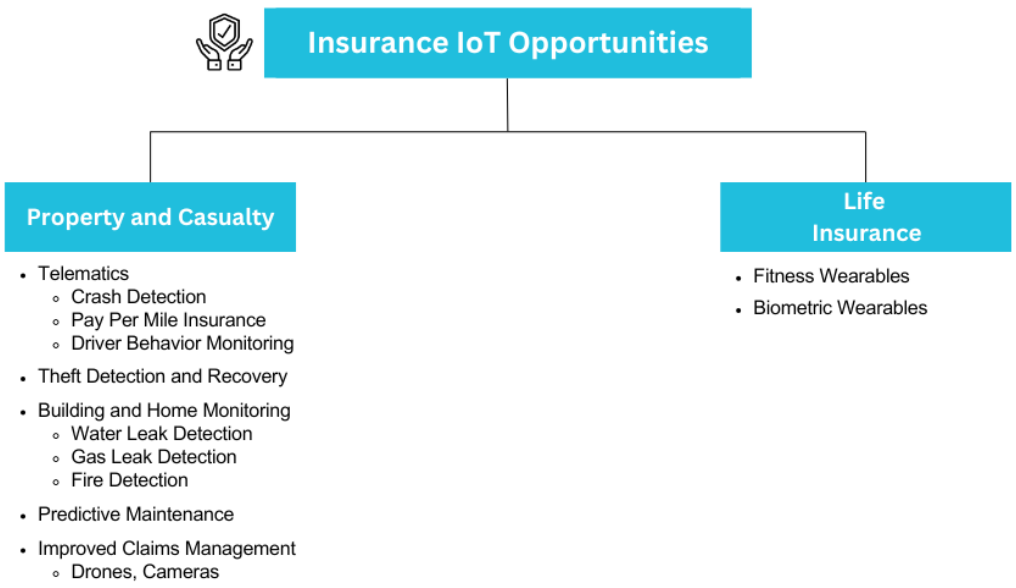


Figure 16-1: Insurance: Use Case Categories and Selected Use Cases

Data is crucial to the insurance industry. Data from a variety of sources provides information on the development of insurance products, understanding of risks and underwriting premiums. IoT provides insurers with another source of data that complements their existing data sets. IoT sensors and connected smart devices enable insurers to gather real-time data on previously

[570] "IoT Insurance Market to Grow USD 317.31 B…", GlobeNewswire, July 2022. Link

[571] This type of insurance has two major areas: protection of physical objects and protection against legal liability.

[572] Annuities are contracts that accumulate funds or pay out a fixed or variable income stream. They are commonly used to provide a guaranteed income in retirement that cannot be outlived.

© Strategy of Things, 2025. All rights reserved.

unmeasurable factors, leading to more accurate underwriting, proactive risk mitigation and personalized insurance products.

The use of IoT sensors in vehicles is an area of opportunity for insurers. While telematics is a long running use case that is commonly used in the transportation and logistics industry, its use in consumer vehicles allows insurers to offer innovative Usage Based Insurance (UBI) products with premiums based on actual driving habits rather than statistical assumptions. This incentivizes safer driving and allows insurers to create personalized insurance policies for individual risk profiles, ultimately reducing claims costs and improving profitability. Similarly, IoT asset trackers allow stolen vehicles to be quickly found and recovered. Crash sensors in vehicles detect serious accidents and can immediately notify first responders and emergency personnel. These new IoT capabilities enable new opportunities for insurers to create new value for their customers.

IoT changes the insurer-customer relationship. Insurers create monitoring services, using IoT devices, such as water leak detection systems or predictive maintenance applications on HVAC systems, to monitor building and facility infrastructure. Upon detection of a problem, the insurer works with the property owner to mitigate and address the problem. Early detection of problems, especially those that were not monitored before, helps avoid costly repairs by minimizing damage and disruptions from loss of use. Integrating IoT applications into the claims adjustment systems leads to proactive and timely processing of claims and allows customers to act quickly to repair the problems. The monitoring service creates a new and recurring means of engaging the customer on a regular and collaborative basis, leading to customer retention and greater loyalty while reducing claims losses.

16.2.1.1. Use case and industry challenges alignment

The insurance industry faces several challenges, some of which are described in Section 16.1.2. Figure 16-2 below shows the fit between the proposed use case subcategories and the documented industry challenges.

© Strategy of Things, 2025. All rights reserved.

Challenge	Role of IoT	Use case examples
Customer expectations	Enhance customer support and engagement, improve insurer proactiveness and responsiveness and increase loyalty and customer retention.	• Auto accident detection and automatic kickoff of claims process • AI-based camera systems and drones to determine accident and disaster damages to property
Underwriting risks	Enable insurers to assess risks, create risk-tailored products and improve pricing decisions.	• Telematics and driver behavior monitoring • Theft detection and recovery • Remote equipment monitoring and notification
Commoditization	Facilitates insurer innovation and development of differentiated insurance offerings and responsive services.	• Mileage and usage-based auto insurance • Remote equipment monitoring and notification • Predictive monitoring of home and business equipment • Health monitoring and wearables (life insurance)
Legacy infrastructure	Extend usefulness of legacy systems by adding real-time data and insights to complement existing static data on policyholders.	• Vehicle telematics for individual driver behavior determination • Wearables for health monitoring for life insurance

Figure 16-2: Insurance: Use Case and Industry Challenges Alignment

16.2.1.2. IoT use case details

Figure 16-3 below provides details on each of the use case subcategories shown in Figure 16-1.

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Description
Property & Casualty	Telematics	Monitor driving behavior, such as speed, braking and location. These data are used to provide customized auto insurance policies based on the driver's behavior.
	Theft detection and recovery	Track and monitor asset movements and location, which can be used to assist recovery from theft, misplacement and other losses.
	Building & Home monitoring	Monitor equipment and infrastructure to detect problems early to prevent or minimize loss and loss of use through early warnings and notification of relevant support teams.
	Predictive maintenance	Sensor data on equipment providing data to predict when equipment, infrastructure and assets will need maintenance before failure. Prevent unplanned breakdowns, safety issues and reduce loss of use by proactively scheduling maintenance based on actual conditions.
	Improved claims management	Sensors and cameras monitor and determine the extent of damages which is used to quickly determine and accurately process claims in a timely manner.
Life Insurance	Fitness and Biometric wearables	Monitor activities and health to encourage healthy lifestyle choices and reduce injuries and deaths, better understand the risks associated with a policyholder, provide personalized life insurance policies,

Figure 16-3: Insurance: Use Case Categories Details

© Strategy of Things, 2025. All rights reserved.

16.2.2. Market views of IoT in insurance

To understand market views on IoT and to inform on our gaps discovery and analysis, our research team conducted a survey of 450 people, from adopters to solution providers, across the nine industries studied. The survey respondents were asked their opinion on the importance of IoT for the insurance industry over the next 5 to 10 years. Figure 16-4 below shows a medium expected relative importance of IoT in the insurance industry, as compared to other industries. Some of this may be attributed to a lack of visible IoT-enabled products in the marketplace, as well as privacy and data collection concerns that have hindered adoption.

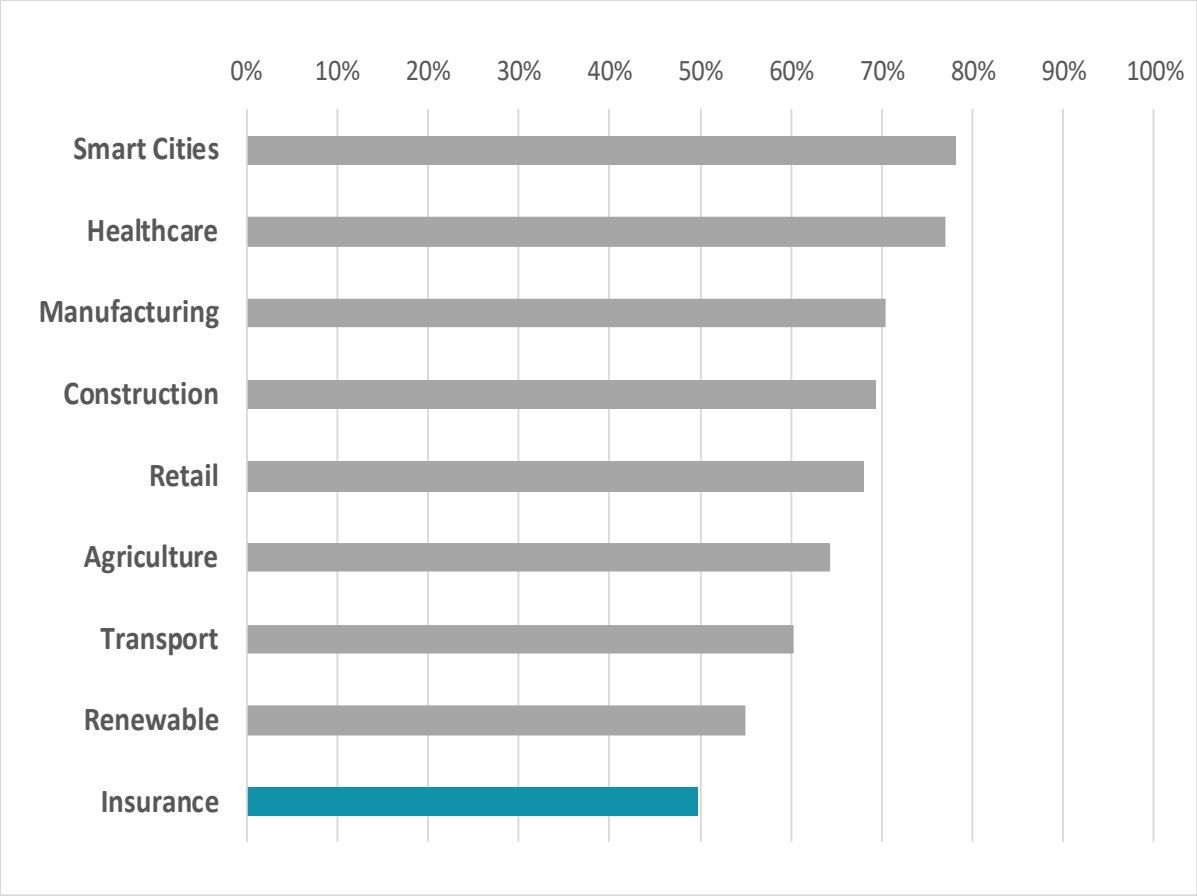


Figure 16-4: Insurance: Importance of IoT

Survey respondents were asked to rate the impact of these use case categories on the insurance industry.[573] Figure 16-5 below shows the percentage of responses in each impact category for each use case category. Overall, this shows a bias to a moderate to high impact of the use case categories in insurance.

[573] In your view, what will be the impact of these use cases in insurance over the next 5-10 years?

© Strategy of Things, 2025. All rights reserved.

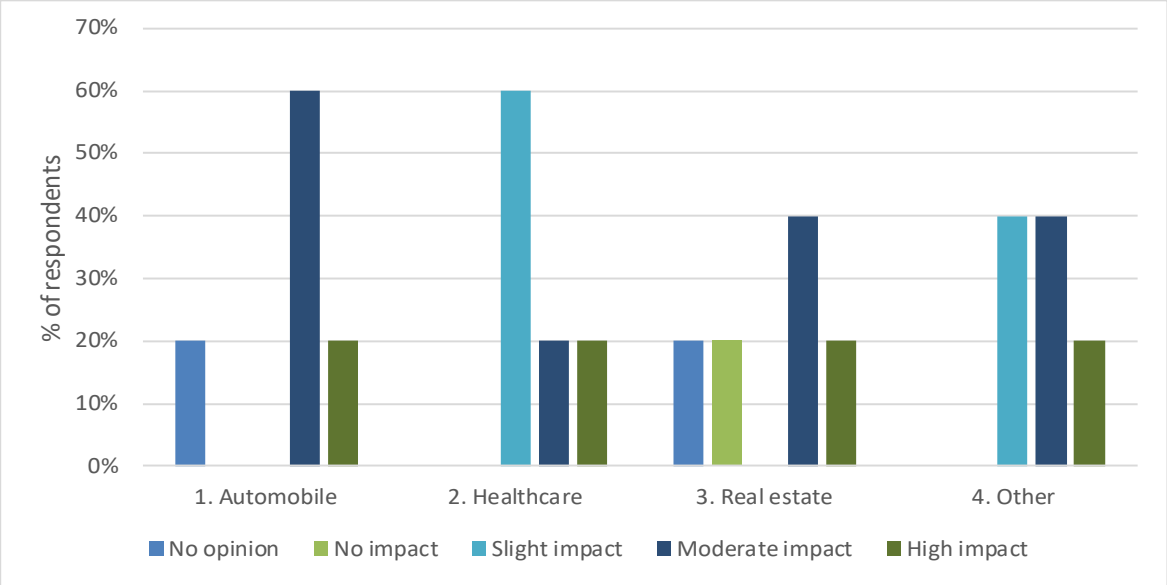
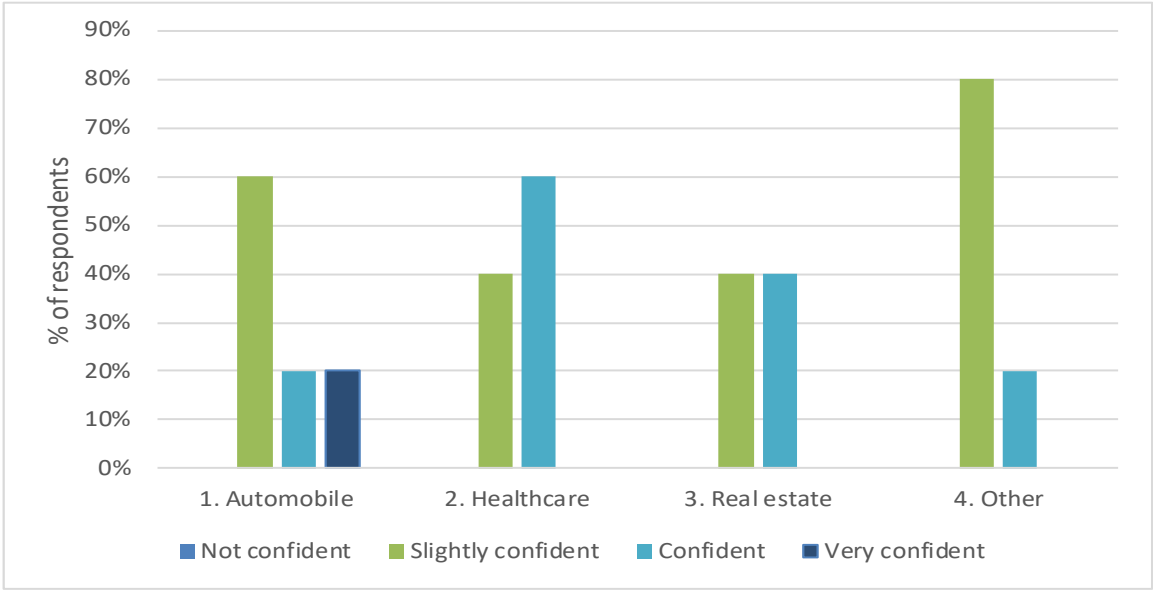


Figure 16-5: Insurance: Use Case Category Impact

In addition, respondents were asked about their confidence in suppliers delivering the services required to operationalize these use case categories.[574] Figure 16-6 below shows the percentage of responses in each confidence category for each use case category. Overall, their responses indicate modest confidence in the ability of suppliers to deliver the necessary services.



[574] How confident are you that suppliers will deliver the services that insurance organizations need from these technologies over the next 5-10 years?

© Strategy of Things, 2025. All rights reserved.

Figure 16-6: Insurance: Confidence in Suppliers Delivering

16.3. IoT gaps and findings in insurance

A combination of interviews, secondary research and surveys was conducted to identify and understand the opportunities and challenges to the development and adoption of IoT. Each research method approached the challenges from a different perspective.

- The survey targeted a large audience but asked specific questions that supported the economic analysis.
- The interviews targeted a small number of people who provided deeper insight and context to supplement the initial information collected.
- The desk research, consisting of a review of online news articles, published research reports, vendor and government white papers, blogs, webinars, videos and other content, provided a broad overview of the application of IoT in the industry.

In the survey, respondents were asked to choose the most important technology areas to operationalize IoT in their industry. Figure 16-7 below shows respondent's selections of the top 10 IoT technologies and the percentage of respondents who chose that technology.[575] The survey results are not seen as a technology gaps list, but rather an indication of what is important to the respondents. This information partially informs the gap selection process.

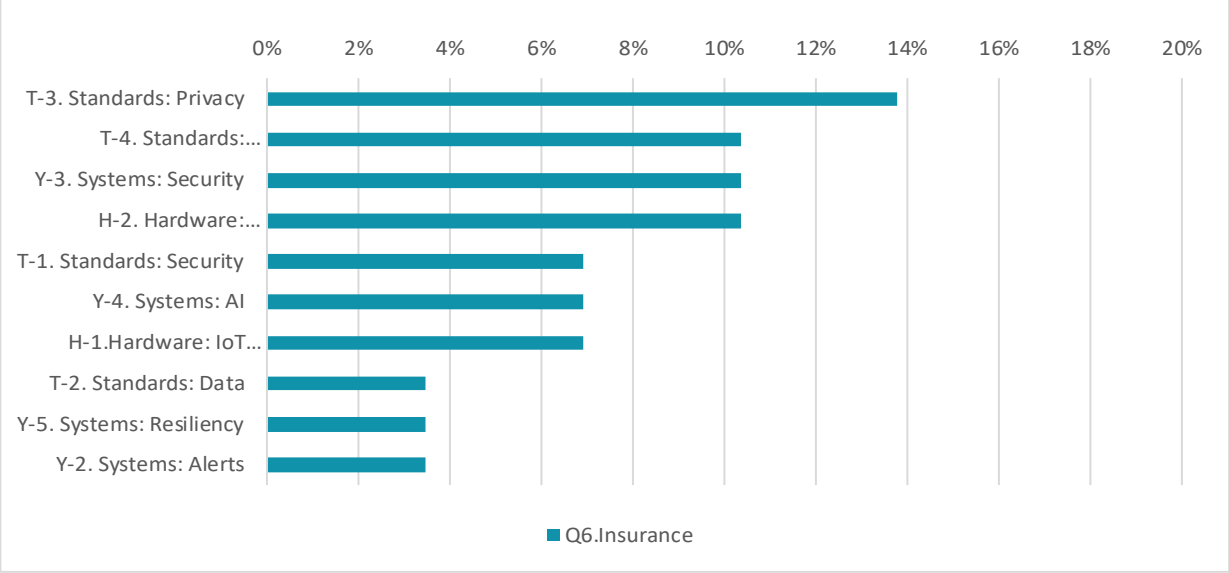


Figure 16-7: Insurance: Top 10 Most Important Single Technologies

16.3.1. Top technology challenges

Using this approach three challenges were selected for further consideration. These are:

[575] Respondents were asked to choose up to 5 out of the 25 technologies listed.

© Strategy of Things, 2025. All rights reserved.

- AI model accuracy and explainability
- Data privacy
- IoT cybersecurity

Each of these is discussed below.

16.3.1.1. Challenge # 1: AI model accuracy and explainability

One of the major gaps in insurance is the ability of AI algorithms and machine learning models used to analyze IoT data to explain outcomes. In a 2019 survey conducted by LexisNexis Risk Solutions of 300 insurance carrier professionals, 62% of respondents are "applying, piloting or planning AI and ML initiatives." Among these AI/ML adopters, "86% agree it's important to explain to consumers and regulators how AI and ML are used. In addition, 55% are concerned about trust in how analytical models are used, with 26% ranking it as one of their top three concerns. Nearly three quarters (71%) of adopters are concerned about bias in AI and ML models."[576]

> *...if the model becomes too complex, which loses the explainability, that is a big barrier.*
>
> *Jerry Gupta, SVP, Swiss Re*[577]

IoT sensors and devices collect large volumes of data that may be combined with other data stored in legacy systems. Machine learning and AI algorithms analyze these data to predict outcomes, determine risks in underwriting policies and create new insurance products. For example, traditional automotive insurance policies are partially based on proxy indicators such as location, credit-based insurance score, age, gender and type of car.[578] However, these indicators do not reflect the true risk rating of drivers and financially penalize careful drivers living in an urban setting.

While the potential value of using IoT data to fine tune models is high, several factors reduce the value of the data and the analytics algorithms that create explainable outcomes. Some applications, especially those that utilize multiple data parameters, require the collection of large volumes of data over a long period of time before sufficiently accurate assessments can be made.

> *Getting enough information so insurers can actually make sound risk decisions is essentially the biggest challenge. For the insurance company to get enough performance data or loss information from a specific device, especially a wide range of devices, it takes a long time—it takes years.*

---

[576] "Hype or Reality? The State of Artificial Intelligence and Machine Learning in the Insurance Industry", LexisNexis Risk Solutions white paper, December 2019. Link

[577] "AI for Impact: Delivering value in the near term", InsurTech Bytes podcast #17, June 27, 2018. Link

[578] "What Determines the Price of An Auto Insurance Policy?", Insurance Information Institute. Link

© Strategy of Things, 2025. All rights reserved.

> *John Beal, Senior Vice President of Analytics and Modeling, Insurance, LexisNexis Risk Solutions*[579]

> *IoT will level the playing field, or at least make it much more fair. The complication is you need large datasets in order to provide actuarilly sound measurements and risk assessment of this. You have to have robust datasets so you are able to control for the other variables that might actually be out there. You have to have a historical data set to provide the type of modeling that justifies your point of view. Ryan Briggs, Vice President, Automotive and Mobility Solutions, Swiss Re*[580]

Another barrier to model explainability is the differences in the data coming from "similar" sensors or different sensors used in similar ways. For example, automotive telematics data can be collected from sensors built-in to the vehicle, aftermarket "plug-in" IoT devices and from an app on a mobile phone tapping into the phone's sensors.

Plug-in devices may not be secured properly in the vehicle's 12V socket and may not always collect data. Data from sensors on mobile phones is problematic as different brands have differences in how they work and record data. In addition, mobile phones can be placed in different locations in a vehicle each time, which affects the calibration/orientation sensors.[581]

When mobile phone sensor data are aggregated with plug-in sensor data, these differences must be accounted for so the algorithms can produce sound outcomes.

> *For vehicle telemetry, the sensors in a cell phone, an aftermarket device and a vehicle all behave differently… a small vehicle and a very large vehicle have different behavioral components. Sometimes it's by choice because the manufacturer of each of those devices builds them differently. They've got different standards. There's actual component level differences. And then there's differences based on what the manufacturer chooses to make available. Harmonizing data from different sets is a huge challenge for the industry. Ryan Briggs, Vice President, Automotive and Mobility Solutions, Swiss Re*[582]

> *The plethora of IoT devices, such as sensors in homes and black boxes aboard vehicles, also means that carriers may receive data in many different formats. To make meaningful decisions with that data, carriers need the expertise and technology to synthesize it to make it compatible and appropriate for their needs. It takes a lot of time and devices to bring data together, normalize it and align it so the signals from all the different devices mean the same thing. On the auto*

---

[579] "Number Crunch: Data Challenges Stemming IoT in Insurance", W. Jones, Independent Agent, May 22, 2018. Link

[580] Research interview, October 5, 2022

[581] "What is Telematics? and is A Box Better Than an App?", S. Olsson, Redtail Telematics blog, September 15, 2021. Link

[582] Research interview, October 5, 2022

© Strategy of Things, 2025. All rights reserved.

> *side, we get signals from black boxes and mobile devices. Depending on the model of the device, you can get a different signal pattern. A lot of work has to be done to normalize those signals.*
>
> *John Beal, Senior Vice President of Analytics and Modeling, Insurance, LexisNexis Risk Solutions*[583]

Another barrier is the expertise to develop explainable AI algorithms and techniques to analyze large volumes of datasets that highlight relationships, identify patterns and infer correlations and outcomes.

A study of 77 insurance companies by Accenture found that 78% are AI experimenters who "lack mature AI strategies and capabilities to operationalize."[584] A LexisNexis Risk Solutions survey found that 40% of AI/ML adopters lack the right analytical skills, while 45% lack the right number of people to apply new AI and ML techniques.[585]

A 2018 LexisNexis survey of 500 insurance professionals reported that "while 70 percent of respondents agree that gathering IoT data is important to their organization's current insurance strategy, only 21 percent have an IoT strategy and just 7 percent have the human and technology resources required to use it in decision making. Of those that said they currently collect data from telematics, wearables, connected home and properties, just 5 percent use it in their day-to-day analytics."[586]

A 2021 research paper published in the Journal of Insurance Regulation suggested that "artificial intelligence (AI)-enabled systems increase the risk of proxy discrimination" and "raise unique ethical implications, particularly regarding accountability among AI actors. Many insurers rely on unregulated third-party algorithm developers and may not have access to the logic embedded in the system."[587]

> *... data exchanges haven't been really very successful. They haven't been able to offer much more than maybe 20, 30, 40% insight into the market. Ryan Briggs, Vice President, Automotive and Mobility Solutions, Swiss Re*[588]
>
> *Capturing and utilizing that information is going to rely on looking at patterns to learn from the information coming in and utilizing techniques like artificial*

---

[583] "Number Crunch: Data Challenges Stemming IoT in Insurance", W. Jones, Independent Agent, May 22, 2018. Link

[584] "How insurers Can Win the Race to AI Maturity", E. Sandquist, Accenture, December 5, 2022. Link

[585] See note 576

[586] "New Study Reveals Most U.S. Insurance Carriers Are Unprepared to Leverage IoT Data for Strategic Business Needs", LexisNexis press release, March 20, 2018. Link

[587] "AI-Enabled Underwriting Brings New Challenges for Life Insurance: Policy and Regulatory Considerations", A. Filabi and S. Duffy, Journal of Insurance Regulation, Vol 40, No. 8, 2021. Link

[588] Research interview, October 5, 2022

© Strategy of Things, 2025. All rights reserved.

intelligence and machine learning. This is information that nobody has seen before. Understanding the importance of data, given the huge volume and variety, is going to require much more sophisticated algorithms.

David Bassi, executive director, EY[589]

16.3.1.2. Challenge # 2: Data Privacy

IoT used in insurance products collects a large amount of data. These devices may be placed in homes, vehicles, buildings, workplaces and on people. For example, moisture sensors placed underneath laundry machines in a home to detect leaks or vehicle sensors collecting data on a driver's true risk rating. When IoT data are used for its intended purposes, it provides value to both the insured and the insurer.

Data privacy concerns, however, may slow IoT innovation and adoption in the insurance industry. In a KPMG survey of 2,000 U.S. adults in 2021, 86% reported that data privacy was a concern, 68% were concerned with the level of data collected by businesses, 40% did not trust companies to use their data ethically, while 30% were not willing to share any personal information.[590]

A 2021 survey of 1,001 U.S. adults, conducted by insurance comparison site Zebra, reported that 45% of drivers between the ages of 18 and 24 were not comfortable with sharing their driving data. Other age groups reported similar sentiments, but at slightly lower levels (31% to 40%).[591]

A survey conducted by the Deloitte Center for Financial Services of 2,193 respondents, representing a wide demographic range, reported that 47% "would not be interested in having their driving monitored under any circumstances."[592]

Insurance regulators, often sensitive to data privacy considerations, have imposed limits on what data can be used. For example, regulators in California only allow mileage data to be considered for ratings.[593]

The California Consumer Protection Act (CCPA) requires companies operating in California to provide consumers with transparency and control of their personal data. Other states, such as Colorado, Hawaii, Louisiana, Illinois, Maine, Nevada, North Dakota, Texas and Virginia also recently enacted data privacy laws.[594]

---

[589] "Number Crunch: Data Challenges Stemming IoT in Insurance", W. Jones, Independent Agent, May 22, 201. Link

[590] "Corporate Data Responsibility: Bridging the Consumer Trust Gap", KPMG, August 2021. Link

[591] "Gen Z Doesn't Want to Share Data With Auto Insurance Companies, But Millennials do", Zebra blog. Link

[592] "Opting in: Using IoT connectivity to drive differentiation. The Internet of Things in insurance", M. Cannon et al, Deloitte Center for Financial Services report, Figure 5. Link

[593] Research interview, Ryan Briggs, VP, Swiss Re, October 12, 2023

[594] "Data Use, Privacy and Technology", National Association of Insurance Commissioners, February 22, 2022. Link

© Strategy of Things, 2025. All rights reserved.

Privacy by Design (PbD) is an approach to systems engineering that calls for privacy to be considered throughout the engineering process. It is based on the following foundations:[595]

- Proactive not reactive; preventive not remedial
- Privacy as the default setting
- Privacy embedded into design
- Full functionality
- End-to-end security with full lifecycle protection
- Visibility and transparency
- Respect for user privacy

Embedding privacy requirements and measures into the design and architecture of the IoT product or system instead of "bolting" it on afterwards is an important factor for the development of "privacy-compliant" products. For example, Willis Towers Watson is piloting the use of a "data trust" built on privacy-by-design principles and is a "legal and technological construct that enables the compliant, ethical and secure sharing of sensitive data among a network of data providers."[596]

IoT devices, however, operate in complex environments with other IoT devices as well as other IT and OT systems. For example, an assisted living smart home will contain many IoT devices of various functions. Smart roads embedded with sensors may communicate and exchange information with vehicle telematics devices. WiFi access points and cellular towers can monitor large quantities IoT devices to determine their locations and timestamps. Further research and development is required in understanding how privacy can be embedded into the underlying infrastructure and systems to create "Privacy by Design" infrastructures and systems at scale.

16.3.1.3. Challenge # 3: IoT cybersecurity

One gap, repeated during the data collection and research process, is IoT security. IoT devices represent new attack surfaces and introduce additional vulnerabilities into the connected networks.

For example, IoT devices connected to home and business networks introduce entry points that allow hackers and cyber criminals to move laterally into the main network.[597] Telematics devices can be breached to allow hackers to send commands through the connected car's internal network.[598] There were 150 automotive cybersecurity incidents reported in 2019.[599] Other

---

[595] "Privacy by Design: The 7 foundational principles", A, Cavoukian. January 2011. Link

[596] "Data sharing models in the insurance industry," C. Holland, G. Zarkadakis, J. Hillier, P. Timms and L. Stanbrough, WTW, February 22, 2021. Link

[597] "Unsecured IoT devices give hackers a backdoor into your network – get protected now," E. Newton, IoT For All, January 12, 2023. Link

598 "Hack of Telematics Device Lets Attackers Mess With Car's Brakes", J. Gitlin, Ars Technica, August 11, 2015. Link

[599] "Car Hacking Danger is Likely Closer Than You Think", S. Blanco, Car and Driver, September 4, 2021. Link

© Strategy of Things, 2025. All rights reserved.

impacts of an IoT breach include failure of the device to perform its intended functions and result in financial losses, loss of personal or critical business data, human injury or death and loss of products.

> *Data fraud and security are two of the most pressing concerns when it comes to adopting IoT. The data that flows between the connected home, connected car and the IoT devices employed by the insurance company is vulnerable to phishing attacks. With this in mind, many customers are reluctant to allow insurance companies to continuously access personal information and data through IoT networks, especially if the proposed benefits from adopting IoT are not consumer focused.*[600]

Insurance carriers are attractive targets for cybercriminals. The carriers collect and use data, including personally identifiable information (PII), to assess risks, create new products and price premiums. They also use data to process claims, detect and fight fraud, enhance customer interactions and experiences. The data they use come from a variety of sources including online forms submitted by customers, anonymized data purchased from brokers and exchanges and most recently, from IoT devices located on customer facilities or worn on their person. The same IoT vulnerabilities that allow hackers to access business networks can now be exploited to enter the insurance company's network.

Despite the significance and value of the data they hold, a study of the top 99 insurance companies found that these carriers are vulnerable to cyber-attacks. Specifically, half of the largest carriers are three times more likely to experience a cyber breach than those with their better prepared counterparts, 18% have a high level of susceptibility to ransomware and 82% are susceptible to a phishing attack.[601]

> *Insurance companies are known to store large amounts of information about their policyholders. This practice makes them a target for cybercriminals. It is expected that attacks against the insurance industry will continue to grow in frequency and severity.*[602]

From telematics devices used in vehicles, to in-home sensors and human health monitors, IoT is increasingly used in new insurance products. Securing those IoT devices, however, is challenging. IoT security brings complex and multi-dimensional challenges. While device security is one challenge, other elements need to be secured as well, including the cloud, mobile applications, network interfaces, software, encryption, user and device authentication and physical security.[603]

---

[600] "IoT in Insurance: Opportunities and Challenges", Value Momentum, February 8, 2022. Link

[601] "A Fight for Coverage: Cyber Insurance Risk In 2022", Black Kite report, 2022. Link

[602] "Cybersecurity In the Insurance Industry", S. Bowcut, Cybersecurity Guide, November 10, 2022. Link

[603] "Security Issues in IoT: Challenges and Countermeasures", G. Polat and F. Sodah, 2019 Volume 1, ISACA Journal. Link

© Strategy of Things, 2025. All rights reserved.

> *Networks of connected devices will be vulnerable to cyber-attacks. Heavy investment in cybersecurity will be required before a greater shift to using more IoT.*[604]

While the cybersecurity challenges presented by IoT devices used in the insurance industry are like those in other industries, breaches of insurance IoT devices create a loss of trust by existing and future policyholders.

Recent research by Fintech OS identified privacy breaches as one of the six causes of mistrust in insurance.[605] The insurance industry is built on both trust and loyalty. Policyholders "trust" that the insurance company will readily pay the indemnity if the casualty occurs and the insurance company "trusts" that the policyholder will not claim an indemnity when it is not due. The insurance industry is unique in that "it is the largest subscription-based business in the world where once a year every customer has to decide whether to renew or not"[606] requiring significant customer loyalty.

In an industry that is commoditizing and where insuretech companies are out innovating the larger carriers, any loss of trust results in a loss of loyalty and customers.

Cyberattacks have financial consequences. A 2023 Cybersecurity Risk analysis reported that the financial and insurance industry has an average loss exposure (probable likelihood and probable financial impact) of $2.1 Million per attack scenario. These scenarios include insider misuse, web application attack, system intrusion, insider error, ransomware, social engineering and denial of service attack.[607]

16.3.2. Other challenges

In addition to the technology challenges, our research has identified other challenges that impact IoT adoption. These challenges did not meet the criteria for research consideration because they were either not a technology challenge or a technology related challenge that can be addressed by current marketplace offerings or capabilities.

These are:

- Uncertain regulatory treatment
- Digital skills gap

[604] "How the Internet of Things is Affecting the Commercial Insurance Industry", Embroker blog, September 2, 2022. Link

[605] "Insurance: the root causes of low trust", Fintech OS Blog, July 30, 2020. Link

[606] "The Key to Building Trust In the Insurance Industry", G. Osborne, Insurance Innovation Reporter, May 17, 2021. Link

[607] "2023 Cybersecurity Risk Report," RiskLens, 2023. Link

© Strategy of Things, 2025. All rights reserved.

16.3.2.1. Uncertain regulatory treatment for IoT

The insurance industry operates in a regulated environment designed to protect the insured, insurers and investors. IoT and some of its adjacent technologies such as AI, are disruptive technologies that insurance regulators are trying to understand and operationalize.

Traditionally, innovation in regulated environments outpaces the ability of regulators to keep up with developments. This "regulatory drag" has resulted in issues for the industry when regulators eventually catch up, understand the implications and impose remedies.

A 2019 LexisNexis survey reported that AI/ML adopters in the insurance industry were concerned that increased regulatory scrutiny, combined with lack of understanding, could hamper their initiatives. Specifically, 74% of the AI/ML adopters were concerned about "increased compliance scrutiny as more data sets are accessed and modeled", 65% were concerned that "Regulators could block applications they don't understand" and 59% were concerned that "Regulators could limit approaches because they don't understand."[608]

> *Regulators are in the mode where they're trying to educate themselves. They are trying to learn what's out there from a technology perspective. And what issues are these technologies addressing? There's so much data out there that insurance companies are monitoring. The regulators are trying to figure out what is beneficial? What is not and what is intrusive? They're trying to really grow their knowledge base right now so they can educate themselves and get up to a point where they can decide, 'Is this something that they need to regulate? Or is this something that they need to get involved with from an insurance product perspective? Kavita Ramcharan, Vice President of Inspection Operations and Client Services, HSB Canada*[609]

While IoT creates opportunities for significant value generation and business model transformation, it also creates potential situations that may not meet existing regulatory frameworks. This may result in regulatory actions, legislation and limited IoT adoption.

For example, the data collected from IoT devices helps insurers better identify, assess and price risks, reduce fraud and losses and create new personalized insurance products. At the same time, the collection of vast amounts of data from IoT devices allows insurers to continually understand, differentiate and price risk pools to ever smaller segments.

This may lead to "uninsurables", or individuals and businesses who are not able to obtain or afford insurance because of their risk rating.[610] This limit to insurance availability may result in regulations that preserve equity, but in doing so, may create barriers that unintentionally slow or limit innovation. Furthermore, there is not always a consistent treatment in addressing these issues, as insurance is regulated at the state level.[611]

---

[608] See Note 576

[609] Research interview, October 12, 2022

[610] "Insurtech: Where are we now?", Norton Rose Fulbright, February 2017. Link

[611] "Commercial Insurance: Regulation", Insurance Information Institute. Link

© Strategy of Things, 2025. All rights reserved.

There are some differences by state and what telematics data is permitted to be shared for which use case. California, for example, won't allow anything other than mileage. It will not allow risk based factors for vehicle rating, where other states will do that. So when you get into the differentiation of the insurance industry on how IoT can be applied, that's a much longer discussion. Much, much longer. Ryan Briggs, Vice President, Automotive and Mobility Solutions, Swiss Re[612]

16.3.2.2. Digital skills gap

Digital innovation is transforming the insurance industry. A shortage of digital skills and talent, however, is slowing the ability of the insurance companies to innovate and deliver new products and experiences, execute and operate new business models and to re-engineer existing processes and digitize operations.

Several factors contributed to this shortfall. The insurance workforce is aging and approaching retirement, while younger workers are less inclined to enter the industry. The U.S. Bureau of Labor Statistics (BLS) estimates that the number of insurance workers ages 55 and up has increased 74% in the last ten years.

Moreover, the BLS estimates that 50% of the current workforce will retire, leaving more than 400,000 open positions unfilled. At the same time, workers aged 35 or younger only represent 25% of the industry workforce.[613]

A Valen Analytics research reported that 44% of millennials do not find a career in insurance interesting.[614] A survey of underwriting leaders found that 64% stated that their teams are understaffed while 56% said that more than 20% of their job openings have remained unfilled for three or more months.[615]

A second contributing factor for the shortfall is the need for a new set of skills in the digitally transforming industry. Automation of formerly manual tasks and activities will drive the need for technological skills and will increase 55% from 2016 to 2030.[616] A survey of 23 global insurance companies with revenues of more than $1 billion identified the largest digital skills gaps as big data analytics, cloud-based IT infrastructure, cognitive and AI, cybersecurity and Internet of Things.[617]

The insurance industry is embarking on various initiatives to address the talent shortage. According to the 2021 Mercer Global Talent Trends Study research, 81% of insurers surveyed

---

[612] Research interview, October 5, 2022

[613] "The America Works Report: Industry Perspectives", U.S. Chamber of Commerce, June 1, 2021. Link

[614] "Insurance Industry Talent Crisis", AmTrust Financial blog. Link

[615] "The Insurance Industry Talent and Technology Tug-Of-War", J. Stammen, PropertyCasualty360, February 2, 2023. Link

[616] "Transforming the Talent Model In the Insurance Industry", T. Catlin et al, McKinsey and Company, July 6, 2020. Link

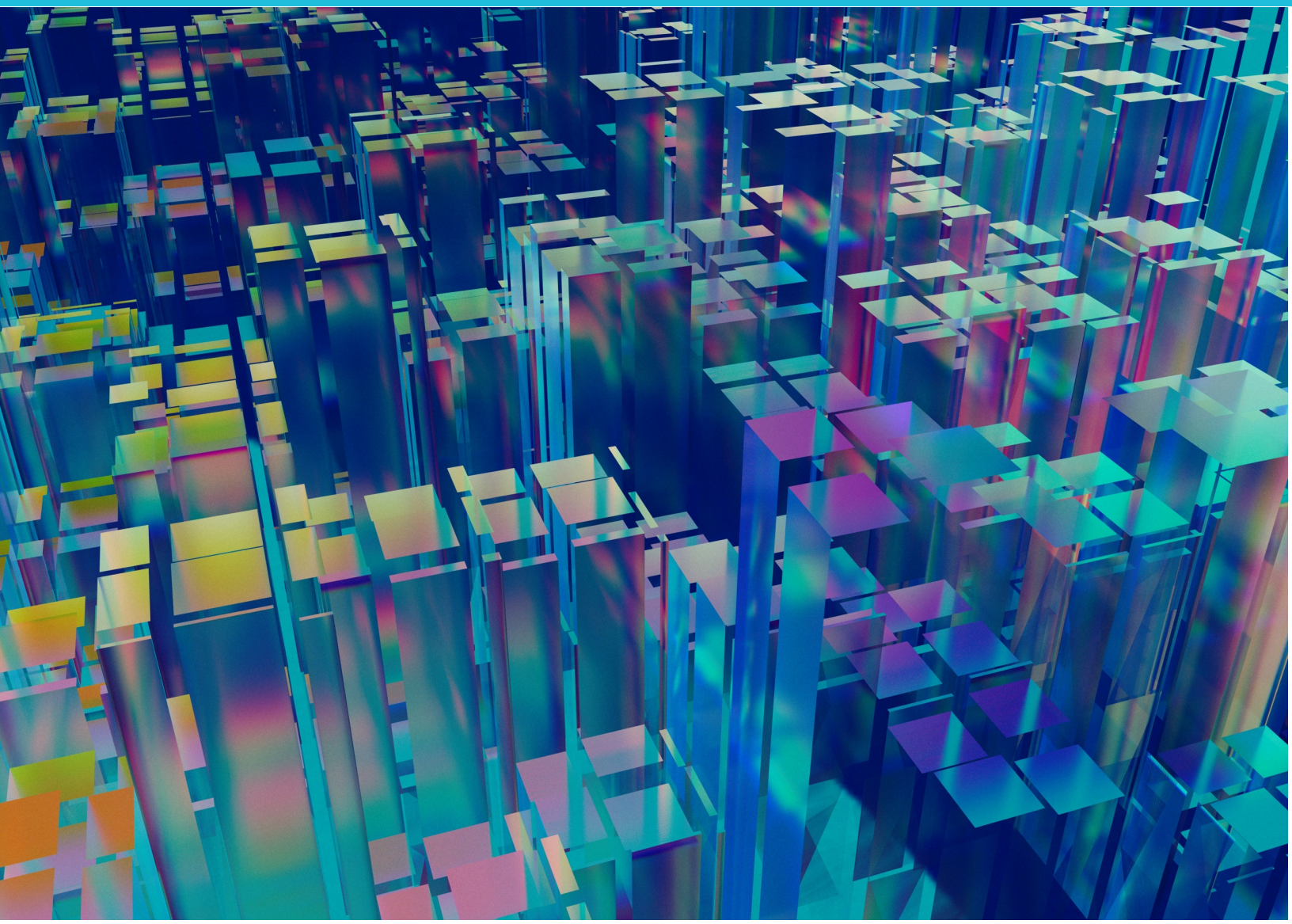
[617] "How Insurers Can Close Their Digital Skills Gap | Sherpas In Blue shirts", Everest Group blog, R. Doshi and P. Dave, July 2, 2018. Link

© Strategy of Things, 2025. All rights reserved.

are implementing or have implemented plans to loan or share talent internally, 63% have increased or plan to increase the use of variable/contingent talent pools and 60% have intensified or plan to intensify the development of remote working skills.[618]

[618] "2021 Global Talent Trends - Insurance Industry Outlook", Rl Baker, Mercer Consulting. Link

© Strategy of Things, 2025. All rights reserved.



Appendix: Cities

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

© Strategy of Things, 2025. All rights reserved.

17. Appendix: Cities

This section describes the research findings for IoT technology infrastructure in U.S. smart cities. The topics discussed here include:

- Industry overview
- Use of IoT in cities and municipalities
- IoT challenges in cities and municipalities

17.1. Industry overview

As of January 1, 2022, the population of the United States stood at 332,403,650, an increase of 706,899 (0.21%) from January 1, 2021.[619] There are an estimated 286.5 million people living in one of 384 designated metropolitan statistical areas (MSA) in the United States as of July 1, 2021,[620] representing 86.2% of the total American population.

The top ten metropolitan areas in the United States are home to 87 million people. This is 30.4% of the 286.5 million people living in the 384 MSAs and 26% of the total U.S. population.[621] The top ten metropolitan areas are:

1.	New York-Newark-Jersey City, NY-NJ-PA-	19,768,458
2.	Los Angeles-Long Beach-Anaheim, CA -	12,997,353
3.	Chicago-Naperville-Elgin, IL-IN-WI	9,509,934
4.	Dallas-Fort Worth-Arlington, TX	7,759,615
5.	Houston-The Woodlands-Sugar Land, TX	7,206,841
6.	Washington-Arlington-Alexandria, DC-VA-MD-WV -	6,356,434
7.	Philadelphia-Camden-Wilmington, PA-NJ-DE-MD	6,228,601
8.	Atlanta-Sandy Springs-Alpharetta, GA	6,144,050
9.	Miami-Fort Lauderdale-Pompano Beach, FL	6,091,747
10.	Phoenix-Mesa-Chandler, AZ	4,946,145

17.1.1. Key facts

The following key facts outline the population structure of U.S. cities.

- There are 19,495 cities, towns or other incorporated places in the United States[622] and the majority of these are small.

[619] "U.S. Population Estimated at 332,403,650 on Jan. 1, 2022", Derek Moore, Dec 30, 2021, U.S. Census Bureau. Link

[620] Metropolitan and Micropolitan Statistical Area Population by Characteristics: 2020-2021, U.S. Census Bureau. Link

[621] ibid.

[622] "Population and Housing Unit Estimates Tables, 2021", July 1, 2021, U.S. Census Bureau. Link

© Strategy of Things, 2025. All rights reserved.

- There are 14,685 cities (75.3%) that have a population of less than 5,000 people. The combined population of these 14,685 small towns comprise 16,302,959 people or just 4.9% of the U.S. population.[623]
- A significant portion of the city population lives in a small number of large cities. There are 328 cities that have a population of 100,000 or more, housing a combined population of 96,558,086 or 29% of the U.S. population.
- There are 38 large cities with a population of 500,000 or more. These 38 cities are home to 44,277,046 people, or 13.3% of the U.S. population.
- The United States has 10 cities with a population of over a million. These ten cities are home to 24,624,356 people, making up 7.4% of the total American population.[624]

Despite occupying 2.7% of the country's land mass[625], American cities are economic engines. For example, the economies of the metropolitan areas accounted for 91.1% of the national GDP, 91.8% of all wage income and 88.1% of the jobs in 2018.[626] In 2020, the top ten U.S. metropolitan areas accounted for 37.3% of the total GDP of $18.8 trillion produced in the 384 U.S. metropolitan statistical areas. These top ten metropolitan areas include[627]:

1.	New York-Newark-Jersey City (NY-NJ-PA) -	$1,809 billion
2.	Los Angeles-Long Beach-Anaheim (CA) -	$1,007 billion
3.	Chicago-Naperville-Elgin (IL-IN-WI) -	$ 693 billion
4.	San Francisco-Oakland-Berkeley (CA) -	$ 588 billion
5.	Washington-Arlington-Alexandria (DC-VA-MD-WV) -	$ 561 billion
6.	Dallas-Ft Worth-Arllington (TX) -	$ 535 billion
7.	Houston-The Woodlands-Sugar Land (TX) -	$ 488 billion
8.	Boston-Cambridge-Newton (MA-NH) -	$ 480 billion
9.	Philadelphia-Camden-Wilmington (PA-NJ-DE-MD) -	$ 439 billion
10.	Seattle-Tacoma-Bellevue (WA) -	$ 427 billion

Cities generate income from several sources, including user charges and property taxes as well as property sales, net lottery earnings, sales taxes, individual and corporate income taxes, license fees, federal government and local sources.[628]

Across all U.S. cities, the top five income sources representing 81% of all income, are user fees (29.2%), property taxes (18.3%), other/miscellaneous (13.9%), state (13.1%) and general sales

[623] ibid, as of July 1, 2021

[624] ibid, as of July 1, 2021

[625] "Land Use and Land Cover Estimates for the United States", Economic Research Service, USDA, April 27, 2022. Link

[626] "U.S. Cities Factsheet", University of Michigan Center for Sustainable Systems. Link

[627] "CAGDP1 Gross Domestic Product (GDP) Summary By County And Metropolitan Area", Bureau of Economic Analysis, December 21, 2021. Link

[628] "Local Government Revenue Sources – Cities", Government Finance Officers Association. Link

© Strategy of Things, 2025. All rights reserved.

tax (6.7%). For smaller cities with less than 25,000 people, the top three sources of income are user fees (41.7%), property taxes (20%) and the state (9.2%). In contrast, the top three income sources for larger cities are user fees (24.1%), other (17.7%) and property taxes (16.3%).[629]

A 2015 survey found that the 100 largest cities, with an average annual operating budget per city of $2.146 billion spent an average of $2,605 per citizen per year.[630] Common areas of city expenditures include public safety, social and health services, housing and urban development, public works and transportation, parks, recreation and cultural facilities, education, general government, debt service and other/miscellaneous.[631]

17.1.2. Industry challenges

City projects face several challenges that constrain their growth. Four key challenges, which are relevant to the Internet of Things for municipalities and cities are:

- Infrastructure
- Budgeting
- Digital operations and services
- Public safety

Each of these is discussed in detail below.

17.1.2.1. Infrastructure

Infrastructure is the backbone of any city. Roads, water, sewage, power, telecommunications and broadband are essential to the operation and growth of the city. This infrastructure is, however, often old and in need of major repair and replacement. The American Society of Civil Engineers (ASCE) releases a report every four years that assesses an infrastructure's capacity for current and future demand, the existing and future condition, current funding and future needs, maintenance, public safety, resilience and innovation.[632]

ASCE rated the state of U.S. infrastructure as C- in its most recent 2021 Infrastructure Report Card.[633] This is a slight improvement from the previous report card in 2017 which rated the state of U.S. infrastructure as D+.[634]

[629] See note 628

[630] "Analysis of Spending in America's Largest Cities", Ballotpedia. April 2015. Link

[631] "The Fiscal Landscape of Large U.S. Cities", Issue Brief, Pew Charitable Trusts, December 13, 2016. Link

[632] "Making the Grade" Infrastructure Report Card, 2021. Link

[633] "Making the Grade" Infrastructure Report Card, 2021. Link

[634] "2017 Infrastructure Report Card", American Society of Civil Engineers. Link

© Strategy of Things, 2025. All rights reserved.

The National League of Cities, in its 2022 State of the Cities report, identified infrastructure as the number one issue among city mayors. Since 2015, infrastructure has been one of the top three issues as shown below in Figure 17-1.[635]

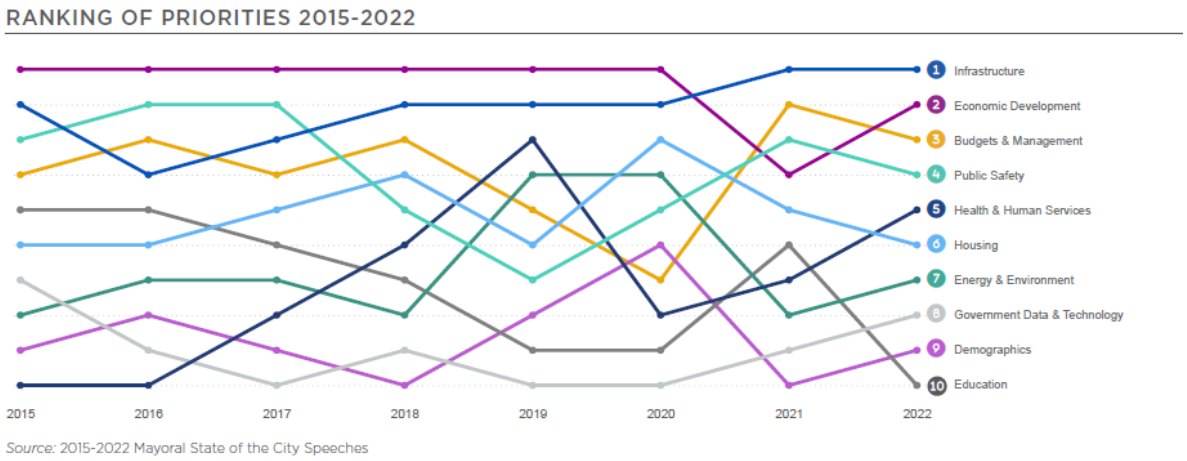


Figure 17-1: Smart Cities: Top 10 Mayoral Priorities (2015 to 2022)

The top five municipal infrastructure priorities are streets and roads (88% of mayoral respondents), water systems (85%), sewer system/storm water drainage (74%), public power utility system (63%) and water treatment and reclamation (59%).[636] At the same time, the National League of Cities found that 91% of local officials said that insufficient funding was the top factor regarding decisions to build local infrastructure projects.[637]

Some representative examples illustrating the poor state of city infrastructure include:

- **Drinking Water Systems.** The U.S. drinking water infrastructure received a grade of C- from the ASCE. The United States has over 2.2 million miles of underground pipes that deliver drinking water. There is a water main break every two minutes and an estimated 6 billion gallons of treated water are lost each day.[638]

  Millions of Americans are still receiving their drinking water from old and unsafe pipes made of lead.[639] A 2018-2020 NRDC analysis that found 56% of the U.S. population, or roughly 186 million people, drank from water systems with detectable lead levels of 1 part per billion, 61 million people drank from water systems with detectable lead levels of 5 part per billion and 7 million people drank from water systems with detectable lead

[635] "2022 State of the Cities," F. Omeyr, E. Grabowski and B. Rainwater, National League of Cities, Page 6,2022. Link

[636] "NLC releases 2023 State of the Cities Report," Press Release, National League of Cities, Figure 2, July 2023. Link

[637] "Stateside Chat: Small Cities, Big Infrastructure Challenges", CAP. June 2021. Link

[638] "Drinking Water, Overview", Infrastructure Report Card, 2021. Link

[639] "The Time is Now to Modernize U.S. Infrastructure", The White House. Link

© Strategy of Things, 2025. All rights reserved.

levels of 15 part per billion.[640] The Environmental Protection Agency (EPA) has declared lead poisoning the number one environmental health threat in the United States for children under 6.[641]

- **Sewage and Wastewater.** The U.S. wastewater infrastructure received a D+ grade from the ASCE.

  Many of the treatment plants were built in the 1970's after the passage of the 1972 Clean Water Act and had an average life span of 40-50 years.[642] This aging infrastructure and inadequate capacity lead to the discharge of 900 billion gallons of untreated sewage into U.S. waterways each year.[643] The EPA estimates that between 1.8 million and 3.5 million people become ill each year due to recreational contact such as swimming with water that is contaminated by the overflow of sanitary sewers.

- **Stormwater.** The U.S. stormwater infrastructure received a D grade from the ASCE.

  Stormwater system challenges result in urban flooding, causing annual damages of around $9B.[644] Stormwater runoff causes pollution, with nearly 600,000 miles of rivers and streams and over 13 million acres of lakes, reservoirs and ponds considered impaired for human use.

  Federal funding averages $250 million per year, leaving an $8 billion annual funding gap to meet stormwater regulations.[645]

- **Roads and Bridges.** The U.S. roads and bridges infrastructure received a D and C-grade, respectively, from ASCE.[646]

  Of the four million miles of public roadways in the United States, 43% are in poor or mediocre condition. Currently, 42% of the 617,000 bridges are at least 50 years old. Approximately 7.5% of bridges are considered structurally deficient with 178 million trips taken across these structurally deficient bridges every day.[647] The poor state of this infrastructure leads to road closures for repairs or unplanned maintenance, detours, congestion, slower traffic speeds and increased wear and tear and fuel usage by

---

[640] "Causes and Effects of Lead in Water", NRD. September 2023. Link

[641] "EPA Lead Poisoning Prevention Week…", EPA. October 2015. Link

[642] "Wastewater", Infrastructure Report Card." 2021. Link

[643] "Understanding America's Water and Wastewater Challenges", Bipartisan Policy. May 2017. Link

[644] "Framing the Challenge of Urban Flooding in the United States", National Academies. 2019. Link

[645] "Stormwater", Infrastructure Report Card. 2021. Link

[646] "Making the Grade: U.S. infrastructure assessment," 2021 Report Card for America's infrastructure, ASCE, 2021. Link

[647] "Bridges", 2021 Report Card for America's Infrastructure, American Society of Civil Engineers. 2021. Link

© Strategy of Things, 2025. All rights reserved.

transportation vehicles

The ASCE estimated the poor road infrastructure resulted in motorists paying an additional $1,000 annually in time and fuel, 36,000 road deaths and rising pedestrian fatalities.[648] The Council on Foreign Relations has estimated traffic congestion delays are costing the economy between $120 to $160 billion per year.[649]

- **Broadband.** Nearly a quarter (23%) of U.S. adults do not have broadband connections at home.[650] The Federal Communications Commission (FCC) estimates 21.3 million Americans lacked access to a fixed terrestrial broadband connection supporting downloads of 25 Mbps and uploads of 3 Mbps service at the end of 2017.[651] An independent study by Broadband Now Research estimated the actual number to be twice that or 42 million Americans.[652]

  While broadband service affordability is one of the causes,[653] another contributor is a lack of available infrastructure. This is most prevalent in the low-income parts of urban areas and in rural and tribal communities.[654] As a result, 40% of schools and 60% of healthcare facilities outside of metropolitan areas lack broadband connectivity.[655]

  Broadband on tribal lands lags behind the rest of the country with 18% of people living there unable to access broadband service as of 2020.[656] Financial constraints limit broadband investments in these areas. The broadband service companies need adequate returns to justify their infrastructure investment in towers and cables.

  The limited ability of low-income Americans, however, to pay along with low population densities limit the ability of service providers to recoup their investments.[657]

---

[648] "Roads", 2021 Report Card for America's Infrastructure, American Society of Civil Engineers. 2021. Link

[649] "The State of U.S. Infrastructure", Council on Foreign Relation. September 2023 Link

[650] "Internet/Broadband Fact Sheet", Pew Research Center. April 2023. Link

[651] "Revised draft broadband deployment report continues to show America's digital divide narrowing significantly," Press Release, FCC News, May 1, 2019. Link

[652] "FCC Reports Broadband Unavailable to 21.3 Million Americans, BroadbandNow Study Indicates 42 Million Do Not Have Access," J. Busy and J. Tanberk, Broadband Now Research, February 3, 2020. Link

[653] "Closing the Digital Divide for the Millions of Americans without Broadband", GAO. February 2023. Link

[654] ibid.

[655] "America's Digital Divide", PEW Research. July 2019. Link

[656] "Closing the Digital Divide for the Millions of Americans without Broadband", GAO. February 2023. Link

[657] See note 651

© Strategy of Things, 2025. All rights reserved.

17.1.2.2. Budgeting

Budgets are a source of ongoing challenge for municipal governments. These challenges were amplified by the COVID-19 pandemic and its lingering effects. The National League of Cities, in its 2022 State of the Cities report, identified budget and management as the third most important issue and priority among city mayors.[658] Since 2015, budget and management have been in the top four issues in six of the past eight years as shown above in Figure 17-1.[659]

Some representative examples illustrating budget challenges include:

- **COVID-19 impacts.** The pandemic led to municipal revenue shortfalls and unplanned expenses. The National League of Cities projected that cities, towns and villages will face a $360 billion budget shortfall from 2020 to 2022.[660] A study of thirteen major cities reported general fund budget shortfalls ranged from 1.9% (Boston) to 17% (Detroit).[661] The infusion of $900 billion in federal fiscal assistance programs, including the Coronavirus Aid, Relief and Economic Security (CARES) Act, the Families First Coronavirus Response and Relief Supplemental Appropriations Act (CRRSAA) and the American Rescue Plan Act (ARPA), eased some of these shortfalls.[662]

  As the COVID-19 pandemic eased, remote work and worker reluctance to return to in-office work continued to impact city budgets. While the national average for remote work is 39% in April 2022, workers in the ten largest metropolitan areas spent 57% of their workdays working remotely.[663] Tax revenues generated from retail and dining businesses decreased due to lower foot traffic and sales.

  Furthermore, remote work has driven down the need for office space, resulting in falling rents and lowered property values, creating lower property tax revenues for cities. For example, New York City was estimated to have lost $2.5 billion in property tax revenue in 2021.[664]

- **Easing of federal fiscal assistance.** The American Rescue Plan Act (ARPA) was passed as part of President Biden's plan to provide direct relief to Americans, contained COVID-19 relief and supported the economy.

---

[658] "2022 State of the Cities," F. Omeyr, E. Grabowski and B. Rainwater, National League of Cities, 2022. Page 6. Link

[659] ibid. p. 6.

[660] "What COVID-19 Means for City Finances," A. Yadavalli, C. McFarland and S. Wagner. National League of Cities. 2020. Page. 4. Link

[661] "How the Pandemic Has Affected Municipal Budgets in Philadelphia and Other Cities," E. Haider and J. Hachadorian, Pew Charitable Trusts, March 30, 2021. Link

[662] "The Resilience of State and Local Government Budgets in the Pandemic", J. Clemens, EconoFact, March 29, 2022. Link

[663] "As Remote Work Persists, Cities Struggle to Adapt", T. Henderson, Stateline Article, Pew Charitable Trusts, May 24, 2022. Link

[664] "Virus Siphons $2.5 billion in N.Y.C. Property Tax Revenue" New York Times. January 2021. Link

© Strategy of Things, 2025. All rights reserved.

Of the $350 billion provided in funding for state and local governments, $195 billion was provided evenly to states and $130 billion was divided between cities and counties.[665] The funds were used to replace lost public sector revenue, respond to public health and economic impacts due to the pandemic, provide premium pay for essential workers and invest in water, sewer, broadband infrastructure, natural disaster emergency relief, surface transportation projects and Title 1 education projects.[666]

As federal assistance funds run out, many cities are facing significant budget gaps. For example, New York City is calling for cuts to schools and libraries to address an anticipated $2.9 billion budget shortfall. Oakland is experiencing the largest general fund deficit in city history at $345 million.[667] Milwaukee is discussing the possibility of cutting hundreds of firefighter and police officer positions and closing libraries and fire stations to cover an estimated $156 million budget gap.[668] "SF Muni", San Francisco's municipal transportation agency, faces a budget deficit of $130 million in 2025 and $214 million in 2026, as their $4.5 billion in federal aid expires in 2025. [669]

Cities "became addicted to" these funds as they put a temporary cover on looming budget issues that are now coming to light.[670]

- **Underfunded pensions.** U.S. public pension funds are also on record for their largest setback since the Great Recession, with stock and bond losses resulting in pension funds estimated to only cover 77.9% of promised benefits.[671]

  The group Truth in Accounting reported that New Orleans only has 55 cents for every dollar of pledged pension benefits accounted for and Portland sits even lower at 44 cents per dollar.[672]

  This highlights a nearly $500 billion dollar gap between assets and what retirees are owed. The American Legislative Exchange Council (ALEC) recently calculated that other post-employment benefit liabilities across the United States. amounts to over $1

---

[665] "American Rescue Plan Spending: Recommended Guiding Principles", GFOA, 2022. Link

[666] "Coronavirus State and Local Fiscal Recovery Funds", U.S. Department of the Treasury. 2023. Link

[667] "Cities Stare Down Huge Budget Gaps", Route Fifty. May 2023. Link

[668] "'Emergency situation': Milwaukee officials discuss possible budget cuts", Wisconsin Public Radio. April 2023. Link

[669] "S.F. Muni Faces Massive $214 Million Deficit. Here's What Might Happen Next", San Francisco Chronicle. February 2023. Link

[670] "Houston Will Face A Budget Crisis By 2025 Unless It Cuts Spending Next Year, City Controller Says", Houston Public Media. July 2023. Link

[671] "Public Pensions Face Worst Funding Decline Since Great Recession." Bloomberg. July 2022. Link

[672] "The U.S. Cities Drowning in Debt", Forbes. February 2023. Link

© Strategy of Things, 2025. All rights reserved.

trillion dollars.[673]

Moody's Investor Service has an even bleaker estimate, reporting that public pensions are underfunded by $4.4 trillion dollars, a result of over optimistic actuarial assumptions, financial crises, real estate crises, lower than expected investment returns, the increased lifespan of retirees and a lack of corrective actions by local governments.[674] These underfunded pensions leave governments with the choice of collecting more taxes or cutting spending.

17.1.2.3. Digital operations and services

Local and state governments face a range of technological challenges to support modern municipal needs and digital government initiatives. While residents and businesses prefer accessing government services through digital channels by a two-to-one margin,[675] many public services are built around legacy technology systems and offered only through in-person means. The pandemic exacerbated this gap when office closures and remote working resulted in the reduction of in-person public services.

Another challenge municipalities face is increasingly frequent cyberattacks. Since 2016, there have been over 400 ransomware attacks on U.S. cities and counties.[676] Finally, the complexity, interoperability and obsolescence risk of existing legacy systems hamper the integration, deployment and effectiveness of smart city and other innovative technologies.[677]

This increasing importance of technology was reflected in a National League of Cities study. In 2022, government data and technology were the 8th most important mayoral issue and priority. While technology has been in the top 10 mayoral priorities since 2015, its importance among mayors has risen since the onset of the pandemic. In 2019 and 2020, technology was ranked 10th out of ten but rose to 9th in 2021 and 8th in 2022.[678]

Some representative digitalization challenges include:

- **Legacy systems.** Proprietary legacy systems and applications are used in local, state and federal government agencies. These systems support a variety of public services, such as permitting, licensing and tax payments.

  The Center for Digital Government reported found that one-third of the 250 state IT

[673] "Other Post-Employment Benefit Liabilities", ALEC, 2019. Link

[674] "The Time Bomb Inside Public Pension Plans", Knowledge at Wharton, August 2018. Link

[675] "Governments can deliver exceptional customer experiences – here's how", A. Dave, M. Jacobs, K. Modi and S. Tucker-Ray, McKinsey & Company, November 16, 2022. Link

[676] "Amid A Surge in Ransomware Attacks, Cities Are Taking Some of the Biggest Hits," J. Marks, Washington Post, September 3, 2021. Link

[677] "Let Interoperability be the Foundation Of Smart Cities," Paradox Engineering, Cities Today, January 14, 2021. Link

[678] "2022 State of the Cities," F. Omeyr, E. Grabowski and B. Rainwater, National League of Cities, 2022. Page 6. Link

© Strategy of Things, 2025. All rights reserved.

systems reviewed were legacy systems, defined as "a business-critical system that was implemented prior to Oct. 25, 2001, and is currently unable to meet user demands," while another 14% were legacy systems that were in the process of being modernized.[679]

Legacy systems incur high maintenance and operating costs. It is estimated that 80% of an agency's technology budget is used to support the operations and maintenance of existing systems.[680] Other legacy system issues include finding staff experienced with older technology and programming languages, the inability to support evolving agency missions and needs and increased cybersecurity risks.[681] Finally, degraded performance and efficiency, compromised good data governance, diverting resources and slowing innovation are additional risks with using legacy systems.[682]

- **Cybersecurity risks.** Aging technology infrastructure and systems create increased cyberattack surfaces. Between 2018 and 2023 the U.S. government experienced 330 ransomware attacks. These attacks affected over 230 million people and resulted in over $70 billion in downtime alone.[683]

  In many cases, the cost of downtime or rebuilding hijacked systems has cost more than the initial ransom. For example, Imperial County, CA faced a $1.2 million ransom in April 2019 and declined to pay. The County restored their operations in 6 days at a cost of $4 million. Similarly, Plainfield Town, CT also experienced a $199,000 ransom in March 2022 and incurred a cost of $350,000 to restore the systems.

  While legacy systems are vulnerable, the integration of internet connected smart city devices in the municipal network creates new risk surfaces. As more public services are offered digitally, municipalities must recruit and add more cybersecurity staff. A recent 2022 Center for Digital Government (CDG) data found that 98% of states, 76% of counties and 83% of cities will need to hire more cybersecurity staff over the next few years.[684],

- **Implementation.** Municipalities face several challenges implementing digital technology initiatives. A Gartner survey of over 150 government sector CIOs reported the top

---

[679] "Data Suggests One-Third of State IT Systems are Old and Broken", Government Technology. Link

[680] "Outdated and Old IT Systems Slow Government and Put Taxpayers at Risk", U.S. Government Accountability Office, February 2023. Link

[681] "Information Technology: Agencies need to continue addressing critical legacy systems," K. Walsh, Testimony before the subcommittee on Cybersecurity, Information Technology and Government Innovation, Committee on Oversight and Accountability, House of Representatives. United States Government Accountability Office. GAO-23-106821. May 10, 2023. Link

[682] "Five Ways Your Legacy Systems Hold Your Business Back," P. Godwal. IEEE Computer Society. August 18, 2022. Link

[683] "Ransomware Attacks on U.S. Government Organizations Cost Over $70bn from 2018 to October 2022", Comparitech. Link

[684] "Threats, Costs and people: Cybersecurity by the Numbers", Government Technology. Link

© Strategy of Things, 2025. All rights reserved.

challenges to adoption and implementation of digital solutions include siloed strategies and decision making, business culture blocking change, insufficient budgets and funding and insufficient depth and breadth of digital skills.[685]

A 2022 Center for Digital Government (CDG) survey of 127 leaders from mid-sized cities and counties reported that the top challenges for technology projects were funding IT modernization (69% of respondents), staffing challenges (65%), time (53%), expertise/skill sets (40%), legacy technologies (35%) and integration (32%).[686] The integration of technology is often complex due to the incompatibility of new software with existing IT infrastructure and back-end systems.[687]

Another major challenge is the risk adverse change culture found in the public sector,[688] as digital innovation often means there are new systems and processes to learn, adding to staff's existing workload. A McKinsey and Oxford University research study reported that public sector IT projects are six times as likely to experience cost overruns when compared to the private sector, while also facing heightened sensitivity to security risks, multistage decision making with various government stakeholders and bureaucratic procurement processes.[689]

17.1.2.4. Public Safety

Public safety is an ongoing concern for municipal governments. The National League of Cities in its 2022 State of the Cities report, identified public safety as the fourth most important issue among city mayors. Since 2015, public safety has been among the top five issues in seven of the past eight years as shown above in Figure 17-1.

Some representative examples illustrating key public safety challenges include:

- **Crime.** While crime rates have fallen from 2010 to 2019, crime remains a persistent challenge for American cities. For example:

  - Robberies declined by 51% during the period 2011 to 2021, but murder/manslaughter and aggravated assaults increased by 46% and 22%, respectively during the same period.[690]

[685] "5 Key Digital Transformation Challenges Government CIOs Must Tackle", Gartner, March 2022. Link

[686] "IT Infrastructure in Mid-Sized Cities and Counties: Moving Towards Resilience and Sustainability", A Center for Digital Government Research Report. Link

[687] "IT Infrastructure in the Public Sector: Benefits and Challenges", My Tech Magazine, February 2022. Link

[688] "Capturing Value from IT Infrastructure Modernization in the Public Sector", McKinsey & Company, November 2019. Link

[689] "Mitigating Risk in IT Megaprojects", McKinsey & Company, January 2018. Link

[690] "2023 Crime Rates in U.S. Cities Report", R. Gabriele, Safe Home, May 31, 2023. Link

© Strategy of Things, 2025. All rights reserved.

- Burglaries and larceny thefts declined by 55% and 25% respectively although motor vehicle thefts rose 21% over this period.[691] Vehicle thefts are considered "keystone crimes" because they facilitate the commission of homicides or other criminal offenses.[692]

- Retail theft and organized retail crime are common in many large cities. Over 56% of small businesses experienced theft in their stores according to recent data provided by the U.S. Chamber of Commerce.[693] The National Retail Federation reported that shrinkage resulted in a $112.1 B loss in 2022 alone.[694] The report also highlighted that 88% of shoplifters were somewhat more or much more aggressive and violent with violent shoplifting incidents up 35% on average.

- While crime occurs in urban, suburban and rural communities, urban areas have higher crime rates. For example, during the period 2018 to 2020, data from the National Crime Victimization Survey found violent crime rates were 29% to 42% higher in urban areas than in rural communities. In 2021, the violent crime rates for urban and suburban areas were 121% and 48%, respectively, higher than in rural areas.[695]

- Crime impacts cities in a variety of ways. They inflict physical, emotional and economic harm to victims and communities. Higher crime levels can lower property values, raise insurance premiums, reduce local investments and lower retail earnings and tax collections.

  Taxpayers incur nearly $300 billion annually to police communities and incarcerate 2.2 million people. The societal costs of incarceration include lost earnings, health effects and damage to families. The total economic burden is estimated to be $1.2 trillion annually.[696]

- **Addiction.** Drug abuse has also impacted cities with overdose deaths rising 44% since 2016, reaching a historic level of over 91,000 deaths in 2020.[697] Use of illegal drugs has many negative impacts such as an increase in crime, healthcare needs, lost work

---

[691] ibid.

[692] "Homicide, Other Violent Crimes Decline in U.S. Cities, but Remain Above Pre-Pandemic Levels", CCJ Press Release, Council on Criminal Justice, July 20, 2023. Link

[693] "Small Retailers Say In-Store Theft is Getting Worse", T. Swanek, U.S. Chamber of Commerce, September 22, 2022. Link

[694] "Retail Theft, Other Shrink Factors Drained $112B From Stores Last Year", B. Schulz, USA Today, September 27, 2023. Link

[695] "Criminal Neglect", J. Anderson, City Journal, October 4, 2022. Link

[696] "The Economic Costs of the U.S. Criminal Justice System", T. O'Neill Hayes, American Action Forum, July 16, 2020. Link

[697] "Overdose Death Rates", National Institute on Drug Abuse. Link

© Strategy of Things, 2025. All rights reserved.

productivity and other societal damages with the total cost of drug abuse estimated at $272 billion in 2017. The budget for National Drug Control program agencies has now reached a record $42.5 billion dollars, an increase of $3.2 billion from FY 2022.[698]

Some drug users may turn to criminal activity, such as robbery, burglary, theft and selling of stolen goods to support their habits. A 1991 Bureau of Justice Statistics (BJS) national survey of inmates found at least 17% of State Prison Inmates and 13% of convicted jail inmates committed their offenses to get money to buy drugs. In 2002, local jail inmate statistics showed that nearly 25% of convicted property and drug offenders in local jails had committed their crimes to get money for drugs.[699]

- **Homelessness.** The Department of Housing and Urban Development (HUD) reported there were over 582,000 Americans experiencing homelessness in 2022.[700] The National Alliance to End Homelessness has also reported that homeless rates have been climbing nationally at about 6% per year since 2017,[701] with a 30% surge in homeless between 2015 and 2020.[702]

    - Homeless people are at an increased risk for substance abuse, sexual abuse, violence, behavioral problems and the likelihood of entering the criminal justice system. The Substance Abuse and Mental Health Services Administration (SAMHSA) compiled a summary on homelessness statistics and related issues from multiple data sources in 2011 providing a general overview of the characteristics of the homeless population.[703]

      Of the homeless people in shelter systems, 26.2% had a severe mental illness and 34.7% had chronic substance abuse issues. Of those suffering from chronic homelessness, 30% had mental health conditions and 50% had co-occurring substance use problems. Other data in the report showed over 60% of chronically homeless people have experienced a lifetime of mental health problems and over 80% experienced alcohol and/or drug problems.

    - The report also found that 15.3% of jail inmates had been homeless at some point the year before incarceration and of those incarcerated, 79% had symptoms indicating drug or alcohol use or dependence, 75% showed symptoms of a mental illness and nearly half had experienced an act of violent crime.

---

[698] "National Drug Control Budget", The White House, March 2022. Link

[699] "Drug Use and Crime", Bureau of Justice Statistics. Link

[700] "How Many Homeless People Are In the US? What Does the Data Miss?", USA Facts, March 16, 2023. Link

[701] "Homelessness rose in the U.S. after pandemic aid dried up", K. Brooks, CBS News, June 21, 2023. Link

[702] "State of Homelessness: 2022 Edition", National Alliance to End Homelessness. Link

[703] "Current Statistics on the Prevalence and Characteristics of People Experiencing Homelessness in the United States", SAMHSA, July 2011. Link

© Strategy of Things, 2025. All rights reserved.

- The Los Angeles Police Department reported that since 2018, over 60% of homeless-involved crime was violent. The San Diego County District Attorney found that homeless individuals were 514 times more likely to commit felony-level crimes in 2019 to 2021.[704] The San Diego County data from 2021 also showed that members of the homeless population are at a higher rate of being victims of crimes, including being 19 times more likely to be murdered, 27 times more likely to be a subject of attempted murder, 12 times more likely to be assaulted and 9 times more likely to be sexually assaulted when compared to the non-homeless population. [705]

- Public safety risks increase dramatically in these affected communities, as businesses and residents can experience theft, vandalism, violent crime and exposure to toxic substances and biohazards, all leading to a loss of property value and decreased quality of life.

  During 2017, California, Kentucky, Michigan and Utah reported over 1,500 hepatitis A infections, with most of those infected reporting drug use or homelessness.[706] The California city of Berkeley made the news when they collected over 75 tons of trash and hazardous waste including sewage and drug paraphernalia from 16 make-shift encampments from September 2021 to March 2022.[707]

- **Road Safety.** Road safety in the United States is decreasing as the number of pedestrians killed on the roadways has increased 62% since 2009.[708] The National Highway Traffic Safety Administration (NHTSA) estimated that 42,915 people died in motor vehicle traffic crashes in 2021, a 10.5% increase from 2020, reaching a 16-year high.[709]

  Distracted driving and drunk driving were found to be the leading causes of traffic deaths,[710] while the record increase in road user (drivers, pedestrians) deaths has also been attributed to increased speeding and reckless driving behaviors resulting from fewer people using the roadways during initial pandemic lockdowns.[711]

---

[704] "New Data Reveals Link Between Homelessness and Crime Wave in California", Andrew Noh, KOGO, March 29, 2022. Link

[705] "Homelessness and Crime: California's hot-button political issues are even more complex than you think", J. Vankin, California Local, June 17, 2022. Link

[706] "Hepatitis A Virus Outbreaks Associated with Drug Use and Homelessness – California, Kentucky, Michigan and Utah 2017" Centers for Disease Control and Prevention, November 2, 2018. Link

[707] "75 Tons of Waste Removed from Homeless Camps In Democratic Stronghold Berkeley", T. Richards, Washington Examiner, July 21, 2022. Link

[708] "Report Shows the U.S. Must Do More to Prevent Pedestrian Deaths", E. Blazina, Governing, July 13, 2022. Link

[709] "Newly Released Estimates Show Traffic Fatalities Reached a 16-Year High in 2021" NHTSA, May 17, 2022. Link

[710] "10 Deadliest Cities for Drivers", U.S. Insurance Agents, May 28, 2023. Link

[711] "Pandemic Lockdowns Made Rush-Hour Speeding, Risky Driving the New Normal", IIHS, June 21, 2022. Link

© Strategy of Things, 2025. All rights reserved.

Many cities are not allocating the appropriate resources or political force into creating safer pedestrian spaces. For example, while Vision Zero programs promise to reduce traffic deaths, only 45 cities have pledged to launch such programs. [712]

- **Emergency Response.** First response is a critical capability for public safety. An analysis of Calls for Service data from fifteen major law enforcement agencies, serving cities that cover fifteen percent of the U.S. population found that average response times have been rising from 2019 to 2022.[713]

  For example, the city of New Orleans experienced the largest increase for high priority incidents, with the average response time rising from 15.3 minutes in 2019 to 32.4 minutes in 2022.[714]

  In an interview with a local news station, Los Angeles Fire Department paramedics indicated that while a 3 to 4 minute response time was average, 15 minutes is common and 20 minutes could be the new norm.[715] The union representing rank-and-file police officers for the Los Angeles Police Department has proposed that police stop responding to 28 different types of 911 calls so as to transfer officers to more serious crimes.[716] Fifteen cities have adopted co-responder programs that send non-law enforcement responders to certain situations.[717]

  One cause is a shortage of first responder personnel while call volumes have increased. The pandemic and labor shortages have stretched resources with many facing burnout.[718] This has resulted in low morale in departments with an Austin Texas detective recently stating that "So many people have left our department that it's not uncommon for you to be put on hold and wait four or five minutes to get someone to answer a 911 call."[719]

  A study of 774 call centers conducted by the International Academies of Dispatch

---

[712] "Vision Zero Might Actually Be Working but Only a Few American Cities", E. Marquis, Jalopnik, November 28, 2022. Link

[713] "Police Are Taking Longer to Respond," J. Asher, Jeff-alytics, January 9, 2023. Link

[714] ibid.

[715] "'It happens every day': LAFD paramedics say 911 response times continue to rise", G. Silva, Fox11, February 23, 2023. Link

[716] "Los Angeles Police Union Proposes Limits to 911 Responses", Associated Press, U.S. News, March 1, 2023. Link

[717] "Rethinking how law enforcement is deployed," R. Subramanian and L. Arzy, Brennan Center for Justice, November 17, 2022. Link

[718] "These UC cities Defunded the Police: 'We're Transferring Money to the Community'", S. Levin, The Guardian, March 11, 2021. Link

[719] "Low Morale Public Support Leading to Policing Crisis", S. Kalich, D. Clark and L. Tepper, Newsnation, July 27, 2022. Link

© Strategy of Things, 2025. All rights reserved.

(IAED) and the National Association of State 911 Administrators (NASNA) reports that "more than half of 911 centers in the United States are facing a genuine staffing emergency."[720] The study reported that nearly all call centers had unfilled positions, with 26% of call centers having vacancy rates of 31% to 50% and 29% having a vacancy rate of 21% to 30%.

Similarly, a survey conducted by the American Ambulance Association reported paramedic and EMT turnover rates were 20 to 30% annually and 100% every four years.[721]

Finally, there is a shortage of police. Officer resignations were up 47% in 2022 compared to 2019 levels and retirements were up 19% according to a Police Executive Research Forum of 200 police agencies.[722] A 2019 survey by the International Association of Chiefs of Police found 78% of agencies have issues recruiting qualified candidates, 50% changed internal policies to gain qualified candidates and 25% eliminated services or positions due to the inability to staff.[723]

Another reason is outdated 911 systems technology. Legacy 911 systems were designed to support emergency calls from landline phones. Today over 70% of 911 calls come from mobile phones which cannot be accurately routed to the most appropriate call center.[724] Legacy systems cannot support video, mapping and text services which facilitate emergency response.

Finally, legacy systems are susceptible to hackers who may disrupt 911 response systems. In one incident described as the largest cyberattack on the country's emergency-response system, a hacker forced iPhones to repeatedly call 911 centers across the country.[725]

Upgrading to next generation 911 (NG911) systems is expensive and ranges from $5 to $7 million for agencies serving major metropolitan centers.[726] While NG911 systems are an improvement over legacy systems, they create new attack surfaces and entry points for

[720] "Survey: More Than Half of 911 Centers Face Staffing Crisis," 911.gov Connects, April 2023. Link

[721] "Ambulance, EMT First Responders Face 'Crippling Workforce Shortage'," N. Weixel, The Hill, October 27, 2021. Link

[722] "The U.S. is Experiencing A Police Hiring Crisis", Associated Press, NBC News, September 6, 2023. Link

[723] "'Vicious Cycle': Inside the Police Recruiting Crunch With Resignation on the Rise", P. Charalambous, ABC News, April 3, 2023. Link

[724] "Cities, States, Plod Toward 'Next Generation 911'", S. Breitenbach, Stateline, July 29, 2016. Link

[725] "911 Systems Are Getting Old and the Public Can Be In Danger When They Fail", T. Henderson, Washington Post, April 1, 2017. Link

[726] See note 724

© Strategy of Things, 2025. All rights reserved.

hackers to disrupt operations.[727]

17.2. IoT in Cities

Although the term "smart cities" has multiple definitions, it commonly refers to cities that use IoT and other technologies, including sensors, connectivity, cloud and edge computing and data analytics to create outcomes supporting their community of residents, businesses and visitors. Those outcomes include operational efficiency and productivity, sustainability, health and wellness, mobility, economic vibrancy, public safety, quality of life and resilience.[728]

A 2018 survey of 51 cities published by The U.S. Conference of Mayors reported the top objectives for implementing smart city projects include improving government responsiveness, increasing citizen satisfaction and increasing collaboration across city departments and reducing city operation costs.[729]

While the application of IoT to cities brings significant benefits, community support for smart city technologies varies. A July 2022 Harris Poll survey of 3,185 U.S. city residents, respondents reported that 87% felt it was important for their city to invest in emerging technologies, but the levels of enthusiasm, awareness and engagement varied by age of the respondent and the specific technology. [730] For example, 48% of the respondents strongly supported air quality sensors, but only 29% felt the same about facial recognition technology.

Despite its benefits, the adoption of IoT in the United States to create smart cities is relatively limited and "smart cities" today are "just cities with a few or several standout smart projects" that are not "networked, end-to-end."[731] One reason is a lack of funding to both start a project and then obtain the financial resources to sustain the project.[732] A second reason is concern that the deployment of IoT and other technologies to create smart cities may conflict with "legacy governance, social justice, politics, ideology, privacy and financial elements."[733]

Finally, concerns about cybersecurity and privacy slow smart city adoption. A 2023 report from the Information Technology and Innovation Foundation Cities urged city officials and communities to balance leveraging smart technologies against concerns of cybersecurity risk,

---

[727] "911? We have an Emergency: Cyberattacks on Emergency Response Systems", M. Grzegorzewski and W. Holden, Lawfare, May 3, 2023. Link

[728] "Planning Sustainable Smart Cities With the Smart City Ecosystem Framework," B. Chan, Strategy of Things, January 24, 2018. Link

[729] "Cities of the 21st Century: 2018 Smart Cities Survey," U.S. Conference of Mayors/IHS Markit Technology Market Report, June 2018. P. 24. Link

[730] "These 5 Charts Show What City Residents Think About City Tech", Dan McCarthy, Tech Brew, November 1, 2022. Link

[731] "The Inconvenient Truth About Smart Cities," K. Smith, Scientific American, November 17, 2017. Link

[732] See note 729. P. 25.

[733] See note 731

© Strategy of Things, 2025. All rights reserved.

commercial use of data and potential government surveillance against other concerns including public safety, sustainability, beneficial uses of data and cost.[734]

Two factors are poised to accelerate the adoption of IoT in cities. First, cities have matured in their thinking of smart cities, moving away from "technology first" to "resident first."[735] Some of this was due to the pandemic, which highlighted several socio-economic inequalities, including healthcare access and outcomes, digital access for work and education and accessibility for the disabled.[736] This shift is in better alignment with how cities operate and plan.

Second, federal funding is a key facilitator for overcoming many of the challenges. For example, the U.S. Department of Transportation awarded the city of Columbus, Ohio $40 million to create an integrated smart transportation system that would use data, applications and technology to help people and goods move more efficiently. This Smart City Challenge drew strong interest and applications from 78 cities. [737] Federal funding from the Infrastructure and Jobs Act (IIJA) and the American Rescue Plant Act (ARPA) represents significant funding opportunities to incorporate IoT and smart technologies into infrastructure projects such as roads, bridges, airports, ports, rails and public transportation.

17.2.1. IoT use cases

Our research indicates that the industry has several use cases where IoT solutions can be effectively used to streamline operations, increase productivity, improve community engagement, maintain compliance and increase agility. These use cases fall into the following five categories:

- **City Operations**: Automated processes and operations orchestrated by a city platform and following data-driven planning approaches.
- **Public Safety**: These technologies help emergency managers predict and mitigate flooding, wildfires and other natural disasters. They also provide image and video analysis, saving time and reducing errors.
- **Environment and Sustainability**: Use data collection and information technology to optimize water, natural resources and energy use.
- **Mobility and Transportation**: Additional information on the status of a range of transport modalities.
- **Smart Buildings and Campuses**: Connected buildings improve maintenance services and provide information on building status.

---

[734] "Balancing Privacy and Innovation in Smart Cities and Communities", Ashley Johnson, ITIF, March 6, 2023. Link

[735] "Smart City Evolution: How Cities Have Stepped Back from A 'Tech Arms Race'," D. McLean, M. Rachal and D. Zukowski, Smart Cities Dive, November 9, 2021. Link

[736] "5 Things COVID-19 Has Taught U.S. About Inequality," J. Myers, World Economic Forum, April 18, 2020. Link

[737] "Smart City Challenge", U.S. DOT. Link

© Strategy of Things, 2025. All rights reserved.

These use cases are shown below in Figure 17-2.

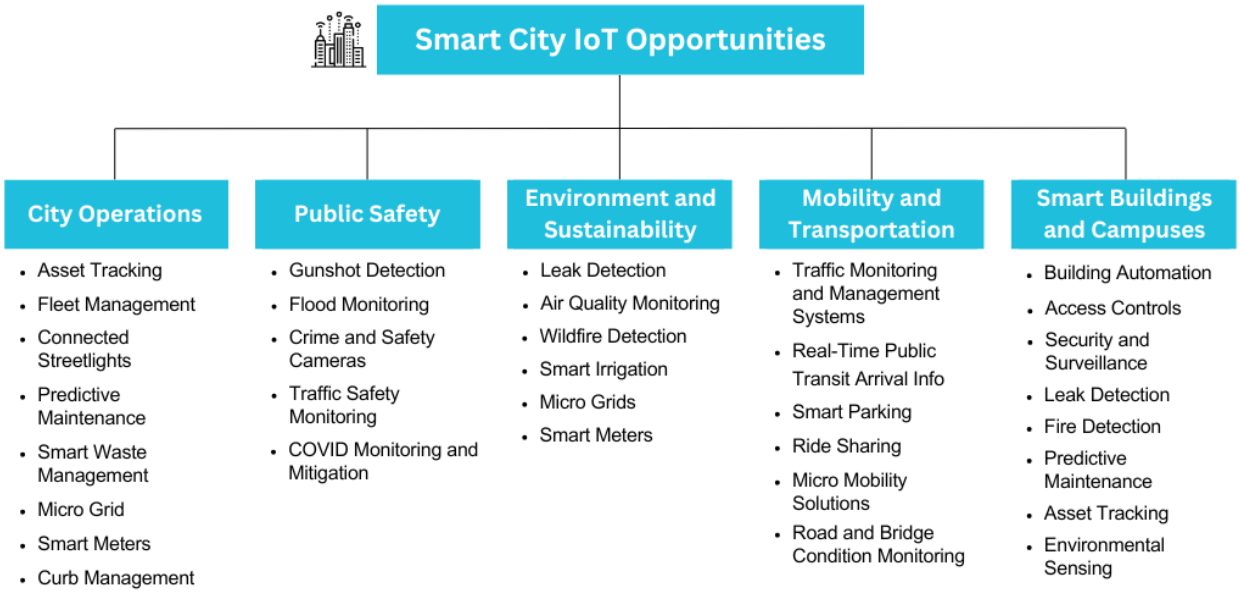


Figure 17-2: Smart Cities: IoT Use Cases Categories and Selected Use Cases

The value that IoT brings to cities and municipalities is significant. Cities and municipalities are faced with a range of challenges that the application of IoT and smart city technologies can address. For cities with limited budgets and resources to conduct day-to-day tasks, IoT solutions help increase staff productivity while reducing operational costs, resources and the time needed to complete activities. The top three functional areas for implemented and planned smart city projects are governance, mobility and transport and energy and resource efficiency.[738]

One example is connected streetlights or smart streetlights. These connected street lighting systems employ IoT sensors that allow city officials to increase and decrease illumination levels during different times of day and weather conditions as well as during incidents or special events to increase safety or save on energy costs.[739]

Smart streetlights detect light outages and immediately notify maintenance staff, eliminating the need to conduct periodic "drive by" manual inspections of each streetlight, freeing up maintenance staff and budget for other tasks leading to streetlight repairs in days instead of months.

Smart parking systems are vehicle parking systems that help drivers find a vacant spot.[740] These systems often use IoT sensors, digital signage and mobile apps to direct drivers to available

[738] Ibid. p. 21.

[739] "Connected Street Lighting: A Strong Foundation for a Smart City", IIoT World, June 12, 2019. Link

[740] "Smart Parking", PC Mag. Link

© Strategy of Things, 2025. All rights reserved.

spaces, reducing or eliminating driving for spots, lessening street congestion and encouraging more people to visit downtown areas and shop due to increased convenience and accessibility. Similarly, smart parking solutions help enforcement officers quickly identify where parking violations occur. This lessens the need for more enforcement officers and frees up resources and budget for other activities.

Cities and municipalities have physical infrastructure and assets that must be maintained and serviced. For example:

- Connected water level sensors on rivers and creeks and storm drains alert the community of potential flood conditions and allow proactive measures to be taken to avoid damage and loss of life.
- Connected strain gauges monitor the structural health of bridges and other structures and communicate "out of spec" conditions to engineers.
- Cameras mounted on city vehicles detect and alert maintenance staff to potholes and other potentially dangerous street conditions.
- Other IoT solutions detect the operating state of city vehicles and equipment and predict when maintenance service is needed.

The use of IoT solutions increases staff responsiveness to infrastructure maintenance needs, maximizes infrastructure operating life and prevents dangerous conditions.

Public safety is a priority in most communities. IoT solutions can prevent and facilitate response to emergencies and incidents. For example, a network of IoT based acoustic sensors detects and pinpoints the location of gunshots. This information is relayed to emergency dispatchers without anyone calling for help and directs police and first responders to the scene.

Automated License Plate Recognition (ALPR) systems can automatically capture an image of a vehicle's license plate and transform the image into alphanumeric characters using optical character recognition. The captured plate number is then compared to one or more databases of law enforcement vehicles of interest and can alert law enforcement when a vehicle of interest has been detected. Data is also used to help identify vehicles associated with certain suspects or persons of interest and can assist investigators in directing resources.[741] Similarly, camera systems employing facial recognition technology help identify suspects and facilitate crime solving.

Intelligent traffic monitoring and management systems are designed to detect and track vehicles and pedestrians and can estimate safety metrics for an intersection by recognizing the same object across successive time frames. This gives the platform the ability to estimate trajectories and object speeds.[742] These data can be paired with signal data to adjust traffic signals in real-time to reduce congestion or to give priority to public transit and emergency response vehicles.

In addition, cameras and LiDAR sensors monitor street intersections and collect data on traffic patterns and road user behaviors. The city's traffic engineers use this information to develop and

[741] "California ALPR FAQs", NCRIC. Link

[742] "Intelligent Traffic Management Reference Implementation", Intel, December 12, 2022. Link

© Strategy of Things, 2025. All rights reserved.

evaluate initiatives to control road speeds, minimize accidents and lessen the severity of injuries and fatalities.

17.2.1.1. Use case and industry challenges alignment

Smart cities face several challenges, some of which are described in Section 17.1.2. Figure 17-3 below shows the fit between the proposed use case subcategories and the documented industry challenges.

© Strategy of Things, 2025. All rights reserved.

Challenge	Role of IoT	Use case examples
Digital Operations and Services	Monitor physical assets, infrastructure and the environment and integrate into city operations and systems. Data collected gives managers and residents greater visibility and helps inform policies and decisions, as well as improve operational responsiveness.	• Asset tracking • Air quality monitoring • Traffic and traffic safety management and monitoring • Resource usage monitoring (water, electricity, gas)
Condition of Infrastructure	Monitor the condition of city infrastructure and improve responsiveness to service and repair of broken equipment and infrastructure. Increase proactiveness by predicting maintenance needs of assets and infrastructure.	• Infrastructures such as bridges, roads, water pipes, buildings, dams and levees and reservoir condition monitoring • Predictive maintenance of infrastructure facilities and equipment • Leak detection of pipes and irrigation systems
Government Budgets	Improve city staff and resource efficiency, effectiveness while creating cost savings and cost avoidance on assets and infrastructure.	• Smart waste management • City vehicle fleet management • Connected streetlights • Water leak detection • Building energy monitoring and management

© Strategy of Things, 2025. All rights reserved.

Challenge	Role of IoT	Use case examples
Public Safety	Monitor conditions impacting public safety and the ability of first responders to address them such as traffic, crime, fire, infrastructure conditions, river levels and scene situational awareness.	• Security and surveillance • Traffic monitoring and management systems • Gunshot detection • Connected streetlights • People location analytics and tracking inside buildings • River and stream water level monitoring • Drones for public safety and disaster response

Figure 17-3: Smart Cities: Use Case and Challenges Alignment

17.2.1.2. IoT use case details

Figure 17-4 below provides details on each of the use case subcategories as shown in Figure 17-2.

Category	Use case	Definition
City Operations	Asset tracking	Monitor and track the location and status of city assets, including vehicles, equipment, and resources. Aids in location, deployment and theft recovery.
	Fleet management	Monitoring and managing a fleet of vehicles or transportation assets. It includes tasks such as managing vehicle utilization, condition, maintenance, optimizing routes and usage and ensuring compliance with regulations.
	Connected streetlights	Sensors and controllers monitor streetlight operation and status (on/off), detect broken lights, optimize energy consumption and control lighting levels.

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Definition
	Predictive maintenance	Monitors key parameters on machinery and equipment. Detects out of spec conditions early and alerts technicians to service equipment before failure.
	Smart waste management	Sensors on waste bins collect data on bin levels, waste generation patterns and behavior to optimize waste collection, reduce costs and improve sustainability.
	Microgrid	Local grid within a community that connects local distributed energy resources (solar, batteries) to help meet local electricity demand at certain times and lessen need for power from upstream sources.
	Smart meters	Measure and monitor energy usage and other resources (gas, water) consumption in real-time.
	Curb management	Sensors manage the use of curb space for various purposes such as parking, loading/unloading or transit stops. It can help reduce congestion, improve safety and support sustainable transportation modes. A broader use of smart parking.
Public Safety	Gunshot detection	Gunshot detection systems use acoustic sensors to detect gunshots in real-time and alert law enforcement agencies. They can help reduce response times and improve public safety.
	Flood monitoring	Measure water levels in rivers, lakes or other bodies of water. These data can issue early warnings to residents and be used to predict and plan future flood responses.
	Crime and safety cameras	Crime and safety cameras are video surveillance systems used by law enforcement agencies to monitor public spaces for criminal activity or safety hazards.

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Definition
	Traffic safety monitoring	Monitor traffic conditions on road and adjust timing to reduce congestion, optimize traffic flow, increase pedestrian safety and improve air quality conditions.
	COVID monitoring and mitigation	Use various technologies such as contact tracing apps, temperature scanners or air quality sensors to monitor the spread of COVID- in public spaces.
Environment and Sustainability	Leak detection	Leak detection systems use sensors to detect leaks in pipelines or other infrastructure systems. This helps prevent environmental damage, reduce repair costs and ensure regulatory compliance.
	Air quality monitoring	Sensors to measure air quality levels in real-time. These data are used to identify and inform community members of real time conditions, detect pollution hotspots, inform public health policies and support sustainable urban planning.
	Wildfire detection	Cameras and other sensors to detect wildfires in real-time. This helps improve response times, aids community evacuations and minimizes wildfire damage.
	Smart irrigation	Smart irrigation systems use sensors or weather data to optimize irrigation schedules for city parks. This helps conserve water resources and reduce costs.
	Microgrids	Local grid within a community that connects local distributed energy resources (solar, batteries) to help meet local electricity demand at certain times and lessen need for power from upstream sources.
	Smart meters	Measure and monitor energy usage and other resource consumption such as gas and water in real-time.

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Definition
Mobility and Transport	Traffic monitoring and management systems	Monitor traffic conditions on the road and adjust timing to reduce congestion, optimize traffic flow, increase pedestrian safety and improve air quality conditions.
	Real-time public transit arrival info	Monitor public transit arrival information systems provide passengers with up-to-date information on bus or train schedules in real-time using GPS technology.
	Smart parking	Sensors or cameras to monitor parking spaces in real-time and provide drivers with information on available parking spots nearby.
	Ride sharing	IoT enabled transportation services that inform multiple passengers traveling in the same direction to share a ride using a single vehicle. This helps reduce traffic congestion and carbon emissions.
	Micromobility	IoT-enabled transportation, such as electric bikes or scooters, which are designed for short trips within urban areas
	Road and bridge condition monitoring	Monitor condition of key transportation infrastructure. Detect issues and notify public works personnel to address maintenance and repair.
Smart buildings and Campuses	Building automation	Monitor, manage and control building wide systems such as HVAC, lighting, alarms, security access and cameras, energy consumption, based on usage conditions.
	Access controls	Monitor, manage and track authorized and unauthorized access to an area, or to certain operations.

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Definition
	Security and surveillance	Detect unauthorized access, commission of illegal and unsafe activity and suspicious behaviors in public and private spaces. Alert first responders and safety personnel.
	Leak detection	Detect leaks in pipelines or other infrastructure systems. This helps prevent environmental damage, reduces repair costs and resource waste.
	Fire detection	Detect fire or smoke in a building. This can be used to alert occupants of a fire emergency, automatically trigger fire suppression systems and alert first responders.
	Predictive maintenance	Monitor key parameters on machinery and equipment. Detects out of spec conditions early and alerts technicians to service equipment before failure.
	Asset tracking	Monitor and track the location and status of city assets, including vehicles, equipment, and resources. Aids in location, deployment and theft recovery.
	Environmental sensing	Sensors collect data about air quality, noise levels, weather conditions or other environmental factors.

Figure 17-4: Smart Cities: Use Case Categories Details

© Strategy of Things, 2025. All rights reserved.

17.2.2. Market views of IoT in cities

To understand market views on IoT and to inform on our gaps discovery and analysis, our research team conducted a survey of 450 people, from adopters to solution providers, across the nine industries studied. Survey respondents were asked their opinion on the importance of IoT for smart cities over the next 5 to 10 years. Figure 17-5 below shows a high expected relative impact of IoT, as compared to other industries. One reason for this high rating is that the applications of IoT in cities are numerous and often highly visible to residents. For example, many residents are familiar with ridesharing, micro-mobility services and surveillance security camera systems.

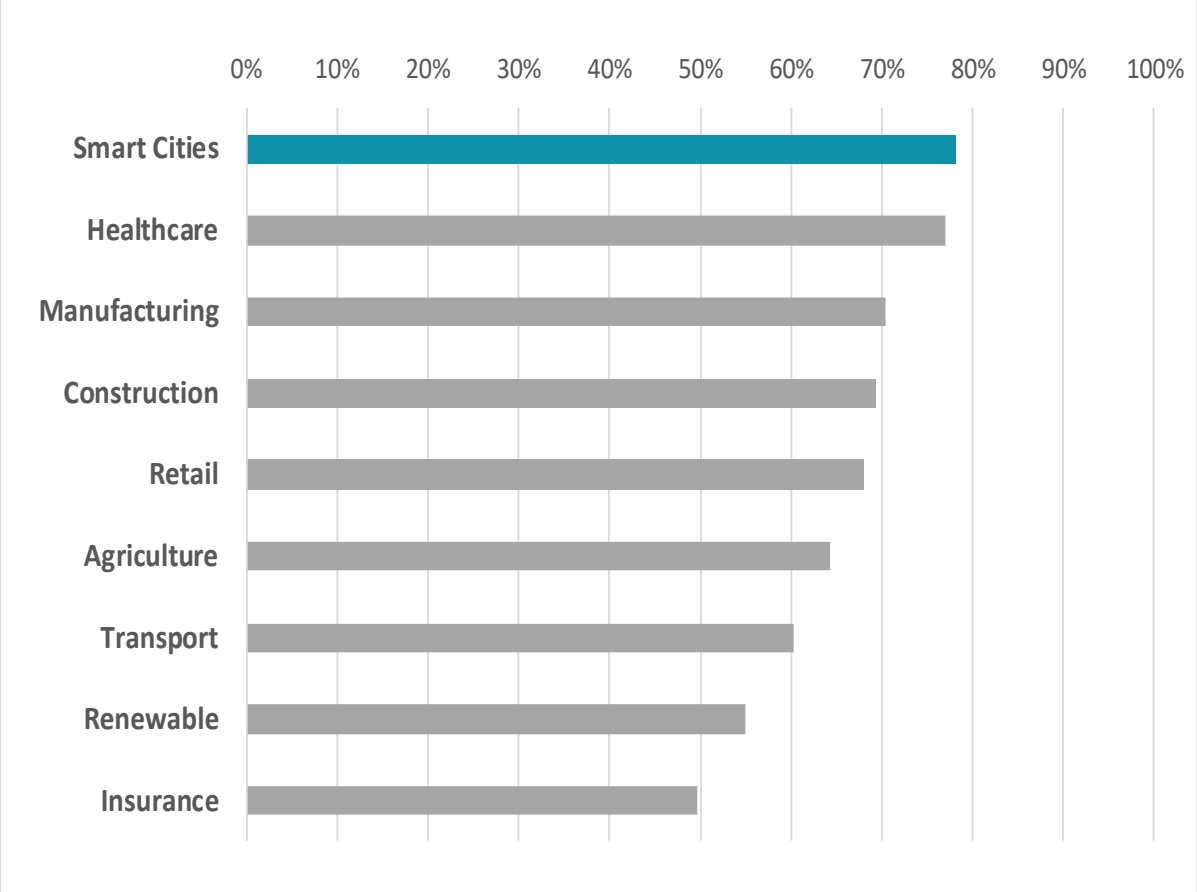


Figure 17-5: Smart Cities: Importance of IoT

Survey respondents were asked to rate the impact of these use case categories on cities.[743] Figure 17-6 below shows their responses which show a bias to a high impact of the use case categories for cities.

[743] In your view, what will be the impact of these use cases in cities over the next 5-10 years?

© Strategy of Things, 2025. All rights reserved.

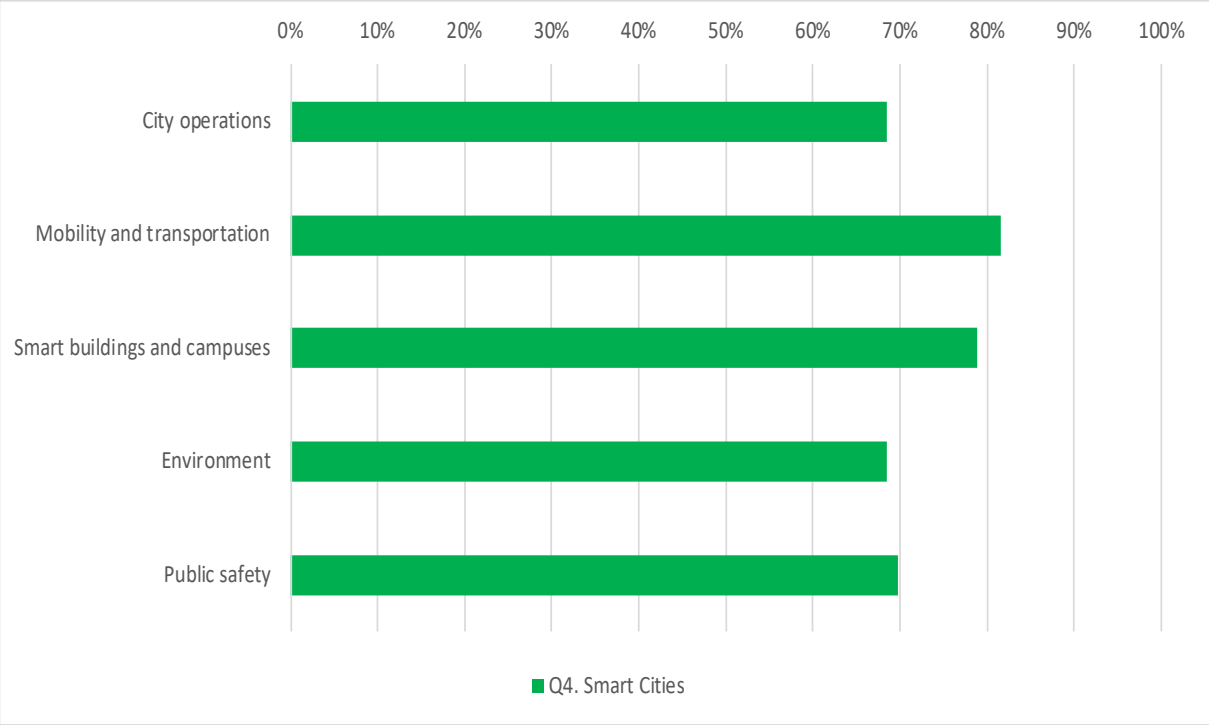


Figure 17-6: Smart Cities: Importance of IoT Use Case Technology

17.3. IoT gaps and findings for cities

A combination of interviews, secondary research and surveys was conducted to identify and understand the opportunities and challenges to the development and adoption of IoT. Each research method approached the challenges from a different perspective.

For example, the survey targeted a large audience but asked specific questions that supported the economic analysis. The interviews targeted a small number of people who provided deeper insight and context to supplement the information already collected. Finally, the desk research, consisting of a review of online news articles, published research reports, vendor and government white papers, blogs, webinars, videos and other content, provided a broad overview of the application of IoT in the industry.

In our survey, respondents were asked to choose the most important technology areas to operationalize IoT in their industry. Figure 17-7 below shows respondent's selections of the top 10 IoT technologies and the percentage of respondents who chose that technology.[744] The survey results are not seen as a technology gaps list, but rather an indication of what is important to the respondents. This information partially informs the gap selection process.

[744] Respondents were asked to choose up to 5 out of the 25 technologies listed.

© Strategy of Things, 2025. All rights reserved.

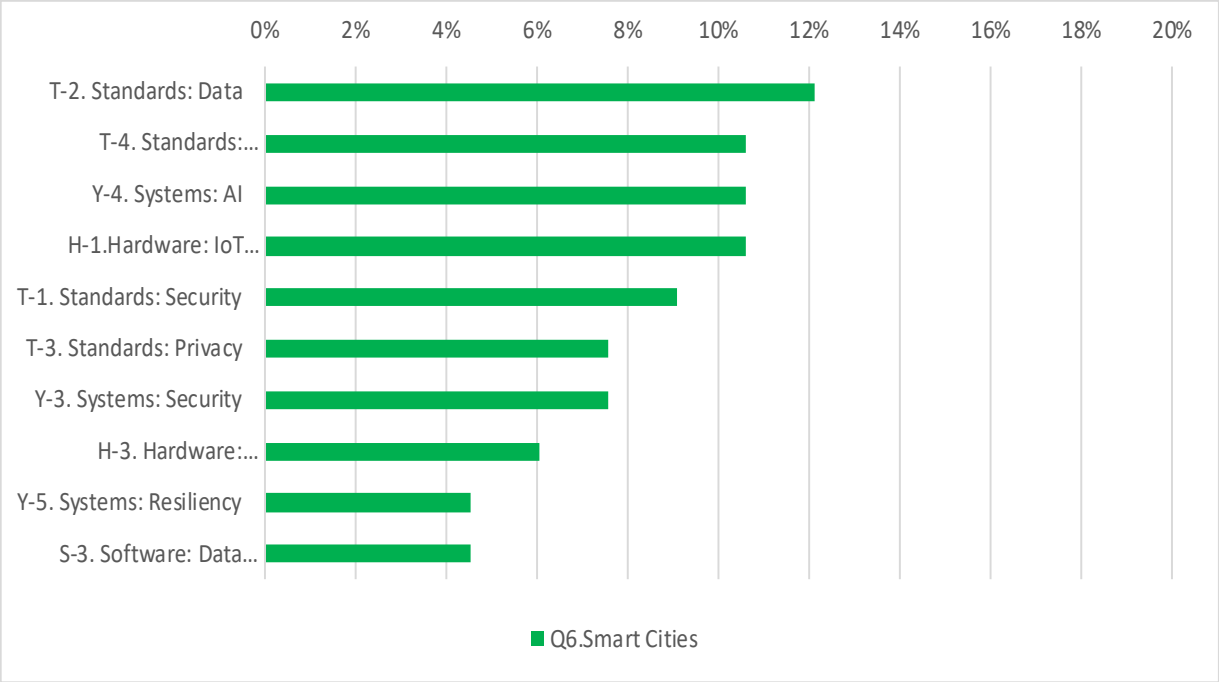


Figure 17-7: Smart Cities: Top 10 Most Important Single Technologies

17.3.1. Top technology challenges

Based on the approach described above, the following three IoT technology challenges were identified:

- Interoperability
- Privacy
- Edge infrastructure

Each of these is discussed below.

17.3.1.1. Challenge # 1: Interoperability

The lack of IoT interoperability for smart cities is a major technical obstacle, hindering the realization of interconnected urban environments.

Cities host a range of smart technologies, IoT devices and systems that are independently owned and operated by a variety of municipal and non-municipal organizations. These organizations do not always communicate or interact with each other. For example:

- A city's traffic agency owns and operates traffic cameras and intelligent traffic signal systems.
- The police department owns surveillance cameras and gunshot detection systems.
- The state transportation department operates its own intelligent traffic signals on state roads that run through cities.

© Strategy of Things, 2025. All rights reserved.

- Utility districts own and operate smart meters while the regional air quality district owns a network of air quality monitors.

In an ideal smart city environment, these disparate systems would communicate and collaborate with each other to create outcomes benefiting city residents and businesses.

For example, audio sensors detect gunshots. Once detected, the streetlights on nearby streets could increase in brightness to facilitate the ability of witnesses to identify the shooters and for police cameras to capture better quality surveillance footage. The information is then routed to the city's 911 response call center, which then informs the operator and provides situational awareness information to responding police officers.

In practice, the individual IoT applications were independently procured by different city organizations with little consideration for interaction and communication with each other. This leads to the deployment of technology systems that have the following characteristics:[745]

- Not extensible or cost effective because they are custom systems that cannot communicate and exchange information with each other.
- Based on a diverse set of proprietary architectures, standards and protocols that have not yet converged.
- Not sufficiently interoperable and scalable to support smart city applications and outcomes.

The lack of interoperability in IoT applications for smart cities remains a challenge, stopping the seamless integration and collaboration among diverse devices and systems.[746] This stops the municipality and other non-municipal organizations from realizing the full value of a smart and connected city. The consequences include:

- **Inability of disparate systems to interconnect.** This covers incompatible data formats and communication protocols between systems, as well as the exchange of data with different meanings. More importantly, this lack of interoperability reduces orchestration of different applications requiring costly custom integrations. These integrations are usually application-specific and are not extensible to other applications.
- **Limited ability to inform decision-making and support city governance.** The lack of standardized data formats and definitions exacerbates interoperability challenges. Each IoT device generates and processes data in a unique way, making it difficult to aggregate and analyze information across diverse platforms. This lack of standardization reduces the integration of data and the development of comprehensive, city-wide analytics that could inform intelligent decision-making for urban planning, traffic management and resource allocation.
- **Lock-in to specific vendors and/or solutions.** IoT technologies based on proprietary protocols do not work with systems having different standards and protocols. This "locks in" the city to procuring and using only systems from the vendor and its ecosystem

[745] "A Consensus Framework for Smart City Architectures", IES-City Framework Release 1.0, IES-City Framework Public Working Group, September 30, 2018. Link

[746] "Open standards: The answer to the smart city data dilemma", Opinion, 2019. Link

© Strategy of Things, 2025. All rights reserved.

partners. These systems may be more expensive, have fewer innovative features or have capability limitations. Migrating from these systems to other lower cost or more innovative alternatives is difficult and may require significant switching costs.

There are a variety of ongoing public and private initiatives to address interoperability issues.

- **The U.S. Department of Homeland Security (DHS).** The DHS is assessing the current state of smart cities standards for public safety applications with research, design and testing of a Smart City Interoperability Reference Architecture (SCIRA) interoperable framework that integrates commercial proprietary IoT sensors for public safety applications at the community level.[747]
- **NIST.** In collaboration with international industry partners, NIST has developed version 1.0 of the Internet-of-Things-Enabled Smart City (IES) City Framework to facilitate "the emergence of smart city technologies that are Interoperable, Composable and Harmonized."[748] This framework is based on Pivotal Points of Interoperability (PPI) which are "consensus standardized interfaces that deal with composition of Cyber-Physical Systems (CPS) without constraining innovation."[749] PPIs are a middle ground between complete standardization and no standardization.
- **The Fiware Foundation.** The foundation is building an ecosystem around its open source Fiware platform and its context broker Application Programming Interfaces (API) that allow the exchange of data between various smart city applications.[750]
- **The Open Connectivity Foundation.** The foundation is developing open standards for smart homes and buildings.[751]
- **The Institute of Electrical and Electronics Engineers (IEEE).** The IEEE has several ongoing smart city standards initiatives including one standard that "provides an architectural blueprint for Smart City implementation leveraging cross-domain interaction and semantic interoperability among various domains and components of a Smart City."[752]

Current government and industry efforts represent only part of the research needed to fully address interoperability challenges in smart cities. Continued efforts from the federal government, industry players, standardization bodies and policymakers are required to establish common frameworks and standards that facilitate seamless communication and integration across diverse smart city applications. Some areas of future research include:

---

[747] "Smart City Interoperability Reference Architecture," U.S. Department of Homeland Security Science and Technology Directorate, July 8, 2022. Link

[748] See note 745

[749] See note 745

[750] Fiware website. Link

[751] Open Connectivity Foundation website. Link

[752] IEEE Standards for Smart Cities. Link

© Strategy of Things, 2025. All rights reserved.

- Standards for IoT and smart cities.
- Communication Protocols for data exchange and collaboration.
- Standardizing data formats and models.
- Security and privacy frameworks that can be uniformly implemented across various smart city applications.
- Testbeds and pilots to design and evaluate interoperable smart city solutions.
- Policy and governance aspects of interoperability, such as regulatory frameworks, data privacy and governance models.

17.3.1.2. Challenge # 2: Privacy

While IoT and other smart city technologies bring new capabilities to help cities address challenges in new and more effective ways, privacy is a concern for the community. A resident survey of Long Beach (California), a city of 456,021 people, reported community sentiments typical of many cities. The survey found that 80% of respondents were "strongly concerned" or "somewhat concerned" that the use of smart city technologies could mean less privacy.[753] Three-quarters of respondents stated that sale of their personal data by the city to third parties should be prohibited.[754]

Fears that the data collected from the IoT sensors, including video cameras, could potentially be used to monitor and track people and their movements have led the American Civil Liberties Union (ACLU) to call smart cities "surveillance cities."[755]

Today's approaches to smart city privacy are static, piecemeal and have limited effectiveness. For example, many cities employ policies and regulations that ban or limit the use of facial recognition systems.

Smart city solutions may be configured to disable certain functionality or limit data collection and storage. While this achieves individual privacy objectives, they also keep the city from realizing the full range of benefits from smart city technologies. In addition, "blanket" approaches may only be effective in certain settings. As IoT devices are increasingly integrated into city infrastructure and operations, managing privacy through existing "device by device" approaches may no longer be effective, sustainable or relevant.

Addressing privacy in smart cities require a comprehensive approach that cuts across political, technical and socioeconomic lines. The development of privacy technologies and methods that achieve the intent of the legislation and policies across a variety of conditions while preserving privacy protections is essential for IoT and smart city technologies to scale.

---

[753] "Survey depicts residents' perceptions on smart cities and data privacy," City of Long Beach, Resident Survey Findings: Smart Cities And Data Privacy, June 8, 2021. Link

[754] ibid.

[755] "How to Stop 'Smart Cities' From Becoming 'Surveillance Cities'," C. Marlow and M. Saifuddin, ACLU, September 17, 2018. Link

© Strategy of Things, 2025. All rights reserved.

Two broad areas warranting further research include Context Aware Privacy and Privacy Enhancing Technologies. Each of these is examined below.

Context-Aware Privacy. Research analyst firm Gartner defines context aware computing as "a style of computing in which situational and environmental information about people, places and things is used to anticipate immediate needs and proactively offer enriched, situation-aware and usable content, functions and experiences."[756]

Similarly, context-aware privacy is an approach that considers the location, the environment and the specific situation and seamlessly adjusts how and what data are collected, processed and shared. This approach recognizes that different situations and conditions warrant various levels of data collection.

For example, smart parking systems that employ cameras analyze video images in real time to detect open parking spaces and relay that information to a mobile app. In normal situations, the cameras do not scan for license plate information, nor store any video images. When an Amber Alert is issued for the local region, however, the system is automatically enabled to scan license plates and relay the location of the vehicle matching the description to law enforcement. Upon cancellation of the Amber Alert, the parking system returns to its normal privacy mode.

Context-aware privacy is an emerging systems-based approach for addressing complex privacy challenges in smart cities. To be effective, context-aware privacy must accommodate a wide range of diverse city use cases, sensors, devices, settings and locations. It must automatically adjust how data from these systems are utilized based on the information needs of the specific scenarios.

Affected residents know when information is requested and specify and control what is shared and how it is used in different situations. Privacy settings adjust dynamically in real time to remain relevant during fast-changing situations. Privacy policies are designed with safeguards to minimize and mitigate the risks for individual privacy of data sharing. The operations and systems managing and governing privacy and consent are transparent, intuitive and easy to use.

Context-aware systems perform a series of functions, including:

- **Context acquisition.** Collection and gathering of data from various sensors and devices.
- **Context representation.** Verification, authentication and transformation of the collected data into a standardized format for use and sharing.
- **Context storage.** Storage, encryption and management of data for use over its useful life cycle.
- **Context interpretation.** Derivation of the high-level situational context from the collected data.
- **Context adaptation.** The identification and delivery of the necessary services and resources to adapt device and system behavior in response. [757]

---

[756] "Context aware computing," Information Technology Glossary, Gartner Glossary, Gartner Research. Link

[757] "Future challenges in context-aware computing," N. Malik et al., Conference Paper, IADIS International Conference, 2017. Link

© Strategy of Things, 2025. All rights reserved.

Several broad research areas need to be addressed for the implementation of context-aware computing and privacy for smart cities and other domains. These include context definition, context-aware architectures, context sensing, context prediction based on limited to no data, context representation, context interpretation and adaptation, evaluation of context aware systems and privacy control.[758]

In addition to these broad areas, examples of other challenges to be addressed by research to support context-aware privacy include:

- **Notification and consent.** Users receive notifications requesting their consent to information and how that information is used and shared. Existing notifications are, however, lengthy, written in legalese, too many in number, "take it or leave it" consent and presented at points in the process with limited ability to engage.[759]

  Smart cities have hundreds or thousands of unique devices and systems. Residents and users would be inundated with a stream of notifications and consent agreements from devices they encounter throughout the city. Furthermore, many of the smart city notifications and consent come from voice and IoT based devices that will not have display screens.[760]

  Research is needed to develop adaptive consent mechanisms and models that allow individuals to provide context-specific consent for the use of their data in smart city applications under a variety of conditions[761] and avoid the insufficiencies of existing notice and consent models.

  One example is a "software based trusted virtual agent that acts as an intermediary by communicating the privacy preferences of the person to the data collecting entity/technology."[762]
- **Context-aware privacy protection methods.** IoT devices in smart cities and other domains collect user and operational information that may be vulnerable to breaches. Research is needed to provide improved protections of these data. This may range from the use of Software Defined Networking (SDN)[763] to anonymization techniques that consider the specific context in which data are used and applies the most appropriate anonymization methods.

---

[758] See note 757 Table 1.

[759] "Redesigning data privacy: Reimagining notice & consent for human-technology interaction," A. Joesphine-Flanagan, et al., White Paper, World Economic Forum, July 2020. P. 7. Link

[760] See note 759. P. 11.

[761] Schaub, F. (2018). Context-Adaptive Privacy Mechanisms. In: Gkoulalas-Divanis, A., Bettini, C. (eds) Handbook of Mobile Data Privacy. Springer, Cham. Link

[762] See note 759. P. 24.

[763] "A context-aware privacy-preserving method for IoT-based smart city using Software Defined Networking," M. Gheisari et al., Computers & Security, Volume 87, 2019, 101470, ISSN 0167-4048. Link

© Strategy of Things, 2025. All rights reserved.

- **Algorithmic explainability.** Intelligent algorithms and automation are key components in context-aware systems. These algorithms interpret the collected data to develop the necessary context and then adapt systems to take the most appropriate actions.[764] These algorithms, however, may result in actions that cannot be easily explained or deconstructed.[765] Research is needed to develop tools and methods that aid in the identification and mitigation of potential biases that may arise in different contextual situations, including where automation and AI are used for data processing and decision-making.
- **Risk assessment of potential harms.** Cities have complex and dynamic ecosystems. The introduction of IoT and other technologies creates new and unanticipated privacy risks in certain situations and contexts. Research is needed to develop a risk assessment framework to help cities understand and evaluate the privacy risks associated with different contexts and guide the development and implementation of policies and privacy protections.
- **User-centric tools, processes and interfaces.** In a contextually based privacy environment, notification and consent provide challenges for residents and users. The volume of notices and consent requests is overwhelming, disruptive and burdensome.[766] There is, however, no universal way that residents interact with these notifications to manage their privacy.

  For example, residents have different levels of digital literacy. Some may be visually impaired and not be able to see notices while others may not be able to read or write English. Research is necessary to develop the platforms, tools and interfaces that residents can use in an intuitive, non-burdensome and transparent manner.
- **Frameworks and standards.** There is limited integration of disparate IoT and smart city solutions in cities today. Many solutions are deployed as standalone systems and privacy policies are solution specific. Research is needed to develop frameworks and models for defining context-aware privacy systems and the deployment and scaling of these systems.

Addressing these challenges requires interdisciplinary research involving computer science, law, ethics, urban planning and social sciences to develop comprehensive solutions that consider both technical and societal aspects of context-aware privacy policies in smart cities.

Privacy Enhancing Technologies. Privacy enhancing technologies (PETs) are a "broad set of technologies that protect privacy by removing personal information, by minimizing or reducing

[764] Hoel, T., Chen, W. & Pawlowski, J.M. Making context the central concept in privacy engineering. RPTEL 15, 21 (2020).Link

[765] See note 759. P. 24.

[766] "Privacy in context," M. Ackerman, T. Darrell and D. Weitzner, Massachusetts Institute of Technology. Link

© Strategy of Things, 2025. All rights reserved.

personal data or by preventing undesirable processing of data while maintaining the functionality of a system."[767] Some examples of these technologies include:[768]

Cryptographic algorithms

- Homomorphic encryption which enables computation on encrypted data.
- Secure multi-party computation which enables computation from multiple encrypted data sources.
- Differential privacy which adds statistical noise to data.
- Zero knowledge proofs which allow information to be validated without revealing underlying data.

Data masking

- Obfuscation which replaces sensitive information with distracting or misleading data.
- Pseudonymization where identifier fields are replaced with fictitious data along with data minimization.
- Communication anonymizers which replace online identity with a one-time untraceable identity.

Artificial intelligence and machine learning algorithms

- Synthetic data generation which uses artificially created data.
- Federated learning which trains algorithm across multiple decentralized edge devices.

Other

- Trusted execution environments[769] which creates a secure area on a device to execute select operations in isolation.
- Zero party data[770] which covers data that a customer intentionally shares.

[767] "National Strategy to Advance Privacy-Preserving Data Sharing and Analytics," Fast-track action committee on advancing privacy-preservation data sharing and analytics, Networking and information technology research and development subcommittee, National Science and Technology Council Report, March 2023. Link

[768] "Top 10 Privacy Enhancing Technologies & Use Cases in 2023," C. Dilmegani, AI Multiple, July 21, 2020. Link

[769] "The New Generation of Privacy Preserving Technologies," R. Potter, CapGemini Expert Perspectives, June 13, 2022. Link

[770] "Straight From the Source: Collecting Zero-Party Data From Customers," S. Liu, Forrester Research Blog, July 30, 2020. Link

© Strategy of Things, 2025. All rights reserved.

PETs help mitigate some of the concerns but have limited adoption. PETs are seen as a gap because of "the need for more research and development, limited technical expertise, perceived and possible risks, financial cost and the lack of generalizable solutions."[771]

Continuing research and development is necessary to address some challenges and accelerate these privacy enhancing technologies. For example, the National Strategy to Advance Privacy-Preserving Data Sharing and Analytics report cites cryptographic technologies having initial success for real world adoption in simple applications. They still, however, have "scalability and efficiency challenges that need to be addressed in the context of a broader set of threat model."[772]

In addition, PET technologies lack consensus standards. While some standards development is underway for homomorphic encryption and zero knowledge proofs, the same report cites "more standards that specify foundational cryptographic primitives and other Privacy Preserving Data Sharing and Analytics (PPDSA) technologies would facilitate adoption and trust in solutions." Finally, the report notes that "there are no widely adopted standards for data formats, application programming interfaces or system architectures that are necessary to facilitate the interoperability and deployment of PPDSA technologies."

17.3.1.3. Challenge # 3: Edge Infrastructure

Gartner research projected that enterprise data created and processed outside of the cloud data center will grow by 75% from 2018 to 2025.[773] In a traditional IoT architecture, shown previously in Figure 11-1, data are routed from the device to a remote cloud data center for processing and storage. Not all data collected, however, needs to be or should be sent to the cloud for processing. For example, sending data collected from sensors on autonomous vehicles to the cloud creates additional latency. Processing needs to be done on the vehicle for the car to properly respond to sensor readings. In mission critical applications or in those where connectivity is intermittent or unreliable, processing is performed at the gateway or on the device. Privacy considerations also drive the need for on-device and edge processing. Camera-based smart parking systems process images locally then initiate an action, such as transmitting the location of open parking spaces and then delete the information to ensure unintended preservation of sensitive information.

Edge computing is an emerging paradigm for smart cities. For example, the city of Las Vegas is evaluating an edge-based traffic monitoring system on 16 intersections and plans to roll out the

[771] "Advancing a Vision for Privacy-Enhancing Technologies," A. Macgillivray and T. deBlanc-Knowles, White House Office of Science and Technology Policy blog, June 28, 2022. Link

[772] "National Strategy to Advance Privacy-Preserving Data Sharing and Analytics," Fast-track action committee on advancing privacy-preservation data sharing and analytics, Networking and information technology research and development subcommittee, National Science and Technology Council Report, March 2023. Link

[773] "What Edge Computing Means for Infrastructure and Operations Leaders," R. van der Meulen, Gartner, October 3, 2018. Link

© Strategy of Things, 2025. All rights reserved.

system to the core downtown area.[774] Other application areas include transportation, augmented reality, buildings and urban infrastructure management.[775]

To be effective in supporting smart city applications, edge computing and associated infrastructure must be scalable to support many devices and applications, provide reliable Quality of Service (QoS), be context aware, manage compute and storage resources effectively, be energy efficient, provide resources on demand to support workloads and be interoperable, private and secure.

Some areas of open research opportunities exist to address these requirements and challenges of edge computing in smart cities. These include:[776]

- **Intelligent caching.** Proper positioning and storage of content and data on the network alleviates traffic congestion and latency issues and reduces IoT device energy consumption of smart city applications. The mobility of users in a city environment, however, makes it challenging to identify and position the right data and content. Research and development of reinforcement learning based mobility-aware approaches, such as deep learning to predict cache content needs, is necessary.
- **Collaborative edge computing.** Individual edge computer servers and devices have limited computational and storage capabilities to process smart city applications. Aggregating nearby edge servers to process workloads collaboratively overcomes this limitation. To scale this capability, research is needed in areas like formation of collaboration spaces, social trust-based incentive policies, cooperation policies, interdomain cooperation, intradomain cooperation, smart collaborative networking and mobility management.
- **Cooperative and Sustainable Load Balancing.** Smart city applications impose dynamic workloads on edge servers. These workloads must be balanced in a cooperative manner between different servers and operators to avoid performance issues, excessive energy use and high operating costs. To support this capability, research is needed in game theory assisted incentive mechanisms, adaptive cooperation mechanisms and authentication-based load balancing.
- **Intelligent Edge Computing.** The use of AI and machine learning at the edge enables instant analysis and action. Some research opportunities include development of algorithms that can run on the edge servers with limited processing and storage capabilities, interoperable interfaces that allow large data sets to be shared and used and "system as a service" that enables systems to interact with each other and share data.
- **Network slicing.** The use of software defined networks in smart cities enables the separation of the control plane from the data plane. This enables the creation of virtual networks on top of a shared physical network to provide greater flexibility in the use and

[774] "Will technology be enough to stop Vegas' wrong way drivers?" S. Descant, Government Technology, August 9, 2019. Link

[775] "Edge-Computing-Enabled Smart Cities: A Comprehensive Survey," L. Khan, I. Yaqoob, N. Tran, S.M. Kazmi, April 2020IEEE Internet of Things Journal PP(99):1-1. Link

[776] See note 775

© Strategy of Things, 2025. All rights reserved.

allocation of network resources. Areas of further research include slice management and orchestration, security and adaptive service function chaining.

- **Cyber and physical security.** Smart city and IoT devices, network infrastructure, edge servers and core infrastructure are vulnerable to cybersecurity attacks. Research is needed in network security, authentication and access control to develop new and more effective countermeasures. Some areas of research include the use of Software Defined Networks (SDN) and Network Function Virtualization (NFV) for traffic management to enable secure networking. Lightweight authentication, certificateless public key cryptosystem-based authentication and blockchain based methods that work with the limited computational resources of edge servers are other areas of research. Finally, access control methods, such as attribute based and federated capability-based approaches warrant additional research.

17.3.2. Other challenges

In addition to the technology challenges for further consideration, our research identified other challenges that impact IoT adoption. These challenges did not meet the criteria for research consideration because they were either not a technology challenge or a technology related challenge that can be addressed by current marketplace offerings or capabilities.

17.3.2.1. Lack of funding

There is no one source of funding for smart city initiatives. Funding can come from city budgets, bonds, grants, municipal advertising, consortiums and public private partnerships (PPP).[777] Each source, however, has its challenges. For example:

- Grants from regional, state and federal agencies are often limited in size, scope and area of focus. In most cases, they offer a one-time source of funding for a particular initiative but do not address the larger costs of scaling and operating the smart city initiative.
- PPPs provide a significantly larger amount of funding and resources, but are more complex to create, manage and operate. They bring additional complexity, in areas such as staffing and expertise, roles and responsibilities, ownership, operating models along with funding sustainability, regulations and liability.

One of the challenges facing cities and municipalities is a lack of funding to procure and sustain IoT solutions. A 2018 survey of 51 cities published by The U.S. Conference of Mayors reported the top two challenges hindering smart cities are a lack of funding to start the project and financial resources to sustain the project over time.[778]

The Federation of American Scientists has identified the" lack of discretionary funds sufficient to make upfront, multi-year investments" as a challenge facing smart city initiatives. Smart city pilot projects are funded from "whatever untapped pool of money happens to be available"

[777] "US Ignite Smart City Funding Strategies," U.S. Ignite Funding Strategies Playbook, 2018. Link

[778] See note 729. P. 25.

© Strategy of Things, 2025. All rights reserved.

though the amount of money, $50,000 to $250,000, is often insufficient for the initiative to scale beyond the pilot.[779]

In a survey of 100 national state and government leaders 59% of respondents cited insufficient funding as the top barrier to technology modernization.[780] A 2021 RAND study on smart city initiatives reported that city officials were challenged with negotiating agreements with solution providers to sustain projects beyond the pilot phase, specifically around responsibilities for maintaining business ownership of the project and for funding the operations and maintenance.[781]

Deploying and scaling IoT and smart city projects often require modernization of the IT infrastructure. In a survey of 127 local government leaders from mid-sized counties and cities from across the country, more than two-thirds (69%) reported funding was a top challenge.[782]

17.3.2.2. Lack of trust

The lack of trust in IoT technology is a significant barrier that slows the deployment of IoT based applications. This lack of trust is attributed to several factors, including:

- **Privacy.** IoT applications collect data and information about the surrounding environment and may do so without the knowledge and authorization of residents and visitors. Concerns arise when these systems collect Personally Identifiable Information (PII) and monitor activities that may be constitutionally protected.

  For example, video camera systems are used in several smart city applications, from identifying open parking spaces, monitoring traffic conditions and for surveillance. While these systems may collect, store and use PII, how the data are collected and processed may not be in alignment with their intended application. For example, cameras used to detect open parking spaces should not store any video data. While traffic monitoring systems store data for later analysis by engineers, the data should not contain any identifiable information such as images of license plates or people.
- **Cybersecurity breaches**. IoT systems expose new vulnerabilities that can be exploited by cybercriminals to breach a city's network and disrupt its operations. These breaches may expose IoT data, city data and system controls and functionality.

  In other cases, the integration of IoT with utility infrastructure systems may enable cybercriminals to gain access to the control systems. A 2021 study on the cybersecurity risks of smart city technologies reported that Emergency and Security Alert Systems,

[779] "Smart Cities Technologies: Driving Economic Growth and Community Resistance", Nick Maynard, Federation of American Scientists, March 31, 2020. Link

[780] "Government agencies are transforming physical operations to gain efficiency and resilience," Center for Digital Government Research Report, 2023. Link

[781] "Tech Alone Isn't Enough to Create a Successful Smart City", Jared Mondschein, et. al., RAND Corporation, February 10, 2021. Link

[782] "IT infrastructure in mid-sized cities and counties: Moving toward resilience and sustainability," Center for Digital Government Research Report, 2022. Link

© Strategy of Things, 2025. All rights reserved.

Street Video Surveillance and Smart Traffic Lights/Signals were the top three applications that experts assessed as most technically vulnerable. The study also reported that these three applications would have the most impact on city operations in the case of a successful attack. Similarly, these three applications were determined to have the highest interest level of nation-state attackers.[783] A 2022 IBM report estimates that the average total cost of a data breach was $4.82 million for critical infrastructure organizations, including those in the public sector.[784]

- **Unauthorized data sharing and usage.** Regardless of whether the data collected is PII or not, another concern is how the collected data will be used and who it is shared with and the transparency of how that information is used. Cities may partner with private companies, who will pay for all or some of a smart city application in exchange for access to the data. These companies then use the data to develop targeted advertising or other commercial offerings.

  Cities may also anonymize the collected data and sell access to these data so that companies can offer non-personalized advertising and commercial offerings.[785] Trust concerns arise when residents and community members have no means of knowing how their information is used or be able to opt out or revoke consent to their personal data. In another example, many homes and apartments employ doorbell cameras to help homeowners see who is at the door. The video footage captured by these cameras, however, may also be accessed by police to support law enforcement activities.[786] Privacy advocates are concerned that the sharing of the doorbell camera video has enabled police overreach, as "investigators could request footage of legal or even constitutionally protected activity under the guise of investigating a broad set of potential crimes."[787]
- **Improper or inaccurate outcomes.** Facial recognition technologies are useful in preventing and solving crimes. The use of AI in IoT, however, is not perfect and may lead to erroneous results. For example, AI algorithms can yield inaccurate results for certain demographic groups. A study conducted through NIST's Face Recognition Vendor Test program of 189 algorithms from 99 developers found higher rate of false positives for Asian and African American faces compared to Caucasian faces.[788]

  A second example is cars employing Advanced Driver Assistance Systems (ADAS) and

[783] "The cybersecurity risks of smart city technologies. What do the experts think?" K. Trapenberg-Frick, G. Mendonca-Abreu, et al., UC Berkeley Center for Long Term Cybersecurity, February 2021. Link

[784] "Cost of a data breach Report 2022," IBM Security, IBM. 2022. Link

[785] "Balancing privacy and innovation in smart cities and communities," A. Johnson, Information Technology and Innovation Foundation, March 6, 2023. Link

[786] "The privacy loophole in your doorbell," A. Ng, Politico, March 7, 2023. Link

[787] "Ring's police problem never went away. Here's what you still need to know," D. Priest, CNET, September 27, 2021. Link

[788] "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software", NIST news release, December 19, 2019. Link

© Strategy of Things, 2025. All rights reserved.

autonomous driving technologies. The National Highway Traffic Safety Administration (NHTSA) reported 392 crashes in 2021, of which 273 involved cars with ADAS and 130 involving fully autonomous vehicles.[789] While the number is small relative to the 42,915 accidents[790] in 2021, it led to negative perceptions of these cars. A 2021 Pew Research survey found that 63% of Americans would not ride in a driverless vehicle. Moreover, 44% of Americans think that "widespread use of driverless cars would be a bad idea for society" and 45% would not be comfortable sharing the road with driverless cars.[791]

Public trust and community concerns around privacy, equity and safety are key factors in slowing the scaling of IoT in smart city projects. In some instances, government intervention has limited the initiatives. For example, during the time period around 2022, seventeen cities across the United States banned the government use of facial recognition systems. These cities include Boston, New Orleans, Portland (Oregon) and San Francisco.[792] San Diego temporarily shut down its network of 3,000 streetlight mounted cameras until the city developed an ordinance addressing surveillance technology.[793] The California Department of Motor Vehicles suspended the operating license of General Motor's Cruise autonomous vehicle operations after reports of an accident in which one of its cars dragged a pedestrian.[794] The ambitious Google Sidewalk Labs Toronto Quayside smart city project faced significant backlash and opposition from the community over its data collection and usage and privacy practices and concerns, which slowed its progress and ultimately led to its cancellation due to "economic reasons" in 2020.[795]

17.3.2.3. Lack of digital skills

Many cities lack the new digital skill sets and expertise to work with and support IoT and other technologies. A 2019 PwC report cited talent as one of eight challenges in implementing smart cities, identifying lack of trained workforce, shortage of funds for training and an aging workforce.[796]

The 2021 Gartner Digital Transformation Divergence Across Government Sectors Survey reported digital skills gaps as one of the top 5 digital transformation challenges, identified by

---

[789] "Nearly 400 car crashes in 11 months involved automated tech, companies tell regulators," Associated Press, NPR, June 15, 2022. Link

[790] See note 709

[791] "Americans cautious about the deployment of driverless cars," L. Rainie, C. Funk, M. Anderson and A. Tyson, Pew Research Center, March 17, 2022. Link

[792] "The movement to ban government use of face recognition," N. Sheard and A. Schwartz, Electronic Frontier Foundation, May 5, 2022. Link

[793] "Mayor orders San Diego's Smart Streetlights turned off until surveillance ordinance in place," T. Figueroa, The San Diego Union-Tribune, September 9, 2020. Link

[794] "GM's Cruise loses its self-driving license in San Francisco after a robotaxi dragged a person," A. Marshall, Wired. October 24, 2023. Link

[795] "Sidewalk Labs cancels plan to build high-tech neighbourhood in Toronto amid COVID-19," A. Carter and J. Rieti, CBC News, May 7, 2020. Link

[796] "Creating the smart cities of the future," PwC, May 2019. Figure 5. Link

© Strategy of Things, 2025. All rights reserved.

38% of 166 respondents as either a top, second or third ranked challenge.[797] A national survey of 100 state and local government leaders by the Center for Digital Government reported that nearly three-quarters (72%) of respondents are making technology investments to modernize physical operations, half (49%) implementing or planning to implement emerging technologies and over half (56%) citing a lack of IT/data staff or skills as one of the top three barriers to modernization.[798]

Digital skills are needed to support the technologies used in smart cities. The workforce skills gap includes expertise in technical areas, including software development, data science, network security and systems integration. A European Union research study on digital skills cited that the top technical skills most in demand between 2020 and 2027 were data analysis, AI application development, AI implementation, cloud infrastructure, IoT analytics, cloud integration and APIs.[799]In addition to digital skills, a study of eight major U.S. cities cited personnel and business enabling skills are required smart city skillsets.[800]

There are several reasons contributing to the workforce skills gap. A 2022 state and local government workforce survey found that respectively 78% and 69% of agencies had trouble filling engineering roles and information technology roles.[801]

These agencies are receiving fewer qualified applicants than available posted positions. Most survey respondents reported that they were seeing less qualified applicants for engineering (94%) and information technology (73%) positions.[802] Over half (54%) of the survey respondents stated that wage compensation was not competitive with the labor market.[803]

This was consistent with exit surveys of departing employees that showed non-competitive compensation was the main reason for leaving (51%).[804] This was evidenced by the gaps in average salaries between the private and public sectors. Computer and Information Systems Managers earned an average of $167K in the private sector, as compared to $123K in the local government. Similarly, private sector workers in computer and mathematical occupations earned an average of $102K versus $82K for workers in local government.[805]

---

[797] "5 key digital transformation challenges government CIOs must tackle," A. Gupta, Gartner, March 7, 2022. Link

[798] See note 780

[799] "LEADS presents key findings on digital skills for smart cities at Digital for Planet webinar," LEADS Advanced Digital Skills, June 6, 2023. Link

[800] "Future skills, future cities: New foundational skills in smart cities," W. Markow, D. Hughes and M. Walsh, Business Higher Education Forum. 2019. Link

[801] "State and Local Workforce 2022", G. Young, MissionSquare Research Institute, June 2022. Figure 8. Link

[802] See note 801. Figure 9.

[803] See note 801. Figure 21.

[804] See note 801. Figure 24.

[805] "Why local governments struggle to hire tech workers in 5 charts," M. Brady, Smart Cities Dive, November 17, 2022. Link

© Strategy of Things, 2025. All rights reserved.

17.3.2.4. Adoption barriers

A systematic literature review of 169 papers regarding sustainable smart city development identified 63 barriers, organized into 5 categories of social, environment, economy, governance and urban infrastructure.[806] A Gartner study cited organizational silos and risk averse culture as two of the five key digital transformation challenges.[807] Other barriers include government procurement processes and community and political support.

This section focuses on the key major institutional and organizational governance barriers along with social barriers from the wider community. These are:

- Organizational silos
- Risk-averse culture
- Change resistance
- Community and political support

Each of these is discussed below.

- **Organizational Silos.** City operations, governance and budgets are typically segmented with limited communication and interaction between departments or agencies.[808] IoT and smart city projects often require participation from multiple departments and agencies.

  For example, implementing and operating smart parking requires timely and tight collaboration between the parking operations, public works, information technology, sustainability, community affairs, procurement and city management. A 2022 Gartner report cited "siloed strategies and decision making" as the main CIO challenge for implementing digital solutions, identified by 51% of 166 survey respondents.[809]

  In some cities, a cross-functional role of Chief Innovation Officer was created to work across silos, although these positions were often isolated with little decision-making authority.[810]
- **Risk-averse culture.** Cities are hesitant to embrace innovative technologies and policies even if they have the potential for transformational outcomes. For example, they are hesitant to invest in "unproven" IoT technologies, such as LiDAR for traffic management, due to concerns about both reliability and maintenance costs.

  City systems must operate for decades under a variety of conditions. System failures may

[806] "Drivers and Barriers for the development of Smart Sustainable Cities", Luiza Schuch da Azambuja, AMC Digital Library, 2021. Link

[807] See note 797

[808] "Examining Common Barriers to Smart City Implementation", Luis Casado & Eric Rensel, Water Finance & Management, August 21, 2017. Link

[809] See note 797

[810] See note 781

© Strategy of Things, 2025. All rights reserved.

lead to injuries and death and expose the city to financial and legal liability. This risk aversion is driven by a fear of failure and the potential backlash from community or political leaders if the expected outcomes are not achieved. Cities tend to stay with traditional and proven approaches, even if they are less efficient or innovative, rather than taking the risk of implementing untested solutions and incurring higher costs.

Regulatory and bureaucratic hurdles add to this risk aversion. Innovative solutions may undergo lengthy processes to verify compliance with regulations, such as privacy, before they can be procured. Existing procurement processes are not well suited for acquiring new innovative technologies and may cause delays that discourage city officials from exploring innovative solutions.

Finally, many innovative technologies are developed by small and unproven start-ups, adding to the overall investment risk. [811]

- **Change resistance.** IoT and smart city solutions add complexity that slows adoption and integration into a city's operations. For example, IoT creates new innovative business models, such as "IoT as a Service", that may require modification to existing city policies and processes.

  Revenue or data sharing arrangements not only require policy and operational changes but may also require legislative and community review and approval. Smart waste solutions change the way trash bins are emptied but require renegotiation of existing service contracts with waste management companies.

  Smart city solutions may create changes in roles and responsibilities, which may add new work to existing workloads and require negotiations and approval from employee unions. Other solutions require reskilling and skill updates, which may not fit all the workers' objectives.

- **Community and political support.** Community support is essential to the adoption and deployment of IoT and smart city technologies. Some groups like the American Civil Liberties Union (ACLU) are concerned that some technologies can exacerbate racial or economic inequality instead of distributing outcomes fairly and equally.[812]

  For example, facial recognition systems lead to erroneous outcomes for Asian and African American faces.[813] This may lead to false detentions and arrests. Privacy concerns have led the city of San Diego to shut down its citywide network of cameras temporarily in 2020.[814]

---

[811] "Smart Cities as Large Technological Systems: Collective Action Problems as Organizational Barriers to Urban Digital Transformation", Jared Mondschein, et. al., RAND Corporation, SSRN, December 15, 2020. Link

[812] "Making Smart Decisions about Smart Cities", Chris Conley, ACLU, November 2017. Link

[813] See note 788

[814] See note 793

© Strategy of Things, 2025. All rights reserved.

In addition, IoT and smart city initiatives that are not aligned to current city and community priorities will lead to questions on the spending of public funds for projects that are lower priority compared to other community needs.[815] As a result, cities are shifting away from a "technology arms race" to prioritizing the needs of the community first.[816]

[815] "Smart Cities as Large Technological Systems: Collective Action Problems as Organizational Barriers to Urban Digital Transformation", Jared Mondschein, et. al., RAND Corporation, SSRN, December 15, 2020. Link

[816] "Smart city evolution: How cities have stepped back from a 'tech arms race'," D. McLean, M. Rachal, D. Zukowski, Smart Cities Dive, November 9, 2021. Link

© Strategy of Things, 2025. All rights reserved.

Appendix: Transportation and Logistics

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

© Strategy of Things, 2025. All rights reserved.

18. Appendix: Transportation and Logistics

This section describes the research findings for IoT technology infrastructure in the U.S. transport and logistics industry. The topics discussed here include:

- Industry overview
- Use of IoT in transportation and logistics
- IoT challenges in transportation and logistics

18.1. Industry overview

Transportation and logistics facilitate both communication and commerce. A pervasive transportation and logistics network has helped transform the geographic expanse of the United States into an integrated single market.

A transportation and logistics network are a necessary prior condition to allow trade to be managed on a regular basis and provide a mechanism for markets where goods can be sold or exchanged.

18.1.1. Key facts

The transportation and warehouse industry created $721.3 billion[817] dollars of value in Q1 2022, representing 2.96% of the national GDP. Transportation services, defined as for hire, in-house and household transportation service across other industries, offer another measure of the transportation industry's contribution to the U.S. economy. In 2020, transportation services created $1.16 trillion of value to the GDP.[818]

The largest subsectors within the transportation and warehousing are truck transport ($207.3 B, 28.7% of total transportation GDP), other transportation and support activities ($185.1 B, 25.7%), warehousing and storage ($94.1 B, 13%) and air transportation ($90.6 B, 12.6%).[819]

In 2020, the transportation and logistics industry moved 2.29 billion tons of freight, equal to $3.67 trillion within the United States. This number is projected to grow to 2.907 billion tons and $4.87 trillion by 2030.[820] The modes of freight transportation include truck, rail, air, water, multiple modes and mail and pipeline. The top three modes of freight transportation are truck transportation (918.5 million tons), pipelines (444.9 million tons) and rail (392 million tons) in

[817] Bureau of Economic Analysis. Link

[818] "Contribution of Transportation Services to the Economy and the Transportation Satellite Accounts", Transportation Economic Trends, Bureau of Transportation Statistics. Link

[819] Bureau of Economic Analysis. Link

[820] "Domestic Transportation Mode of Exports and Imports by Tonnage and Value", Bureau of Transportation Statistics, March 31, 2022. Link

© Strategy of Things, 2025. All rights reserved.

2020.[821] By value, the top modes of freight transportation are truck transportation ($2.29 trillion), air ($0.468 trillion) and multiple modes and mail ($0.311 trillion) in 2020.[822]

The U.S. transportation and warehousing industry is a major employer of Americans. The U.S. transportation and warehousing industry employed 5.71 million people in 2020. The three sectors employing the most Americans in 2020 are truck transportation (1.624 million), warehousing and storage (1.141 million) and couriers and messengers (961.3 K). Most of the workers in the industry were employed at firms with less than 500 people (3.826 million, or 67%). There were 1.48 million (26%) of workers employed at firms with less than 50 people and 433,921 (7.6%) people employed at firms with less than 10 people.[823]

The industry created $292.4 B in total labor income, with $84.5 B (28.9%) coming from truck transportation, $52.8 B (18%) from warehousing and storage and $42.7 B (14.6%) from air transportation.[824]

There were 257,785 transportation and warehousing businesses in the United States in 2020. Of this, 256,308 or 99.4% were small businesses employing 499 people or less. 189,479 or 73.5% were small businesses employing less than 10 people[825] and a small portion, 1477 firms or 0.5%, that employ 500 people or more, employ 33% or 1.23 million people.[826]

18.1.2. Industry challenges

The transportation industry in the United States faces several challenges that constrain the growth of the industry. Five key challenges, which are relevant to the Internet of Things in transport are:

- Supply chain resilience
- Aging Infrastructure
- Environment and sustainability
- Labor shortages
- Fuel costs

Each of these is discussed below.

18.1.2.1. Supply chain resilience

The pandemic has highlighted the importance of supply chain resilience. Resilience is the ability of a supply chain to “prepare for and adapt to unexpected events; to quickly adjust to sudden disruptive changes that negatively affect supply chain performance; to continue functioning

[821] ibid.

[822] ibid, in 2017 dollars

[823] U.S. Census Bureau, 2000, CBP Tables 2020. Link

[824] ibid.

[825] ibid.

[826] ibid.

© Strategy of Things, 2025. All rights reserved.

during a disruption; and to recover quickly to its pre-disruption state or a more desirable state."[827]

The COVID-19 pandemic disrupted supply chains and economies around the world. Public health orders required many businesses, factories and schools to limit occupancy and in some cases to close for in-person activities. Demand for discretionary goods dropped while demand for essential goods soared almost overnight. Inventory shortages were common as factories lacked the raw materials, equipment and personnel to produce the goods needed to meet demand. For example, semiconductor shortages resulted in a 21% year-on-year drop in U.S. new car sales[828] as a modern car uses as many as 3,000 semiconductor chips.[829]

Supply chain disruptions are caused by a variety of factors, including:[830]

- Natural catastrophes and calamities, such as hurricanes, earthquakes, floods, that impact infrastructure and disrupt travel.
- Political events, such as wars, coups and trade disputes.
- Transportation issues, such as traffic congestion, accidents and poor weather.
- Supplier challenges, such as poor quality, labor disputes and labor shortages.

According to the Gartner Emerging Risks Monitor Report, supply chain disruptions are one of the top five risks, cited by 73% of the 254 global senior business executives surveyed in Q4 2021.[831] Supply chain disruptions are common, with 56% of companies globally suffering a disruption annually.[832]

In a survey of 750 companies with annual revenues between $500 million and $50 billion, supply chain risk management company Interos reported that the disruptions caused $182 million and $82 million in financial losses per company in 2021 and 2022, respectively.[833]

According to the 2020 Global Data Supply Chain Vulnerability Index, the United States has been identified as having the most vulnerable supply chain in the world as shown below in Figure

[827] "How to Build More Secure, Resilient, Next-Gen U.S. Supply Chains," E. Iakovou and C. White III, Brookings, December 3, 2020. Link

[828] "Car Sales Dampened By Chip Shortage, COVID Measures," Z. Yan, B. Goh, V. Waldersee. Reuters, May 26, 2022. Link

[829] "A Tiny Part's Big Ripple: Global Chip Shortage Hobbles the Auto Industry," J. Ewing and N. Boudette, New York Times, April 23, 2021. Link

[830] "An Insight Into Supply Chain Disruptions," DFreight webpage, February 6, 2023. Link

[831] "Poor Talent Strategy Surpasses Supply Chain Disruption As Top Worry," Material Handling and Logistics, February 8, 2022. Link

[832] "Supply Chain Disruptions and Resilience: A Major Review and Future Research Agenda," K. Katsaliaki, P. Galetsi & S. Kumar, Ann Oper Res 319, 965–1002 (2022). Link

[833] "Costs From Supply Chain Disruptions Drop By Over 50% But Headwinds Remain," A. Lampert, Reuters, August 9, 2023. Link

© Strategy of Things, 2025. All rights reserved.

18-1 below.[834] Some factors that contribute to this assessment include America's reliance on countries like China for production and supply chain issues in transportation and warehousing.[835]

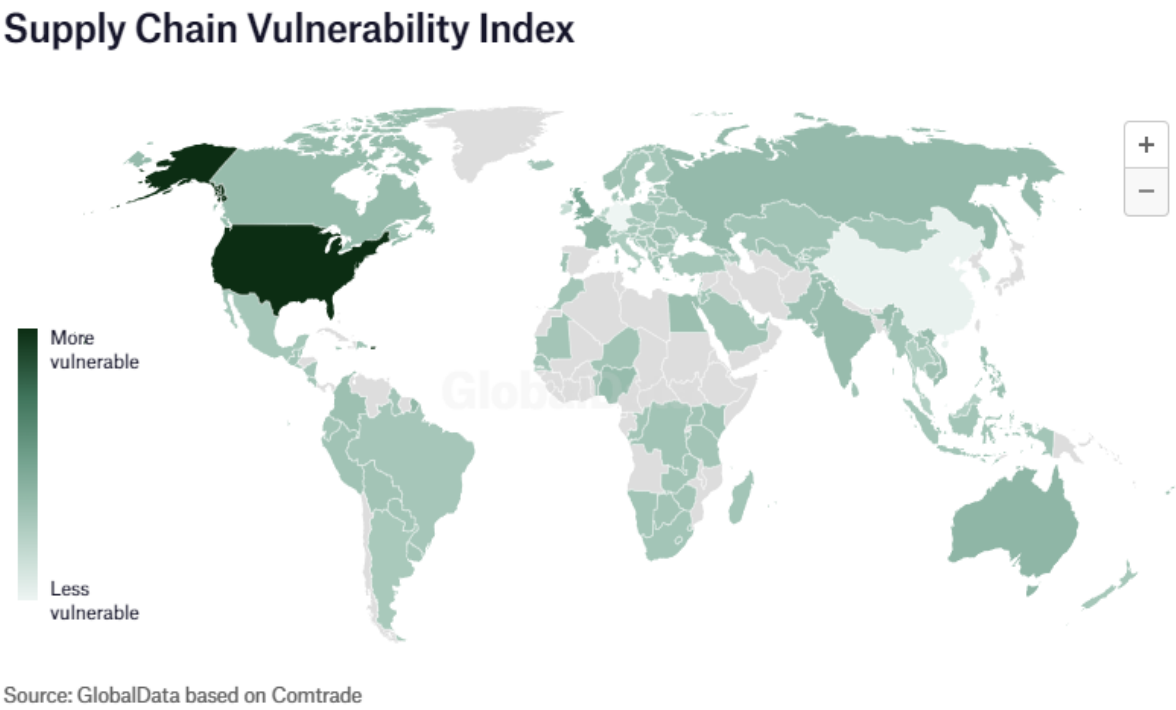


Figure 18-1: Transport and Logistics: Global Supply Chain Vulnerability Index (2020)

Supply chain resilience is a priority for the United States government. To facilitate economic security, national security and job creation, President Biden issued Executive Order (E.O) 14017 on February 24, 2021, "directing a whole-of-government approach to assessing vulnerabilities in and strengthening the resilience of critical supply chains."[836] The executive order focused on four priority product areas during its first 100 days including:[837]

- Semiconductor manufacturing and advanced packaging
- Large capacity batteries
- Critical minerals and materials

[834] "Supply Chain Vulnerability Index Shows Wide Gulf Between U.S. and China," V. Caon, Investment Monitor, February 10, 2022. Link

[835] ibid.

[836] "FACT SHEET: Biden-Harris Administration Announces Supply Chain Disruptions Task Force to Address Short-Term Supply Chain Discontinuities," The White House, June 8, 2021. Link

[837] "Building Resilient Supply Chains, Revitalizing American Manufacturing and Foster Broad-Based Growth. 100 Day Reviews Under Executive Order 14017," White House Report, June 2021. Pages 8-9. Link

© Strategy of Things, 2025. All rights reserved.

- Pharmaceuticals and active pharmaceutical ingredients

Within the four priority areas, the report generated by E.O. 14017 identified the following drivers of supply chain vulnerability, including:[838]

- Insufficient U.S. manufacturing capacity
- Misaligned incentives and short-termism in private markets
- Industrial policies adopted by allied, partner and competitor nations
- Geographic concentration in global sourcing
- Limited international coordination

Underscoring the importance of supply chain resilience, the report recommended the establishment of a Supply Chain Resilience Program. Specifically,

> *We recommend that Congress enact the proposed Supply Chain Resilience Program at the Department of Commerce, to monitor, analyze and forecast supply chain vulnerabilities and partner with industry, labor and other stakeholders to strengthen resilience. We recommend Congress back this program with $50 billion in funding that will give the federal government the tools necessary to make transformative investments in strengthening U.S. supply chains across a range of critical products.*[839]

Other recommendations in the report include:[840]

- Rebuilding U.S. production and innovation capabilities
- Supporting the development of markets with high road production models, labor standards and product quality
- Leveraging the government's role as a market actor
- Strengthening international trade rules, including trade enforcement mechanisms
- Collaborating with allies and partners to decrease vulnerabilities in the global supply chains
- Partnering with industry to take immediate action to address existing shortages.

[838] ibid. Page 10-12

[839] ibid. Page 13

[840] ibid. Page 12-17

© Strategy of Things, 2025. All rights reserved.

18.1.2.2. Aging Infrastructure

The World Economic Forum now ranks the United States 13th in overall quality of infrastructure.[841] The Council on Foreign Relations indicates that U.S. infrastructure is both overstretched and lagging that of its economic competitors, particularly China.[842]

The economic impact of underinvestment in infrastructure is significant. By continuing current under-investment trends, the U.S. GDP could lose more than $10.3 trillion by 2039.[843] For example:

> *The closure of the I-40 bridge, which typically carries more than 40,000 vehicles per day, caused a massive disruption in the flow of people and goods. The more than 12,000 trucks that cross it daily saw their average transit time increase from eight minutes to 76 minutes, costing the industry $2.4 million for every day the bridge was closed. By the time it reopened on July 31, a few feet of cracked steel on a public bridge had directly cost the U.S. trucking industry upwards of $200 million.*[844]

Today, this infrastructure requires repair and upgrade to maintain American economic competitiveness. The American Society of Civil Engineers, in its 2021 report card for America's infrastructure, provided an overall grade of "C minus." For example:

- 43% of the four million miles of public roadways and bridges are in poor or mediocre condition. Every day, 178 million trips are taken across these structurally deficient bridges.
- There are 12,000 miles of navigable waterways that make up the U.S. freight network's "water highway." There is a $6.8 billion backlog in construction projects and 5,000 hours of lock closures between 2015 and 2019.
- There are 140,000 miles of freight rail in the United States, carrying 1.7 million ton-miles of freight per day. While private railroads reinvest approximately 20% of their operating revenue into rail infrastructure, the 606 short line and regional railroads which partner with the seven national railroads to provide the first and last mile delivery, reports a $10 billion shortfall for state of good repair projects needed to retain strong connection to the national (Class I) network.[845]

---

[841] "Modernizing U.S. Infrastructure:The Bipartisan Infrastructure Law," The White House, November 15, 2021. Link

[842] "The State of U.S. Infrastructure," J. McBride, N. Berman, A. Siripurapu, Council on Foreign Relations, September 20, 2023. Link

[843] "America's Aging Infrastructure Needs Our Support," E. Feenstra, Harvard Advanced Leadership Initiative Social Impact Review, June 30, 2021. Link

[844] "Bipartisan Infrastructure Bill is A Win for American Truckers and the U.S. Supply Chain," C. Spear, American Trucking Associations, September 12, 2021. Link

[845] Report Card for America's Infrastructure 2021, American Society of Civil Engineers. Link

© Strategy of Things, 2025. All rights reserved.

The poor state of the infrastructure leads to the short-term closure of roads and waterways for repairs or unplanned maintenance, circuitous detours and alternate routes and transport methods, unplanned congestion, slower traffic speeds and increased wear and tear and fuel use. In addition, some rural roads are unable to accommodate modern trucks and equipment. All of this combines to create delays, increase unpredictability and variability and force use of less optimal routes and methods that increase fuel usage.

Americans experience the poor condition of the infrastructure daily. For example, the American Trucking Associations estimates that each year, "Poor road conditions and congestion cost the typical motorist $1,600 in lost time, lost wages and vehicle repairs." [846]

Overall, traffic congestion costs the United States $305 billion in 2017.[847] The American Transportation Research Institute estimates that congestion costs the U.S. freight sector $74.1 billion annually, $66.1 billion of which occurs in urban areas.[848] The cost of subpar road infrastructure is estimated to increase annual truck fuel consumption by 13%.[849]

18.1.2.3. Environmental Sustainability

Environmental sustainability is a major issue for the transportation and logistics industry. In 2015, the U.S. logistics industry moved more than 49.5 million tons of goods worth $52.7 billion every day and in the process consumed over a billion barrels of oil.[850] Furthermore, the movement of this freight is a major contributor to air pollution in the United States and is responsible for:[851]

- Over 50% of nitrogen oxide (NOx) total emissions
- Over 30% of Volatile Organic Compound (VOC) emissions
- Over 20% of the particulate matter (PM) emissions

Similarly, maritime shipping of freight is responsible for 2 to 3% of global carbon dioxide (CO_2) emissions and could rise to as much as 17% by 2050.[852] In addition to contributing to air pollution, shipping creates noise pollution, contaminates water through vessel discharges such as oil, bilge water, black and gray water adds to port congestion and can introduce invasive marine species through ballast water discharges.[853]

---

[846] "A Blueprint for Smart Infrastructure Investment," American Trucking Associations, March 1, 2021. Link

[847] "The Economic Toll of Traffic and How New Technologies Can Help," Applied Information. April 25, 2019. Link

[848] "Congestion Costs U.S. Cities Billions Every Year," N. McCarthy, Statista, March 11, 2020. Link

[849] See note 846

[850] "Why Freight Matters to Supply Chain Sustainability," U.S. Environmental Protection Agency. Link

[851] ibid.

[852] "What Are Five Environmental Impacts Related to Shipping?" Sinay Maritime Data Solution. Link

[853] ibid.

© Strategy of Things, 2025. All rights reserved.

The U.S. government is taking a "whole of government" approach to address the growing environmental impact of transportation. For example, the U.S. Environmental Protection Agency (EPA), through its SmartWay program, provides shippers and carriers with tools and support to transport freight in the "cleanest, most energy-efficient way possible." Since 2004, SmartWay has avoided the emission of 152 million metric tons of CO_2, 2.7 million short tons of NO_x, 112,000 short tons of PM and saved 357 million barrels of oil.[854]

The Department of Transportation is supporting efforts to meet the President's climate commitments to ensure a 50 to 52% reduction in U.S. emissions by 2030 and a net-zero economy by 2050.[855] One such way is by "supporting innovative programs, policies and projects to reduce environmental impacts associated with freight movements."[856] Finally, the Departments of Energy, Transportation and Housing and Urban Development and the Environmental Protection Agency have jointly developed the U.S. National Blueprint for Transportation Decarbonization, which "offers a whole-of-government approach to addressing the climate crisis and meeting President Biden's goals of a 100% clean electrical grid by 2035 and the 2050 net-zero carbon emissions."[857]

A 2021 survey of 593 small and midsize trucking companies, conducted by digital freight network Convoy, found that nearly two-thirds (64.6%) stated that climate change will have a large or some impact on the trucking industry.[858] One-third (34.9%) felt pressure to reduce carbon emissions in their business. The main reasons for doing so were "more awareness of the environmental impact" (24%) and government regulation (19%). Only 20.3%, however, agreed or strongly agreed that stricter environmental laws and regulations are worth the cost, while over one-third (35.9%) disagreed or strongly disagreed. Nearly one-third agreed or strongly agreed that stricter environmental laws and regulations cost too many jobs and hurt the economy.

There are several challenges the transportation and logistics industry faces in supporting environmental sustainability. These include:

- **Investment and cost considerations.** Implementing technologies and practices that optimize routes, reduce empty miles and improve fuel efficiency contribute to environmental sustainability, but requires upfront operational changes and investments. One survey found that while a majority (92.4%) of the freight carriers stated that fuel economy was important or very important,[859] over half (57%) indicated that class 8 fuel economy standards would moderately or substantially increase their costs.[860] Before Class 8 fuel economy standards in 2011, truck prices increased an average of $2,100 a

[854] "SmartWay Program Highlights for 2022," EPA-420-F-23-007, U.S. Environmental Protection Agency, January 2023. Link

[855] "Climate Action," U.S. Department of Transportation, January 13, 2023. Link

[856] ibid.

[857] "The U.S. National Blueprint for Transportation Decarbonization: A Joint Strategy to Transform Transportation," Office of Energy Efficiency and Renewable Energy, U.S. Department of Energy, January 2023. Link

[858] "Sustainability In Trucking Snapshot Report," Convoy, August 2021. Link

[859] See note 858 Page 13

[860] See note 858 Page 14

© Strategy of Things, 2025. All rights reserved.

year. After 2011, average price increases rose to $2,500 a year.[861]

Similarly, while electric trucks produce zero emissions, their high vehicle purchase prices are one of the largest barriers to freight electrification.[862] In an industry survey, 55.9% of 593 respondents reported that cost is the top barrier to purchasing electric trucks.[863]

Individual businesses face increased upfront costs for purchasing ZE trucks. Today, battery electric trucks cost 15-125% more than a diesel truck.[864]

- **Lack of infrastructure.** The industry is built around an infrastructure based on gasoline and diesel. Transitioning to cleaner and more sustainable energy sources, such as electrification or alternative fuels, requires significant investments in infrastructure, technology and vehicle fleets. For example, one survey reported that distance limits (40.5% of 593 respondents) and lack of infrastructure (35.8%) were two of the top three barriers to purchasing electric trucks. [865]

  "*Refueling/charging infrastructure (especially high-power charging) and power delivery at charging stations is currently insufficient. Because of the high power needs and uncertain utilization, the private business case is not compelling. There is no common standard for refueling/charging infrastructure. Additional obstacles include: Uncertain impacts on the grid; uncertainty regarding ideal location for new infrastructure and availability of land/ space to match charging demand with grid capacity; high costs of charging infrastructure; unfamiliarity with infrastructure. Low utilization rates and uncertainty on how costs are split among parties disincentivize infrastructure construction. There are long lead times for infrastructure, especially in urban areas. Additionally, soft costs of permitting, standardization, utility approvals are highly variable.*[866]

- **Regulatory compliance.** Adapting to evolving environmental regulations and compliance requirements poses challenges for the industry. Compliance with emission standards, fuel efficiency regulations and reporting obligations require resources, investments in technology and changes in operational practices. Staying up to date with changing regulations and ensuring compliance across different jurisdictions can be complex, particularly for businesses operating across state or international borders.

---

[861] "US Truck Fuel Efficiency Standards: Costs and Benefits Compared," Transport and Environment, January 2018. Link

[862] "Electrifying Freight: Pathways to Accelerating the Transition," T. Buholtz et al., Electrification Coalition, November 2020. Page 5. Link

[863] See note 858 Page 15.

[864] "Zero Emission Road Freight Strategy 2020 - 2025," Hovland Consulting LLC, William and Flora Hewlett Foundation, April 1, 2020. Table 1. Link

[865] See note 858 Page 15

[866] See note 864 Table 1

© Strategy of Things, 2025. All rights reserved.

- **Industry Fragmentation**: The transportation and freight industry consist of numerous stakeholders, including carriers, shippers, logistics providers and regulatory bodies across the supply chain. Aligning diverse interests and coordinating efforts across the supply chain to drive sustainability can be challenging. Collaborative approaches and industry-wide initiatives are necessary to overcome fragmentation and drive systemic changes.

18.1.2.4. Driver shortages

71% of freight is transported by trucks across the United States[867] and the industry has a driver shortage. The Minnesota Trucking Association estimates the country has a shortage of 60,000 drivers in 2021. This is due to longtime recruitment issues, early retirement and COVID-canceled driving-school classes.[868] The American Trucking Associations (ATA) estimated that there was a shortage of 80,000 drivers in 2021 and there will be a shortage of 160,000 drivers by 2030.[869] In addition, the ATA estimated that the transportation industry would need to recruit one million new drivers to accommodate industry growth, replace retiring drivers and drivers who leave the industry.[870]

In its survey of over 4,200 industry stakeholders in 2022, the American Transportation Research Institute (ATRI) reported that driver shortages were the number two industry issue, eclipsed only by high fuel prices. This concern was identified by one-fifth (21.4%) of the respondents.[871] Prior to 2022, driver shortage was identified as the main issue every year for the previous five years, starting in 2017.[872] Among respondents identifying as motor carriers in the survey, driver shortage and driver retention were the number one and two industry issues, respectively.[873]

> *... when anticipated driver retirement numbers are combined with the expected growth in freight demand, the industry will need to hire roughly 1.1 million new drivers over the next decade, or an average of nearly 110,000 per year.*[874]

Driver compensation is a consideration in addressing driver retention and shortages. The ATRI survey reported that compensation was ranked as the fourth most important industry concern, behind fuel prices, driver shortage and truck parking. This concern was identified by nearly one-

---

[867] "There is a Massive Trucker Shortage Causing Supply Chain Disruptions and High Inflation," J. Kelly, Forbes, January 12, 2022. Link

[868] "Global Supply Chain Chaos: Trucking Industry May Be Hit Hardest," J. Hoff, WCNC, September 29, 2021. Link

[869] "Driver shortage Update 2021," American Trucking Associations, Inc., October 25, 2021. Link

[870] ibid.

[871] "Critical Issues in the Trucking Industry – 2022," The American Transportation Research Institute, October 2022. Page 6. Link

[872] ibid. Table 4.

[873] ibid. Table 2.

[874] "Failing Infrastructure Threatens the U.S. Supply Chain," American Trucking Associations blog, May 12, 2021. Link

© Strategy of Things, 2025. All rights reserved.

fifth of the respondents (19.2%).[875] Since 2018, driver compensation has been a recurring top three concern.[876] Driver compensation was the top concern among respondents identifying as commercial drivers.[877] Similarly, driver compensation was the number one and three concerns for survey respondents identifying as company drivers and owner-operators/independent contractors, respectively.[878]

> *…While compensation is not the only factor truck drivers consider when looking to join the industry or change employers, it does remain an important consideration for drivers. Separate ATRI research found that compensation was a top motivating factor, with 83.1 percent of company drivers and 90.4 percent of owner-operators / independent contractors listing income as an important / very important motivating factor for why they chose a career in trucking.*[879]

There is no single cause of the driver shortage. The ATA cited reasons, including[880]:

- High average age of current drivers with 30.3% of drivers are over 55.[881]
- Small number of women drivers (7%), well below representation levels in total workforce.
- Inability of prospective and current drivers to pass a drug test.
- Federally mandated minimum age of 21 to drive a truck.
- Leaving the industry due to the pandemic.
- Truck driving training schools training fewer than normal number of students.
- Lifestyle issues, including being away from home for long haul drivers.
- Infrastructure issues, including lack of truck parking spots.
- Inability of potential drivers to meet hiring standards based on driving record or criminal history.

This shortage of drivers has an impact across the U.S. economy. For example, the costs of transporting goods rise as demand for trucking and freight services exceeds the supply of available drivers. Supply chains are disrupted as shipment pickups take longer and goods are delayed in arriving at their destinations. This can result in increased lead times for deliveries, making it challenging for businesses to maintain efficient inventory management and timely

---

[875] See note 871 Page 10

[876] See note 871 Table 4

[877] See note 871 Table 2

[878] See note 871 Table 3

[879] See note 871 Page 10

[880] See note 869

[881] See note 871 Page 6

© Strategy of Things, 2025. All rights reserved.

customer service. Businesses are subject to lost sales and lower profits due to stockouts and the higher cost of inputs.

18.1.2.5. Fuel costs

According to a survey of over 4,200 industry stakeholders conducted by the American Transportation Research Institute (ATRI) in 2022, high fuel prices was the main industry issue. This concern was identified by 27.5% of respondents, who ranked it as one of their top three industry issues.[882] Among independent contractors and truck owner-operators, high fuel prices was ranked as the most important issue ahead of truck parking and driver compensation.[883]

> *ATRI's 2022 Operational Costs of Trucking found year-over-year increases in the fuel cost per mile of over 35 percent, with fleets operating in the west experiencing the highest fuel costs per mile at $0.431. High diesel prices are especially challenging for owner-operators, many of whom operate in the spot market where there is less ability to negotiate fuel surcharges to cover the price volatility. This is now the second year in a row that owner-operator respondents to the survey have ranked fuel prices as their number one concern.*[884]

From the year 2021 to 2022, the price of jet fuel increased by 43.8%, the price of diesel fuel increased by 39.8% and gasoline prices increased by 31.8%.[885] The U.S. Energy Information Administration reported the national average price of diesel set a new all-time-high at the price of $5.75 a gallon in June 2022, costing over $2.40 extra per gallon from a year prior.[886]

The price of gasoline in America also reached a new all-time high in June 2022 at $5.03 a gallon, up from $3.15 per gallon a year prior.

Most businesses depend on supply chains to deliver goods and supplies. Increased fuel prices were the single largest driver of record fleet costs in 2021, at an average of $0.417 cents per mile according to the American Transportation Research Institute.[887] Due to this, many trucking companies must add a fuel surcharge to shipments to account for the increased fuel prices, with reports that less-than-truckload (LTL) carriers are now charging an average 42% fuel surcharge.[888]

Sea transportation has also been impacted by the increased costs of operations and have been adding fuel surcharges to the cost of shipment. Ships have also been slowing down their speed of

---

[882] See note 871 Page 4

[883] See note 871 Table 3

[884] See note 871 p. 4.

[885] "Cost of Transportation: Cost of Fuel", U.S. DOT Bureau of Transportation Statistics, 2023. Link

[886] "Petroleum & Other Liquids", U.S. No 2 Diesel Retail Prices, Monthly, U.S. Energy Information Administration. Link

[887] "High fuel prices push operating costs for trucking to record high: report", Colin, Campbell, Trucking Dive, August 30, 2022. Link

[888] "Freight Rates and Fuel Surcharges", Lorrie Watts, Red Stag Fulfillment. Link

© Strategy of Things, 2025. All rights reserved.

travel to cut down on fuel consumption, a process known as slow steaming.[889] The increased fuel costs have inflated supply chain expenses and have left a domino effect of rising costs for consumers.

Figure 18-2 and Figure 18-3 below shows historical costs of diesel and gasoline.

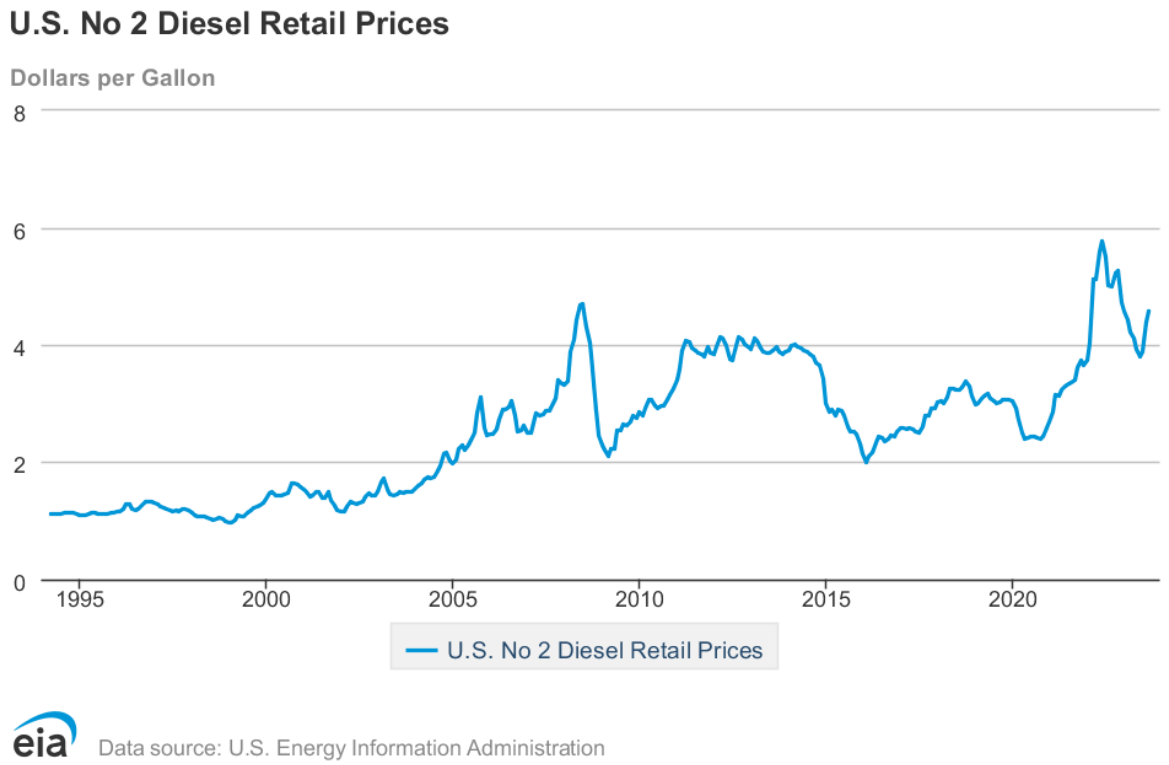


Figure 18-2: Transport and Logistics: Diesel Prices from 1993 – 2023

[889] "The Impact of Rising Fuel Costs on Logistics", Blair Robbins, EisnerAmper, April 5, 2022. Link

© Strategy of Things, 2025. All rights reserved.

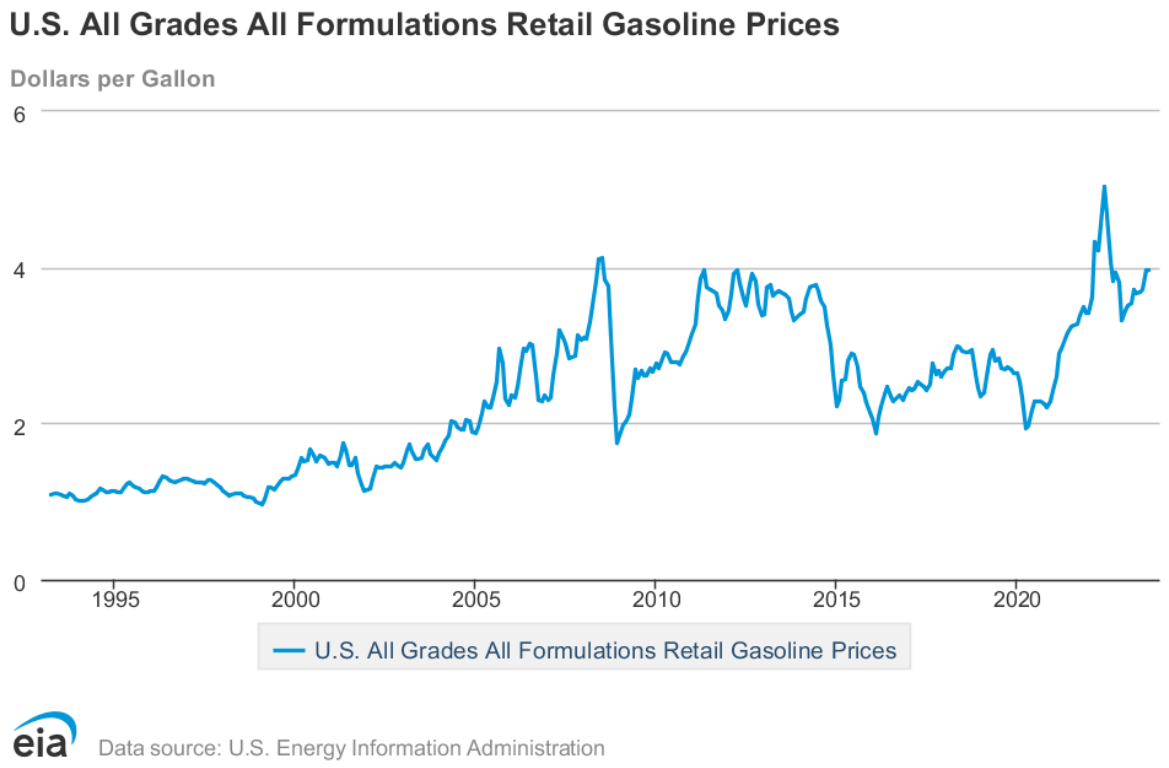


Figure 18-3: Transport and Logistics: Gasoline Prices from 1993 - 2023

18.2. IoT in the transportation and logistics industry

The ability to move and manage material, supplies and inventory from one place to another in a consistent, reliable, timely, cost efficient and safe manner is critical to the health of the national and global economy. The transportation and logistics industry is a critical enabler of the supply chain on which consumers, businesses and organizations rely. This was underscored by the COVID-19 pandemic which disrupted supply chains and the transportation and logistics infrastructures.

A resilient supply chain adapts to a variety of forecasted and unforeseen situations. One common challenge for transportation and logistics companies is accurate Estimated Times of Delivery (ETD).[890] The integration of telematics, GPS and other IoT technologies with fleet management software enables transportation companies to track weather and route conditions, the location of the vehicle and freight and then replan and optimize routes as required to minimize disruptions.

In addition, IoT technologies identify the real time locations and quantities of goods and inventory across a network of warehouses and distribution centers, enabling inventory and logistics planners to draw from the most appropriate locations to minimize disruptions.[891] It is

[890] Current Challenges in the Transportation Logistics Industry, endava, March2022. Link

[891] "How telematics and the IoT work together to improve fleet management," Verizon Connect, June 29, 2021. Link

© Strategy of Things, 2025. All rights reserved.

estimated that over 95 million telematics devices have been shipped worldwide as of 2021 and this is expected to grow at a CAGR of 10.9% reaching nearly 160 million units by 2026.[892] It is also estimated that there are over 130 million units of embedded car OEM telematics units in operation globally as of 2020 and is projected to reach 375 million embedded units by 2026.[893]

In addition to route and freight location information, IoT technologies monitor vehicle status including location, speed, engine performance, driver performance, fuel consumption and other vehicle data to support a variety of fleet management functions. These data are analyzed and used to optimize route planning, monitor operator behaviors for safety and regulatory compliance, track vehicle performance and health and reduce fuel consumption and emissions.[894]

Predictive analytics tools monitor and examine vehicle data to proactively determine if the engine or other components need servicing or repair. This reduces breakdowns and unplanned downtimes, optimizes the scheduling of maintenance technicians and ensures vehicles and equipment continuously operate at optimum performance. The IoT data can be routed to specialty service centers to facilitate complex diagnosis and repairs to support local maintenance centers.

IoT technologies facilitate the monitoring of the freight and inventory in the supply chain. Environmental sensors on freight and cargo can track temperature and humidity levels and monitor defrost cycles to ensuring safety of sensitive freight such as produce, meat, refrigerated foods, vaccines and other pharmaceuticals, which must be thermally controlled during transportation.[895] Out-of-specification conditions are detected early and addressed quickly. This reduces spoilage and damage to the goods as well as ensure safety for the consumers of those goods.

Goods moving along the supply chain typically make one or more stops at terminals, warehouses and distribution centers. At these stops, goods are typically unloaded, moved, stored and reloaded on a truck trailer to be shipped onto the next destination. Tracking sensors, including Radio Frequency Identification (RFID) sensors, help monitor the availability and location of the goods and inventory within warehouses, facilitate movement and improve the accuracy of inventory while reducing manual errors.[896]

IoT technologies can support and facilitate safe operations involved in logistics management. For example, warehouses are potentially dangerous places to work. The National Safety Council reported that Transportation and Warehousing as one of the four most dangerous industries to work in. In 2021, this sector recorded 14.5 deaths per 100,000 workers and 122,700 non-fatal

---

[892] "Outlook on Vehicle Telematics Hardware Global Market to 2026…." Global Newswire, July 15, 2022. Link

[893] "Number of embedded auto telematics units n operation worldwide in 2019 and 2020…", Martin Placek, Statista, March 23, 2023. Link

[894] "Telematics for Fleets: Making Sense of and Cents from Vehicle Data", Intellias, August 28, 2023. Link

[895] "3 Ways IoT Sensors Could Transform Your Fleet", Power Fleet, July 22, 2022. Link

[896] "How RFID is Changing The Future of Logistics and Supply Chain Management?", Nitin Lahoti, Truck Pulse, December 19, 2029. Link

© Strategy of Things, 2025. All rights reserved.

injuries.[897] The four most common injuries include forklift accidents, being hit by objects, caught between objects and slips and falls.[898]

IoT technologies help mitigate and prevent unsafe conditions, such as potential collisions between forklifts and warehouse workers. Motion sensors, ultrasound detectors and wearable IoT sensors alert workers when a forklift enters an area.[899] The use of Automated Guided Vehicles (AGVs) and self-driving forklifts in warehouses allows for inventory items to be moved without human intervention, improving safety, efficiency and reducing labor costs. Other IoT enabled automation technologies include robots that perform repetitive jobs[900] and drones that assist in the counting and tracking of warehouse inventory.[901]

The integration of IoT technologies into transportation and logistics operations has provided the industry with new capabilities and the ability to address a variety of industry challenges. Underscoring the importance of IoT, the global IoT in transportation market size was valued at $83.25 billion in 2020, reached $328 billion by 2023 and is projected to grow to $495.57 billion by 2030, a CAGR of 19.9% from 2021 to 2030 according to a 2022 Allied Market Research report.[902]

18.2.1. IoT use cases

Figure 18-4 shows a representative set of transport use cases organized into five categories. These categories are:

- **Terminals and Ports**: Activities supporting freight and inventory loading and unloading, inspection, clearing customs and transferring from one mode of transport to another.
- **Transport.** Activities supporting the movement of freight. Top transport modes in the U.S. are, in descending order, railroad, truck, pipeline or boat.[903]
- **Maintenance**: Activities supporting maintenance of vehicles, inventory handling equipment and other equipment used to process freight and inventory.
- **Warehousing/Storage**: Activities supporting planning including how much, when and where to store, how to store and handling operations to support the "in" and "out" of storage.
- **Logistics Management**: Activities supporting the planning, control, implementation and management of freights and inventory within the supply chain.

---

[897] "Most dangerous industries, Industry Incidence and Rates", National Safety Council. Compare with 1.4 fatalities per 100,000 in retail. Link

[898] "7 most common warehouse injuries," The Law Office of Matthew E. Russell. Link

[899] "IoT solutions in warehouse management," Hopstack, October 20, 2023. Link

[900] ibid.

[901] "How drones can transform warehouse and inventory management," GEP, May 2, 2023. Link

[902] "IoT in Transportation Market Statistics: 2030", Allied Market Research. Link

[903] "Transportation in the United States", Wikipedia. Link

© Strategy of Things, 2025. All rights reserved.

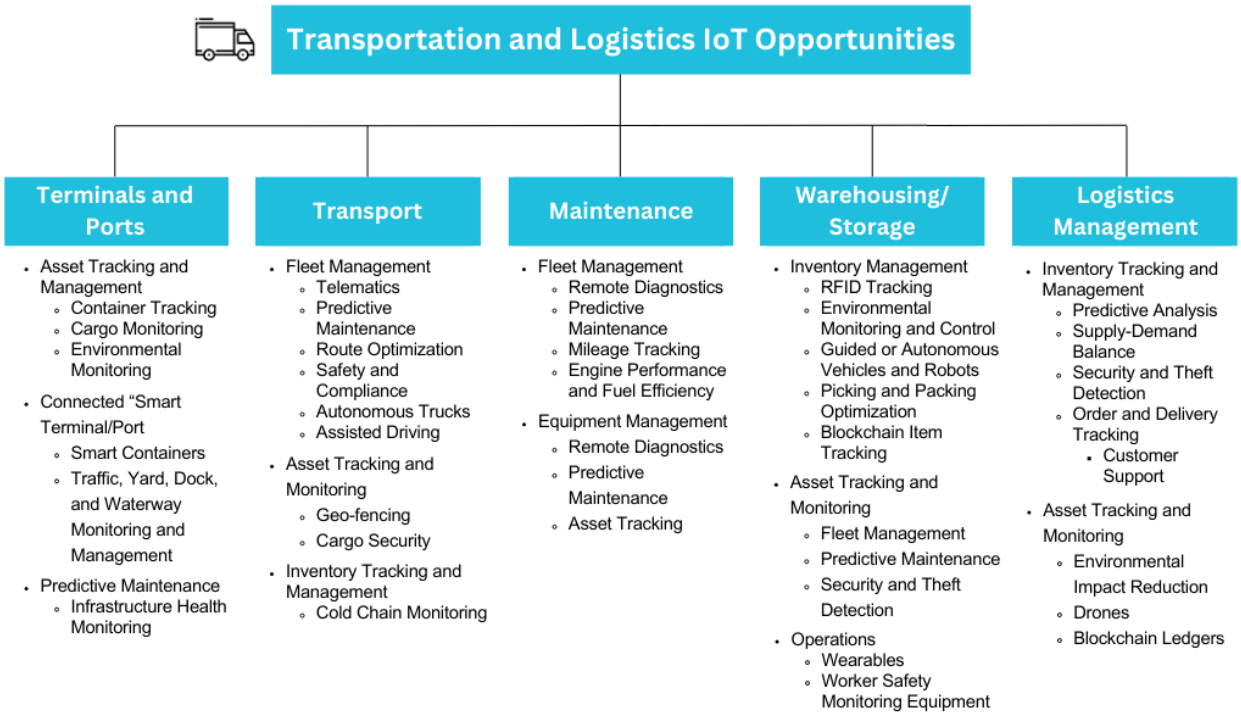


Figure 18-4: Transport and Logistics: Use Case Categories and Selected Use Cases

There are several IoT use cases implemented in the transportation and logistics industry. Three of the most common applications include visibility and tracking, fleet management and supply chain optimizations.

IoT devices incorporate location trackers to provide enhanced visibility and tracking of freight, inventory and physical goods, as well as pallets, containers and transportation vehicles. Sensors can be in the form of RFID or tracking devices, depending on the items to be tracked and the tracking purpose.

For example, RFID is commonly used to track large quantities of individual items such as individual boxes within facilities. GPS trackers are used to track long distance bulk freight such as containers, vehicles and pallets or expensive goods such as machinery and sensitive shipments where real time route tracking is desired. Trackers may also monitor shipment conditions such as temperature and humidity in addition to location.

The increased visibility enabled by IoT facilitates activities around supply chain optimization and management. IoT tracking provides companies with full visibility and control over their supply chains. Real-time data generated by the IoT sensors enables precise tracking of inventory levels, shipment status and environmental conditions throughout the entire logistics process. This granular visibility enables more accurate demand forecasting, improved inventory management and early identification of potential bottlenecks or disruptions. These data and increased visibility facilitate collaboration and communication across the entire network of suppliers, manufacturers, distributors and retailers.

© Strategy of Things, 2025. All rights reserved.

Fleet management applications are a third common IoT use case. IoT sensors are integrated into vehicles to provide real-time monitoring, tracking and optimization of various aspects of vehicle fleet operations. Sensors gather data on factors such as vehicle location, speed, fuel consumption, engine health and driver behavior. These data enable comprehensive insights into fleet performance, allowing for more efficient route planning, proactive maintenance scheduling, fuel cost reduction and enhanced safety measures.

18.2.1.1. Use case and industry challenges alignment

The transportation and logistics industry faces several challenges, some of which are described in Section 18.1.2. Figure 18-5 below shows the fit between the proposed use case subcategories and the documented industry challenges.

© Strategy of Things, 2025. All rights reserved.

Challenge	Role of IoT	Use case examples
Supply Chain Resilience	Facilitate supply chain planning, from demand forecasting, inventory visibility and tracking, to supply replenishment and optimization of transport modes and routes.	• Inventory Tracking • Fleet management • Customer Order and Delivery Tracking • Predictive analytics
Aging Infrastructure	Monitor and track freight shipments during transportation, including optimizing routes and modes to maintain on-time delivery and minimize impacts of delays, congestion and other factors due to poor condition of transportation infrastructure.	• Fleet management • Transportation safety • Predictive Analytics • Telematics
Environment and Sustainability	Monitor and minimize emissions and energy consumption by vehicles and machinery during the transportation and handling of freight and inventory across the supply chain.	• Telematics • Monitoring Environmental Conditions • Engine Performance and Fuel Efficiency • Electric machinery and equipment monitoring • Predictive maintenance of vehicles and equipment
Labor Shortage	Optimize workforce productivity, efficiency and effectiveness through operations planning, task automation, resource optimization and data informed actions. IoT technology helps companies do more with fewer resources and to be more effective doing it.	• Workers' Safety • Robotics • Smart Inventory Management • Autonomous trucks • Robotics

© Strategy of Things, 2025. All rights reserved.

Challenge	Role of IoT	Use case examples
Fuel Costs	Monitor and minimize fuel consumption through data informed actions such as route optimization, load planning and coordination across the supply chain.	• Telematics • Traffic and route optimization management • Fleet management

Figure 18-5: Transport and Logistics: Use Case and Industry Challenges Alignment

18.2.1.2. IoT use case details

Additional details on the use case subcategories shown in Figure 18-4 are provided below in Figure 18-6.

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Definition
Terminals and Ports	Asset Tracking and Management	Monitor and track the location and status of assets, including vehicles, containers, pallets and shipments.
	Connected "Smart" Terminal/Port	A port or terminal incorporating a variety of interconnected IoT technologies to monitor, manage and perform logistics and freight handling operations from container tracking environmental monitoring, robotics and freight or cargo tracking to loading and movement of freight within storage facilities or to transportation vehicles.
	Predictive Maintenance	Monitors key parameters on machinery and equipment. Detects out of spec conditions early and alerts technicians to service equipment before failure.
Transport	Fleet Management	Monitoring and managing a fleet of vehicles or transportation assets. It includes tasks such as managing vehicle utilization, condition, maintenance, optimizing routes and usage and ensuring compliance with regulations.
	Telematics	Monitor driving and vehicle behavior, such as speed, braking and location. Monitor vehicle conditions and performance.
	Autonomous Trucks	Self-driving trucks and vehicles equipped with IoT sensors, 5G and other communication technologies. Transports freight between locations.
	Assisted Driving	Vehicle technologies that provide partial automation or assistance to drivers.
	Asset Tracking and Monitoring	Monitor and track the location and status of assets, including vehicles, containers, pallets and shipments.
	Geofencing	Geo-fencing uses GPS or RFID to create virtual boundaries or zones. It allows fleet managers and operators to monitor, manage and restrict operations within specific areas.

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Definition
	Inventory Tracking and Management	Monitoring, controlling and optimizing inventory of goods, products, or materials with the goal of ensuring inventory levels are maintained at an optimal balance to meet demand while reducing carrying costs and stockout situations.
Maintenance	Predictive Analytics	Using historical IoT and non-IoT data and statistical algorithms to make predictions about future events or outcomes. For example, demand forecasting, maintenance planning or route optimization.
	Fleet Management	Monitoring and managing a fleet of vehicles or transportation assets. It includes tasks such as managing vehicle utilization, condition, maintenance, optimizing routes and usage and ensuring compliance with regulations.
	Remote Diagnostics	Remote monitoring and diagnostics of equipment, machinery and vehicles.
	Predictive Maintenance	Monitors key parameters on machinery and equipment. Detects out of spec conditions early and alerts technicians to service equipment before failure.
	Engine Performance and Fuel Efficiency Monitoring	Monitors key engine parameters that affect engine performance and efficiency. This includes parameters like RPM, fuel consumption and idle conditions.

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Definition
Warehousing/Storage	Inventory Tracking and Management	Monitoring, controlling and optimizing inventory of goods, products, or materials with the goal of ensuring inventory levels are maintained at an optimal balance to meet demand while reducing carrying costs and stockout situations.
	RFID Tracking	Track inventory location using RFID.
	Environmental Monitoring and Control	Use of IoT sensors and devices to monitor and manage temperature and humidity in the supply chain storage facilities and transportation of sensitive goods such as pharmaceuticals and produce.
	Guided or Autonomous Vehicles and Robots	Autonomous or semi-autonomous machines used in transportation or logistics operations to move goods within a warehouse or distribution center or along predefined routes.
	Picking and Packing Optimization	Integration of IoT sensors, devices and data analytics to streamline and improve the various tasks associated with picking and packing items for shipment.
	Asset Tracking and Monitoring	Asset tracking involves using technology such as GPS or RFID to monitor the location and status of valuable assets, including vehicles, containers or equipment. Assets tracking supports fleet managers and can assist with security and theft detection.
	Operations - Wearables	Use of wearable IoT technology to provide real-time data and communications between workers and assets, with uses including asset tracking, worker safety, productivity monitoring, real-time communication, health and safety compliance, health and vital sign monitoring and use of Augmented Reality (AR) to enhance the worker's capabilities.

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Definition
	Worker Safety	IoT sensors, devices and systems are used across warehouses to identify and mitigate potential hazards. Real-time environmental monitoring sensors are used to alert workers of hazardous conditions such as chemical exposure, dangerous air quality or extreme heat or winds.
Logistics Management	Inventory Tracking and Management	Smart inventory management uses technology such as RFID tags or barcode scanners to track inventory levels in real-time and automate inventory-related tasks such as reordering or stocktaking.
	Supply-Demand Balance	Use of IoT to achieve a more precise and efficient equilibrium between the supply of goods and services and demand.
	Security and Theft Detection	Security and theft detection systems help prevent unauthorized access to transportation assets or cargo. They can include surveillance cameras, access control systems, alarms or anti-theft devices.
	Order and Delivery Tracking – Customer Support	Customer order and delivery tracking systems enable businesses to track orders from placement to delivery. These systems provide real-time visibility into order status, location and estimated delivery times
	Asset Tracking and Monitoring	Asset tracking involves using technology such as GPS or RFID to monitor the location and status of valuable assets, including vehicles, containers or equipment. Assets tracking supports fleet managers and can assist with security and theft detection.
	Environmental Impact Reduction	Use of real-time monitoring, data analysis and automation helps shipping companies reduce their environmental impact, lower operating costs and comply with stringent environmental regulations.

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Definition
	Drones	Deployment of unmanned aerial vehicles to gather, monitor, transport and transmit goods and data in a logistics operation.

Figure 18-6: Transport and Logistics: Use Case Details

© Strategy of Things, 2025. All rights reserved.

18.2.2. Market views of IoT in transportation and logistics

To understand market views on IoT and to inform on our gaps discovery and analysis, our research team conducted a survey of 450 people, from adopters to solution providers, across the nine industries studied. Survey respondents were asked their opinion on the importance of IoT for the transportation and logistics industry over the next 5 to 10 years. Figure 18-7 below shows a medium relative expected impact of IoT, as compared to other industries. There are several reasons for this including the reluctance to share data and interoperability which are discussed in the next section.

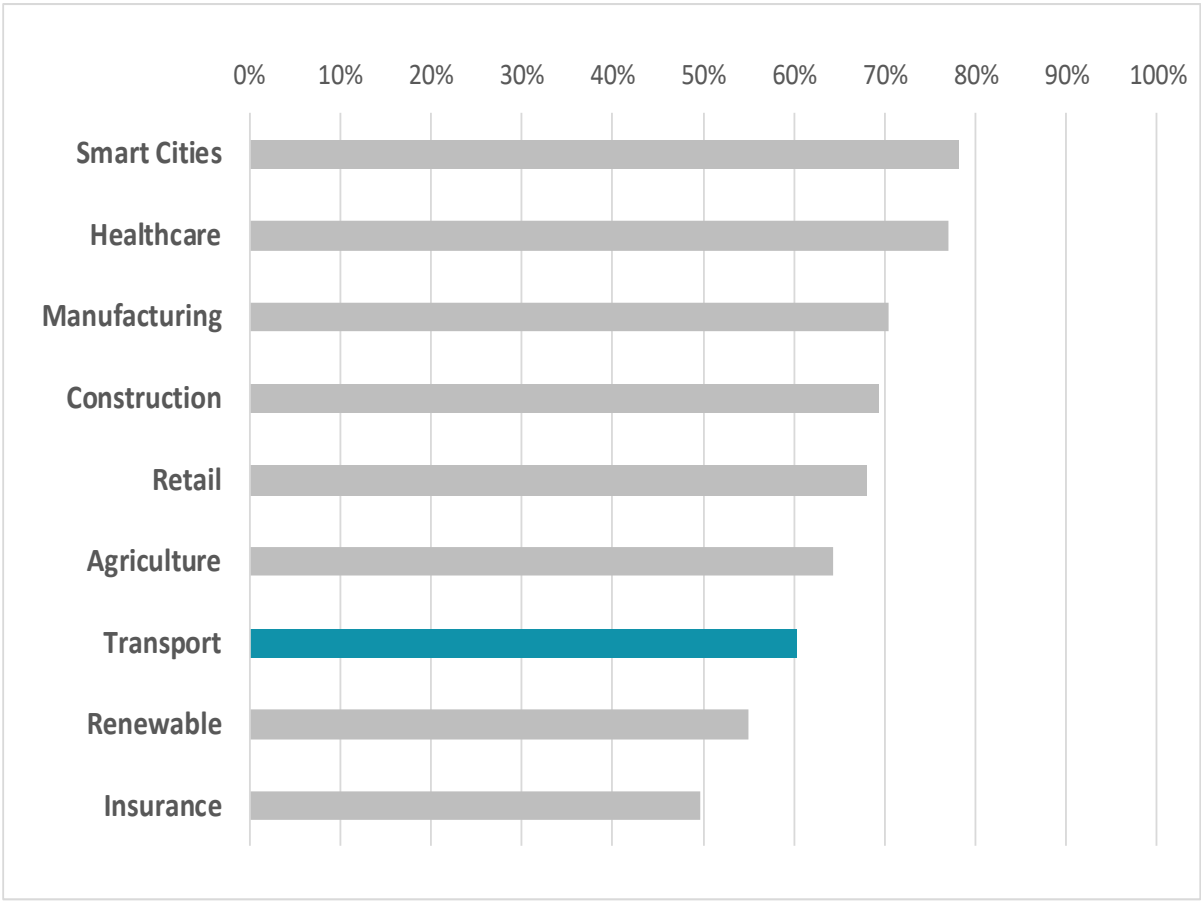


Figure 18-7: Transport and Logistics: Importance of IoT

Survey respondents were asked to rate the impact of these use case categories on the transport industry.[904] Figure 18-8 below shows the percentage of responses in each impact category for each use case category. Overall, this shows a bias to a low impact of the use case categories in transportations and logistics. The highest impact is in the transportation of freight, where shipment tracking is a critical component of supply chain visibility. The perceived low impact in

[904] In your view, what will be the impact of these use cases in transport over the next 5-10 years?

© Strategy of Things, 2025. All rights reserved.

the other categories may be attributed to a lack of awareness and adoption resistance factors. These are discussed in the next section.

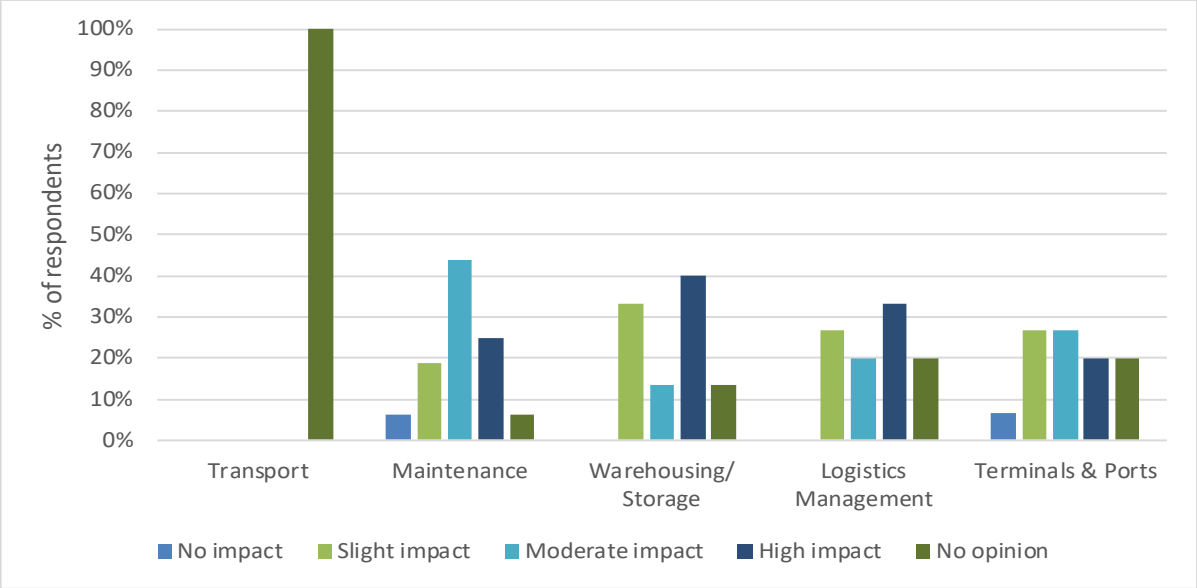


Figure 18-8: Transport and Logistics: Use Case Category Impact[905]

In addition, respondents were asked about their confidence in suppliers delivering the services required to operationalize these use case categories.[906] Figure 18-9 below shows the percentage of responses in each confidence category for each use case category. Overall, their responses indicate some confidence in the ability of suppliers to deliver the necessary services.

[905] Only 3 people responded to the "transport" use case category and each indicated "no opinion."

[906] How confident are you that suppliers will deliver the services that transport organizations need from these technologies over the next 5-10 years?

© Strategy of Things, 2025. All rights reserved.

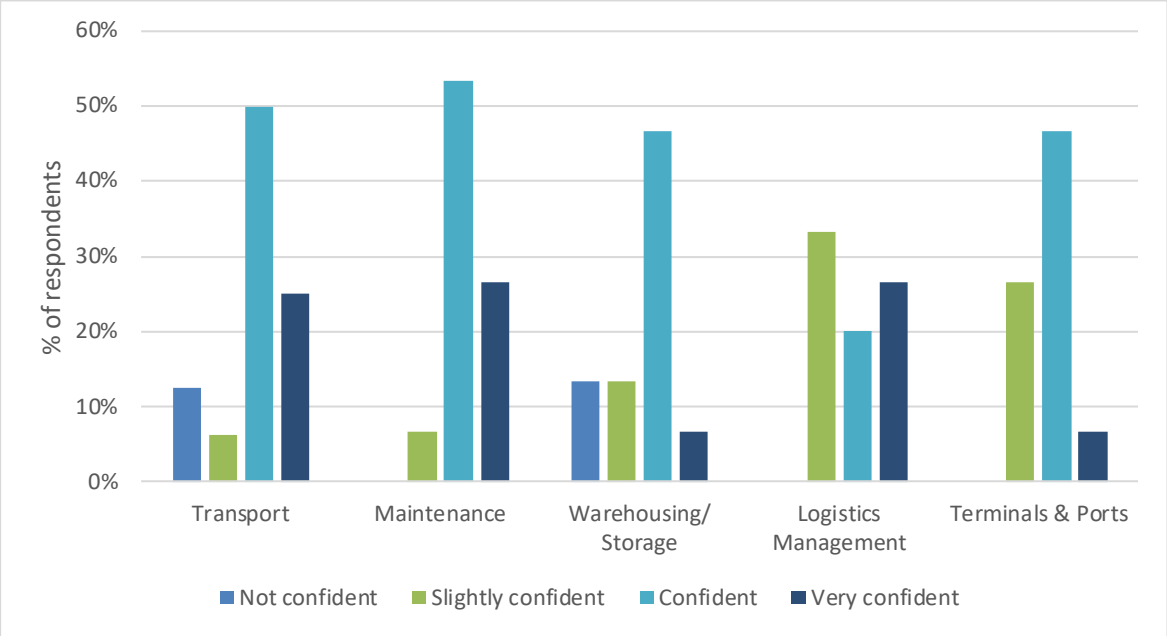


Figure 18-9: Transport and Logistics: Confidence in Suppliers Delivering

18.3. IoT gaps and findings in transportation and logistics

A combination of interviews, secondary research and surveys was conducted to identify and understand the opportunities and challenges to the development and adoption of IoT. Each research method approached the challenges from a different perspective.

For example, the survey targeted a large audience but asked specific questions that supported the economic analysis. The interviews targeted a small number of people who provided deeper insight and context to supplement the information already collected. Finally, the desk research, consisting of a review of online news articles, published research reports, vendor and government white papers, blogs, webinars, videos and other content, provided a broad overview of the application of IoT in the industry.

In our survey, respondents were asked to choose the most important technology areas to operationalize IoT in their industry. Figure 18-10 below shows respondent's selections of the top 10 IoT technologies and the percentage of respondents who chose that technology.[907] The survey results are not seen as a technology gaps list, but rather an indication of what is important to the respondents. This information partially informs the gap selection process.

[907] Respondents were asked to choose up to 5 out of the 25 technologies listed.

© Strategy of Things, 2025. All rights reserved.

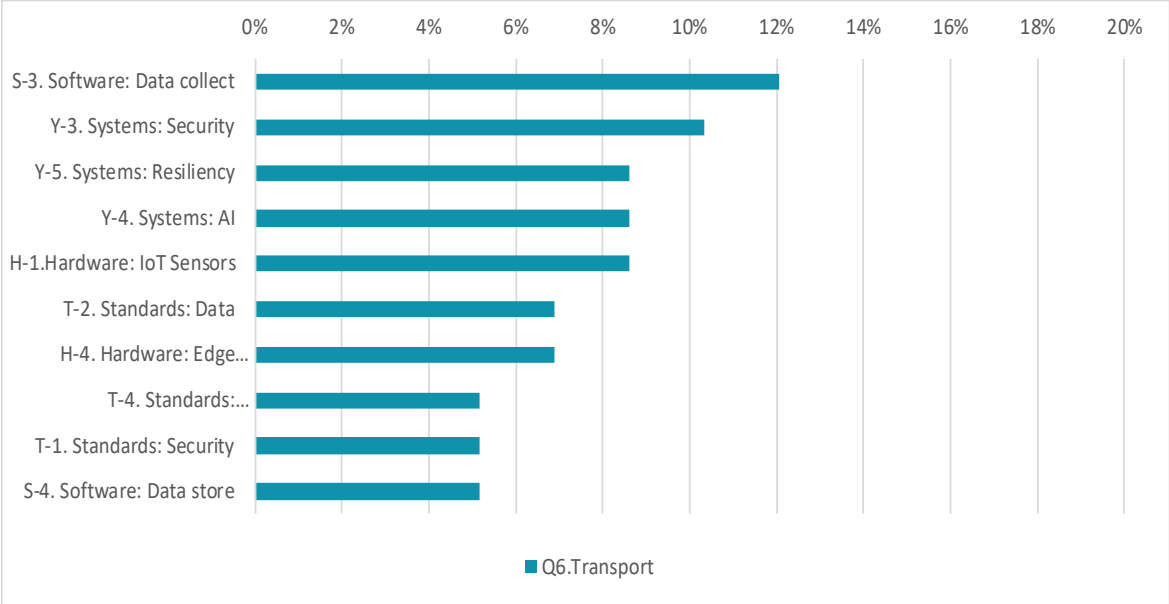


Figure 18-10: Transport and Logistics: Top 10 Most Important Single Technologies

18.3.1. Top technology challenges

Based on the approach described above, three IoT technology challenges were identified as below:

- Interoperability
- Data management
- Artificial intelligence

18.3.1.1. Challenge # 1: Interoperability

The U.S. freight transportation network is seven million miles[908] of highways, local roads, railways, airports, navigable waterways and pipelines and moves 53.6 million tons of goods worth $54 billion[909] each day. Getting these products from origin to destination reliably and on-time requires an accurate and timely flow of information between all the logistics services providers, such as contract or spot transaction carriers, warehouse and terminal operators in the network.

This flow of information is slowed, however, by a lack of interoperability between different systems, technologies and software used across the network and poses a significant challenge to the operation and management of the overall supply chain. This lack of interoperability results in inefficiencies, increased costs, delays and a lack of real-time visibility and traceability.

[908] "Freight Economy," U.S. Federal Highway Administration website. Link

[909] "Moving goods in the United States," Bureau of Transportation Statistics website, U.S. Department of Transportation. Link

© Strategy of Things, 2025. All rights reserved.

One cause of interoperability issues is the lack of universally adopted standards. For example, most freight is shipped through an intermodal transportation network involving two or more modes, such as ocean transport and truck transport or air transport and truck transport. Each transport mode uses its own set of standards.

According to a Brookings Institute commentary article, "air freight has long used well-defined standards developed by the International Air Transport Association (IATA), employing Application Programming Interface (API) documentation as opposed to the Electronic Data Interchange (EDI) to attain real-time visibility. In 2020 ocean freight began developing similar standards with the DCSA, which has as its members leading carriers and shippers, though adoption still lags. Land freight, which includes terminal operations, drayage companies, Third Party Logistics companies (3PLs), freight forwarders and rail processes, has cumbersome visibility and no clearly defined standards."[910]

The Coalition for Reimagined Mobility, noting that interoperability that facilitates the sharing of logistical data in near real-time can reduce global freight emissions by 22%, called upon policymakers worldwide to "Require the use of freight data exchange standards as a condition for accessing ports, to deploy Freight Data Exchange Standards (FDES) that communicate near real-time operation data and allocate authority to national governments and ports to require the use of FDES."[911]

A second contributor to the lack of interoperability is legacy systems. Different participants across the supply chain, including manufacturers and suppliers, shipping companies, carriers, customs agencies and technology providers, use legacy and proprietary systems. These legacy systems often lack IoT capabilities and may use outdated communication protocols.

For example, the ports of Los Angeles and Long Beach in California use different data collection and management software platforms.[912] These proprietary systems have been built and optimized over years of investment and continue to play important roles in supply chain operations. They are unlikely to be replaced, providing a challenge to integrate and share information with other systems in the supply chain.

The lack of interoperability slows the broader adoption of transformative technologies like IoT, AI and blockchain. While these technologies offer the potential to revolutionize supply chain operations by providing real-time data, predictive analytics and enhanced transparency, integrating them into legacy systems is complex and expensive.

Retrofitting legacy devices with IoT sensors and gateways or utilizing IoT middleware to translate between different communication protocols require significant resources and technical expertise.[913] A 2021 survey by satellite operator Inmarsat reported that "integrating IoT

---

[910] "A data-sharing approach for greater supply chain visibility," E. Iakovou and C. White III, Brokings Institute, September 14, 2022. Link

[911] "Solving the Global Supply Chain Crisis with Data Sharing," M. Westervelt, R. Aland and I. Dupraz. Center for Reimagined Mobility, June 28, 2022. Link

[912] ibid.

[913] "Internet of Things (IoT) in Supply Chain Management: Challenges, Opportunities and Best Practices," K. Sallam, A. Mohamed and M. Mohamed. March 2023 Sustainable Machine Intelligence Journal 2. Link

© Strategy of Things, 2025. All rights reserved.

technology with existing platforms" is a major barrier to adoption in transportation and logistics, with 55% of 450 respondents either "encountered in the deployment phase" or "expect to encounter this once deployed."[914]

This lack of interoperability leads to data silos, increased complexity, reduced efficiency and higher operational costs for organizations seeking to leverage IoT's transformational potential.

The ability to exchange data across the supply chain is critical to the development and operation of an agile and resilient supply chain. Real-time end-to-end visibility allows industry participants to be responsive to supply chain disruptions and plan and optimize corrective actions.

The Brookings Institute stated that "U.S. supply chains are a collection of decentralized systems, each with its own objectives, decision rules and levels of visibility. Challenges regarding data quality, availability, interoperability and immediacy increase when attempting to coordinate and manage multiple supply chains and their multi-modal logistics infrastructure. Data are rarely shared across supply chains and only occasionally shared across firms in the supply chain and logistics industry."[915]

Addressing these challenges is complex and requires collaboration with government, standards development organizations and industry participants across the supply chain. Between the shipper and customer is an intermediary network of logistics services providers, such as contract or spot-transaction carriers, warehouse operators and terminal operators, of different sizes and types spread out around the world. Harmonizing the different IT systems, standards and levels of knowledge among this network is a "big puzzle that requires enormous organizational effort."[916]

There are several ongoing private industry efforts to develop standards for the transportation and logistics industry. This includes the formation of the Digital Container Shipping Association which seeks to drive interoperability in the maritime industry.[917]

There are also opportunities for the U.S. federal government to play a role. For example, the Biden-Harris administration announced, in March 2022, "the launch of Freight Logistics Optimization Works (FLOW), an information sharing initiative to pilot key freight information exchange between parts of the goods movement supply chain. FLOW includes eighteen initial participants that represent diverse perspectives across the supply chain, including private businesses, warehousing and logistics companies and ports. These key stakeholders will work together with the administration to develop a proof-of-concept information exchange to ease

---

[914] "The Ins and Outs of the IoT for Transportation and Logistics," A. Stefano, Altoros blog, December 13, 2022. Link

[915] "A data-sharing approach for greater supply chain visibility," E. Iakovou and C. White III, Brookings Institute, September 14, 2022. Link

[916] "Digital transformation at logistics service providers: barriers, success factors and leading practices," M. Cichosz, C. Wallenburg, A. Knemeyer, The International Journal of Logistics Management ISSN 0957-4093, July 14, 2020. Link

[917] Digital Container Shipping Association. Link

© Strategy of Things, 2025. All rights reserved.

supply chain congestion, speed up the movement of goods and ultimately reduce costs for American consumers."[918]

18.3.1.2. Challenge # 2: Data Management

Information is essential to the operation of the digitalized global supply chain. Real-time location of freight and inventory produced by IoT tracking devices enables logistics managers plan, organize and optimize shipments to ensure on-time delivery. For example:

- IoT-enabled sensors monitor the state of the goods being transported and allow logistics managers to minimize damages or spoilage of the goods.
- Vehicle telematics information helps optimize routes while reducing fuel consumption and emissions.
- IoT sensors monitor the health and condition of vehicles and equipment to detect problems early, predict when maintenance is needed and prevent unplanned downtimes.

To make sense of these and other logistics data, the industry is increasingly turning to advanced analytics, incorporating AI and machine learning into their supply chain operations. According to a 2023 survey of 300+ U.S. supply chain executives, three-quarters, or 78%, of respondents are using AI and machine learning in their supply chains. The top applications where AI and machine learning are used include inventory and network optimization (33% of respondents), warehouse resource management (29%), supply chain risk management (26%) and demand forecasting (25%).[919]

> *Data is still one of the core challenges facing supply chain management. Each day millions and millions of data records are generated across the supply chain from multiple systems. The proliferation of digital technologies, IoT devices and advanced tracking systems has compounded the problem. This wealth of data has given rise to greater silos of data within the organization which in turn has led to disconnected data sets. Duplication and misinterpretation will become increasingly problematic, too. Critically, the fragmentation of data impedes the creation of a holistic view of the organization's supply chain.*[920]

[918] "Fact Sheet: Biden-Harris Administration Announces New Initiative to Improve Supply Chain Data Flow," White House Press Release, The White House, March 15, 2022. Link

[919] "Blue Yonder Survey: Supply Chain Executives Turn to Technology Amid Prolonged Challenges," Press Release, Blue Yonder, May 2, 2023. Link

[920] "Supply chain trends 2024: The digital shake-up," P. Liddell, KPMG. 2023. Link

© Strategy of Things, 2025. All rights reserved.

Less than a quarter (21%) of companies have visibility into their Tier 2 supply base and only 2% have visibility into their Tier 3.[921] Improved access to data across the supply chain can lead to a six percent decrease in freight costs per kilometer.[922]

Managing these IoT and non-IoT data is a major industry challenge and is best summarized in a 2023 publication on IoT and supply chain management in the Sustainable Machine Intelligence Journal. This paper states

> *One of the foremost challenges in data management within IoT-enabled supply chains is the sheer volume and velocity of data. IoT sensors continuously stream data points, generating terabytes or even petabytes of information daily. Managing this high-speed data influx requires scalable and robust data infrastructure capable of handling the data deluge.*
>
> *Additionally, organizations must devise efficient data collection strategies to filter out noise and focus on relevant information. Data integration becomes paramount, as IoT data often originates from diverse sources and systems. Ensuring data consistency and quality across the supply chain is a complex endeavor, as data may flow through multiple touchpoints, including manufacturing, transportation and warehousing. Data governance practices, data cleansing and data lineage tracking are crucial components of managing data complexity in IoT-driven supply chains.*[923]

These data management challenges are exacerbated by several factors including:

- **Reluctance to share data.** Supply chain visibility often requires data sharing though logistics companies operate on slim margins and compete on price and speed. They may hesitate to share data due to competitive concerns. Traditionally, data have been safeguarded to avoid aiding competitors.[924]
- **Lack of standards.** While logistics processes across the supply chain network are similar, the data generated and used is difficult to connect to systems and operations across the network.[925]
- **Regulatory compliance.** Data access and handling may be subject to regulations, such as the General Data Protection Regulation (GDPR) in the EU. Other data may be subjected to data sovereignty requirements that require it to be stored in the country where it was

[921] "How COVID-19 is reshaping supply chains," K. Alicke, E. Barriball and V. Trautwein. McKinsey & Company. November 23, 2021. Link

[922] "Solving the global supply chain crisis with data sharing," M. Westervel, R. Aland and I. Dupraz. June 2022. p. 9. Link

[923] "Internet of Things (IoT) in Supply Chain Management: Challenges, Opportunities and Best Practices," K. Sallam, A. Mohamed and M. Mohamed. March 2023 Sustainable Machine Intelligence Journal 2 Link

[924] "Why Data Is the Key to Saving the Logistics Industry," Transmetrics, Blog Post, Forto. Link

[925] "Logistics data standards: Challenges and benefits," Transmetrics Blog, Transmetric, March 19, 2021. Link

© Strategy of Things, 2025. All rights reserved.

collected. Finally, industry specific handling requirements may apply to other data, such as in the food industry.[926]

- **Decentralized data handling.** Logistics service providers manage their data on their systems. Global supply chain management, however, requires decentralized data handling as centralized systems are unable to provide real-time data and have difficulties coordinating with other provider systems.[927]

The exponential growth in data volumes requires that data management technologies evolve. For example, legacy data warehouses store data on servers using traditional Relational Database Management Systems (RDBMS). Whereas to store, process and analyze massive amounts of data from multiple sources in various formats modern data warehouses store data in the cloud.

Data fabrics, an emerging approach uses a network-based architecture to connect various disparate cloud databases and provides virtual access to massive volumes of data not possible with legacy data warehouses.

The growing volumes of IoT data are not unique to the transportation and logistics industry. Continued research and development of data management technologies and operations is important to meeting the evolving data needs across multiple industries.

Data observability software company Monte Carlo has identified eight trends that impact the future of data management.[928] These are:

- Data management that supports and complies with increasing regulatory requirements.
- Data governance plays a more prominent and integrated role in data management.
- Data meshes require that data management support the decentralization of data, with "distributed data products, owned by independent cross-functional teams oriented around data domains."
- Decentralization of data requires data access governance that enables "restricting access only to those who need it as well as applying the right security measures and preventing breaches."
- Automation of data transformation with no-code tools enabling less trained data professionals to perform these activities.
- Increasing need to perform real-time processing of data streams.
- AI-based applications simplify data management.
- Observability supports data management systems in understanding the health and state of data.

---

[926] "Internet of Things (IoT) in Supply Chain Management: Challenges, Opportunities and Best Practices," K. Sallam, A. Mohamed and M. Mohamed. March 2023 Sustainable Machine Intelligence Journal 2. Link

[927] "IoT-based supply chain management: A systematic literature review," S.Taj, A. Imran, et. Al. Internet of Things, Vol 24, December 2023. Link

[928] "The Future of Data Management: 8 Fast Growing Trends," J. So, Monte Carlo, July 15, 2022. Link

© Strategy of Things, 2025. All rights reserved.

Potential areas for research include:

- **Scalable and efficient data storage.** This is needed to manage the increasing volume of data generated by IoT devices by including distributed storage architectures, compression techniques and data deduplication (removing duplicate data) methods to improve storage efficiency.
- **Real-time data processing.** This combined with analytics to enhance real-time processing of IoT-generated data, including advanced algorithms, edge computing and in-memory processing techniques.
- **Security and privacy.** This includes encryption techniques, access control mechanisms and privacy preserving analytics.
- **Data quality assurance methodologies.** To ensure the accuracy and reliability of IoT-generated data, such as developing calibration techniques for sensors, anomaly detection algorithms and data validation processes are required.
- **Data governance.** Includes compliance mechanisms for data protection regulations and standards for cybersecurity data
- **Lifecycle management of IoT data.** Includes data collection, storage, processing, analysis and archiving.

18.3.1.3. Challenge # 3: Artificial Intelligence

Artificial Intelligence (AI) brings transformative benefits to the transportation and logistics industry. AI powered algorithms are well suited to analyzing vast amounts of data that can be used to optimize transportation routes, minimize fuel consumption and ensure timely deliveries. This includes:

- AI-driven inventory management enhances supply chain efficiency by optimizing inventory levels and reducing stockouts.
- Predictive maintenance capabilities enable proactive equipment servicing, reducing downtime and preventing breakdowns.
- Real-time monitoring of vehicle performance and driver behavior enables fleet managers to make informed decisions, improving safety and compliance.

A 2024 survey of 900 professionals working in transportation and logistics in the United States, United Kingdom and Germany found that 50% of respondents used basic data analytics and 25% leveraged AI in supply chain management. These rates are higher for the U.S., with 63% and 34% of respondents using basic data analytics and AI respectively.[929]

According to a 2023 survey of 300+ U.S. supply chain executives, three-quarters, or 78%, of respondents are using AI and machine learning in their supply chains. The top applications where AI and machine learning are used are inventory and network optimization (33% of

[929] "2024 tech trends in transportation & logistics," Survey Report, Here Technologies and AWS, January 2024. Link

© Strategy of Things, 2025. All rights reserved.

respondents), warehouse resource management (29%), supply chain risk management (26%) and demand forecasting (25%).[930]

While AI offers significant benefits, it faces a variety of adoption challenges. These include:

- **Lack of trust in AI.** Businesses and users must trust and accept AI results before scaling the applications. Trust is built on four factors. These are:
    - Capability, the accuracy of outcomes
    - Reliability, consistency of outcomes
    - Transparency, explainability of outcomes
    - Humanity, ethical and fair outcomes.[931]

  Trust in AI is particularly important for those applications that are autonomous or have limited human intervention in sometimes dangerous situations.
- **Limited access to high quality data.** AI algorithms depend on data for training, building, refining and validating models. These data, which comes from a variety of sources, must first be cleaned and standardized to be usable. Many businesses do not have the mass of internal data necessary to train the AI models. Furthermore, these businesses may require access to external data that they rarely track, such as weather data, which are needed by the AI models to create accurate insights and outcomes.[932]
- **Lack of transparency and explainability.** AI algorithms are "black boxes."[933] The results and outcomes produced may not be easily explainable based on the underlying decision-making or inference patterns. This lack of transparency and explainability makes it difficult to trust the AI, especially in critical situations.[934]
- **Biased data and algorithms.** The AI algorithms may not yield the intended outcomes as the underlying training data may be biased and not representative of the entire supply chain. Reluctance of the various industry participants to share data creates incomplete data sets used to train the AI models, resulting in algorithmic bias. Furthermore, circumstances may change, and models will need to be updated to remain valid.[935]

---

[930] "Blue Yonder Survey: Supply Chain Executives Turn to Technology Amid Prolonged Challenges," Press Release, Blue Yonder, May 2, 2023. Link

[931] "Accelerating Adoption of Supply Chain AI: The Critical Role of Trust," S. Patil, L. Carpenter and A. Reichheld. Supply Chain Brain. February 5, 2024. Link

[932] "Two Considerations in Building Trustworthy Supply Chain AI Models," J. Hehman, Supply Chain Brain, November 1, 2023. Link

[933] "AI Wants to Bring Trust to Supply Chains. Can It Be Trusted?" R. Bowman, Supply Chain Brain, July 23, 2023. Link

[934] Ibid.

[935] "Trustworthy, responsible, ethical AI in manufacturing and supply chains: synthesis and emerging research questions," A. Brintup, G. Baryannis, et al. May 2023. Link

© Strategy of Things, 2025. All rights reserved.

- **High costs.** Deploying, using and maintaining AI is costly. Costs may come from hardware to process the AI models,[936] personnel training and overhead and maintenance.[937] These costs are seen as the main barrier to technology implementations.[938]
- **Job losses.** While AI can provide transformational outcomes, it could lead to the loss of jobs.[939] Further, AI can exacerbate economic, racial and social inequalities.[940] These concerns raise the chances of political intervention,[941] slow adoption and create resistance to change.

There are several research opportunities to address some of these challenges. Examples include:

- **AI explainability and interpretability.** Rapid advances in AI were made possible using "black box" approaches, such as deep learning. These "black box" models, however, produce decisions and outcomes that are not easily explained as compared to their less powerful and accurate "white box" counterparts such as linear and decision tree methods. Development of methods and tools that explain and interpret machine learning and AI models is required to build trust in their decisions and recommendations.
- **Addressing AI bias**. The development of strategies and techniques to identify and remove bias in datasets is important to the development of "fair" AI algorithms. This includes methods for preprocessing the data used to train the models, as well as designing "fair and accountable" algorithms. Another area of research is developing "technical ways of defining fairness, such as requiring that models have equal predictive value across groups or requiring that models have equal false positive and false negative rates across groups."[942]
- **Addressing interoperability challenges that block access to data.** The inability to source and standardize data slows the development of AI algorithms.
- **Enable human-AI collaboration**. AI is well suited for certain tasks that require analysis of large amounts of data over a short period of time. Humans offer intuition, creativity and innovation. Research in human-AI collaboration is needed to understand how humans and machines can most effectively augment each other and how to redesign

[936] "Unlocking the Value of Artificial Intelligence (AI) in Supply Chains and Logistics," Blog, Throughput Inc., February 24, 2023. Link

[937] "Artificial Intelligence in Supply Chain Management - A Guide to Help You Disrupt the Industry!" Binary Folks. Link

[938] "2024 tech trends in transportation & logistics," Survey Report, Here Technologies and AWS, January 2024. Link

[939] "US experts warn AI likely to kill off jobs – and widen wealth inequality," S. Greenhouse, The Guardian, February 8, 2023. Link

[940] "How Artificial Intelligence Can Deepen Racial and Economic Inequities," O. Akselrod, ACLU, July 13, 2021. Link

[941] "A.I.'s Threat to Jobs Prompts Question of Who Protects Workers," E. Goldberg, New York Times, May 23, 2023. Link

[942] "Neurodiversity 101: Neurofuturism, Neurodiversity and AI", A. Kirby, November 2023. Link

© Strategy of Things, 2025. All rights reserved.

operational and business processes to best support this collaboration.

18.3.2. Other challenges

In addition to the technology infrastructure challenges for further consideration, our research identified other challenges that impact IoT adoption. These challenges did not meet the criteria for research consideration because they were either not a technology challenge or a technology related challenge that can be addressed by current marketplace offerings or capabilities.

These gaps are a result of:

- Lack of digital talent
- Resistance to change
- Legacy systems

Each of these is discussed below.

18.3.2.1. Lack of digital talent

The lack of digital talent is slowing IoT adoption and scaling. Implementing new technologies often requires skilled IT professionals who may be in short supply due to current low unemployment rates along with the perception that the transport industry may have fewer career opportunities than high technology industries.

A 2021 survey by satellite operator Inmarsat reported that "a lack of in-house skills" is a major barrier to adoption in transportation and logistics. For 73% of 450 respondents, these issues were "encountered in the deployment phase" or "expect to encounter this once deployed."[943]

The S&P Global Market Intelligence Supply Chain Digital Transformation Enterprise Survey 2023 found that skills and people shortage is the most cited hurdle to digital transformation reported by 40% of 500 survey respondents.[944] A 2021 McKinsey survey of 71 global supply chain companies reported that 39% of respondents had no or little digital talent in-house in May 2021, a 2% increase over from May 2020.[945]

In a survey of over 300 senior supply chain executives, half of the respondents cited the talent shortage (50%) as one of their biggest challenges.[946] In terms of hiring talent to address the shortage, 64% said finding the right skill set as the top challenge, followed by a talent shortage in data analytics, optimization and automation (58%) and a reduction in the time-to-hire for open

---

[943] "The Ins and Outs of the IoT for Transportation and Logistics," A. Stefano, Altoros blog, December 13, 2022. Link

[944] "Logistics sector prioritizes digital transformation, but needs technology leadership, skills," M. Fontecchio, S&P Global Market Intelligence, February 15, 2023. Link

[945] "Transforming supply chains: Do you have the skills to accelerate your capabilities?" K. Alicke, E. Dumitrescu, M. Protopappa-Sieke. McKinsey & Company. March 18, 2022. Link

[946] "Supply Chains Can't Find Talent With The Right Skill Sets," B. Straight, Supply Chain Management Review, August 17, 2023. Link

© Strategy of Things, 2025. All rights reserved.

supply chain positions (32%). Retaining talent was cited by 28% while 27% noted the lack of diversity in the talent pool.

As a result, while many transportation and logistics companies recognize the benefits of new technologies, they may struggle to overcome the technical resource constraints to realize these benefits.

18.3.2.2. Resistance to change

A major barrier to IoT adoption and scaling is resistance to change. [947] This resistance is present in two forms, institutional and individual.

- Institutional resistance is associated with a mindset "that the factors that led to past achievements will also be associated with future success."[948]
- Individual resistance is attributed to several factors, including "fear of transparency and control", "fear of job loss", "fear of failure", "a fear of a significant decrease in operational performance and worsening customer experience" when implementing a new digital service or a new operational system.[949]

Another factor driving change resistance in the industry is attributed to concerns from both management and employees. For example, management is concerned with the fear of not achieving the expected results, a lack of visibility into post-transformation workflow and the lack of expertise to drive transformation initiatives. On the other hand, employees are concerned with job security, fear of complexity and lack of visibility of possible benefits.[950]

Legacy mindsets are another form of change resistance. Legacy mindsets are "thinking, strategies and other actions that are outdated and no longer serve you to the extent that they once did."[951] For example, data are rarely shared across supply chains and only occasionally shared across firms in the supply chain and logistics industry to avoid aiding competitors.[952]

Finally, an October 2022 survey of 25 supply chain professionals reported that the top three barriers in response to "When it comes to your supply chain capabilities, which factors provide the greatest resistance to change?" were "Lack of resources" (64%), "Lack of upper management support" (52%) and "Lack of investment budget" (44%).[953]

Despite the transformational value and benefits brought by IoT, resistance to change is complex and involves a variety of psychological, economic and managerial factors. The industry,

---

[947] "Digital transformation at logistics service providers: barriers, success factors and leading practices", May 2020. Link

[948] Ibid.

[949] See note 947

[950] "Resistance to change: A roadblock for digital transformation in logistics and how to overcome it," Blog Post, SuperProcure, November 10, 2022. Link

[951] "The dangers of legacy thinking," D. Burrus, Burrus Research, July 17, 2019. Link

[952] See note 924

[953] "The formula for change in supply chain," Research Brief, Indago, October 17, 2022. Link

© Strategy of Things, 2025. All rights reserved.

however, is changing. Amazon, with its "investments in freight forwarding and air transport present new competition to logistics providers" such that "companies should be concerned that, as competition decreases, Amazon will have an even greater opportunity to dominate the market."[954]

18.3.2.3. Legacy systems

Legacy systems are outdated software and hardware that are still in use. It is best summarized in a blog article which states legacy systems are "an older computer system, software application, or technology infrastructure that is still in use but is considered outdated or is no longer actively supported or developed."[955]

Legacy systems may include complicated, obsolete or outdated business processes and data standards. While legacy systems are often decades old, they are not necessarily defined as a legacy by age but instead by not being able to meet organizational requirements.

These legacy systems are so embedded in the operations of a company that replacing them could be a lengthy and risky task. This leads to many organizations retaining legacy systems despite the benefits they could realize from modernization.[956]

> *It's nearly impossible to wipe legacy systems completely from the industry. There are simply too many companies and supply chain functions that rely on them. For many, abandoning these practices is almost like abandoning the business and its identifying culture.*[957]

Integrating IoT technologies to legacy systems is challenging and often reduces the value enabled by IoT. Some of these challenges include:[958]

- **Compatibility and interoperability**. Legacy technologies may use different or proprietary protocols. Further, they may lack the interfaces to communicate with an IoT solution.
- **Data silos**. The limited integration of legacy systems with other systems creates data silos. IoT devices connected to legacy systems may result in data that are not shared with other systems or participants in the supply or logistics chain.
- **Limited scalability**. Legacy systems are often built on architectures that have limited ability to scale. IoT applications that are based on scalable cloud or edge infrastructures generate large datasets and require processing and storage that legacy systems may not be able to support.

---

[954] "Fighting Amazon's supply chain takeover," M. Bentley. Report: Making E-commerce logistics work. Logistics Management. P.26-30. Link

[955] "What Is a Legacy System? Definition and Challenges", December 2023. Link

[956] "Legacy system integration," B. Babati, Blog article. Your EDI. September 25, 2019. Link

[957] "The Struggle to Wean Supply Chains From Legacy Tech Systems," J. Faubert, Supply Chain Brain, June 26, 2022. Link

[958] ibid

© Strategy of Things, 2025. All rights reserved.

- **Cybersecurity**. Legacy systems were not designed with modern cybersecurity and privacy requirements and capabilities. The integration of IoT with legacy systems may increase the number of attack surfaces.
- **Limited ability and agility to innovate new offerings or services**. Specialized and hard to find expertise is required to support legacy systems. These systems often run old code such as COBOL and use older hardware. Integrating with these systems can be difficult.
- **Maintenance and Updates**. IoT devices require regular updates for security patches and performance enhancements. Legacy systems may not be able keep current with updates leading to potential conflicts and issues.

Unfortunately, many logistic companies are held back by outdated IT infrastructures, fleet management and warehousing systems that are impacting their ability to innovate and digitally transform fast enough to differentiate better and achieve greater. [They] were never designed to interconnect data that is widely distributed between systems specialized to support only individual operations, such as fleet management, warehousing and port or marine operations[959]

[959] "The Rise Of AI In The Transportation And Logistics Industry," C. Gordon, Forbes, September 5, 2021. Link

© Strategy of Things, 2025. All rights reserved.

Appendix: Healthcare

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

© Strategy of Things, 2025. All rights reserved.

19. Appendix: Healthcare

This section describes the research findings for IoT technology infrastructure in the U.S. healthcare industry. The topics discussed here include:

- Industry overview
- Use of IoT in healthcare
- IoT challenges in healthcare

19.1. Industry overview

Healthcare has consistently been one of the largest and fastest growing employment sectors in the United States.[960] This section presents some basic facts about the healthcare industry as well as some key industry challenges.

19.1.1. Key facts

Healthcare is one of the largest areas of consumer and government spending in the United States. National healthcare expenditures in the United States totaled $4.3 trillion in 2021, or $12,914 per person, representing a growth of 2.7% over 2020.[961] This figure is 18.3% of GDP. National health spending is projected to grow at an average annual rate of 5.4 percent during the years 2022 to 2031, reaching 19.6% of GDP in 2031.[962]

Globally, the United States has the highest healthcare spending per capita, at $12,914.[963] Switzerland and Germany were the second and third highest, at $7,383 and $7,179, respectively.

Personal healthcare spending represented 83.5% of the total 2021 healthcare expenditures. In 2021, the top areas of personal healthcare expenditures were hospital care ($1.32 trillion, 31.1% of total), physician services ($633.4 billion, 14.9%), clinical services ($231.2 billion, 5.4%) and prescription drugs ($378 billion, 8.9%).[964]

Healthcare expenditures are paid for by a variety of "payers", including private health insurers (28.5%), Medicare (21.2%), Medicaid (17.2%), personal out of pocket (10.3%), other health insurance programs (4%), third party payers and programs (7.9%), government public health activities (4.4%) and other federal programs (1.7%).[965]

---

[960] "Employment by major industry sector", U.S. Bureau of Labor Statistics. Link

[961] "NHE Fact Sheet, 2021", Centers for Medicare & Medicaid Services. Link

[962] ibid.

[963] "How does health spending in the U.S. compare to other countries?", M. McGough, I. Telesford, S. Rakshit, E. Wager, Peterson-KFF Health System Tracker, February 9, 2023. Link

[964] "National Health Expenditures, 2021: Decline in Pandemic-Related government spending results in 9-percentage point decrease in total spending growth", Apoorva Rama, AMA Policy Perspective, 2023. Link

[965] ibid.

© Strategy of Things, 2025. All rights reserved.

The U.S. health and medical insurance market was valued at $1.1 trillion in 2022. Between 2017 and 2022, this market has experienced an annualized growth of 2.9%.[966]

Some of these expenditures are used to purchase medical equipment, supplies and technology to support patient treatments. The U.S. medical device manufacturers market size was valued at $176.7 billion in 2020 with a Compound Annual Growth Rate (CAGR) of 5.0% projected from 2021 to 2028.[967] The main driver of this growth is attributed to the rising prevalence of chronic diseases and the aging of the baby boomer population.

19.1.1.1. Employment

The U.S. healthcare industry is the largest employer of Americans employing 21.2 million people in 2020.[968] Of that number, 25.6% or 5.41 million worked in businesses employing 1,000 or more people and 32.1% or 6.82 million worked in businesses with 50 people or less. Breaking down by healthcare areas, 7.994 million (37.7%) worked in ambulatory health care services, 6.18 million (29.1%) in hospitals, 3.54 million (16.7%) in nursing and residential care facilities and 3.49 million (16.4%) in social assistance.

Employment in healthcare occupations is projected to grow 16% from 2020 to 2030, adding 2.6 million new jobs.[969] This growth is attributed to the U.S. aging population, creating more demand for healthcare services.

There were 928,174 healthcare and social assistance businesses in the United States in 2020.[970] Ambulatory health care comprised the majority, 642,970 or 69.3%, of the businesses, followed by social assistance (184,970 or 20%), nursing and residential care (93,113 or 10%) and hospitals (7,121 or 7.8%). Of those, 862,297 (92.9%) businesses employed 50 people or less. Businesses employing 1,000 people or more make up a small fraction of the 2,225 businesses.

19.1.1.2. Structure

The United States currently uses an employer-based healthcare system complemented by a range of federal programs including Medicare, Medicaid along with state-based services. The principal service delivery mechanisms are healthcare providers, payers and suppliers. Each of these is discussed below.

- Healthcare providers
    - This covers primary care physicians (PCPs), specialists, nurse practitioners (NPs), nurse assistants and their supporting roles (IT, clinical engineering, billing and administration). These providers work in both for-profit and not-for-profit

[966] Health & Medical Insurance in the U.S. - Market Size 2005–2027, IBIS World, November 29, 2021. Link

[967] U.S. Medical Device Manufacturers Market Size, Share & Trends Analysis Report by Type (Diagnostic Imaging, Consumables, Patient Aids, Orthopedics) and Segment Forecasts, 2021 - 2028, Grandview Research. Link

[968] U.S. Census Bureau, 2000, CBP Tables 2020. Link

[969] "Occupational Outlook Handbook - Healthcare Occupations", U.S. Bureau of Labor Statistics. Link

[970] U.S. Census Bureau, 2000, CBP Tables 2020. Link

© Strategy of Things, 2025. All rights reserved.

institutions. In addition, nonprofit and philanthropic organizations deliver services, implement local policies and undertake research.

- Payers
  - Medicare and Medicaid. Medicare is a federal program with around 65 million participants[971] that delivers services to people over 65 as well as to those under 65 that are temporarily or permanently disabled. Medicaid is a state and federal program with around 93 million participants[972] providing care to people with limited resources.
  - Insurance Companies. These companies function as intermediaries between providers and consumers. Consumers pool their risk to avoid the extraordinarily high costs of health services. Prior to 2014 insurance companies often implemented lifetime expenditure limits[973] and excluded pre-existing conditions[974] from coverage.
  - Health Maintenance Organizations (HMOs). These are medical insurance groups that provide health services for a fixed annual fee. They arrange managed care for self-funded health care benefit plans, individuals and other entities and act as liaisons with health care providers on a prepaid basis.[975] HMOs often require members to select a clinician to function as a gatekeeper to access medical services.
  - Preferred Provider Organization (PPO). These provide a managed health insurance plan with limits on available services.
- Suppliers
  - Pharmaceutical companies. Develop and market medications that are prescribed by clinicians. These companies typically receive remuneration through insurance or governmental drug benefit plans.
  - Medical equipment manufacturers. Undertake the design and production of a range of products, from surgical gloves to artificial joints to imaging equipment. The manufacturing of medical devices is regulated by the U.S. Food and Drug Administration (FDA) to ensure the safety and efficacy of these devices
  - Resellers. This covers the distribution of medical supplies and value-added services such as customer training, maintenance and repair of medical supplies and equipment.

[971] "Medicare Statistics 2023." Link

[972] "June 2023 Medicaid & CHIP Enrollment Data Highlights", Medicare.gov. Link

[973] "Lifetime & Annual Limits", U.S. Department of Health and Human Services. Link

[974] "Pre-existing condition", Wikipedia. Link

[975] "Health maintenance organization", Wikipedia. Link

© Strategy of Things, 2025. All rights reserved.

These mechanisms do not provide universal coverage for the U.S. population with currently around 30 million uninsured people.[976] In addition, this healthcare structure leads to a complex funding flow. Figure 19-1 below shows the path that initial investments from private households to the delivery of health care to the population.

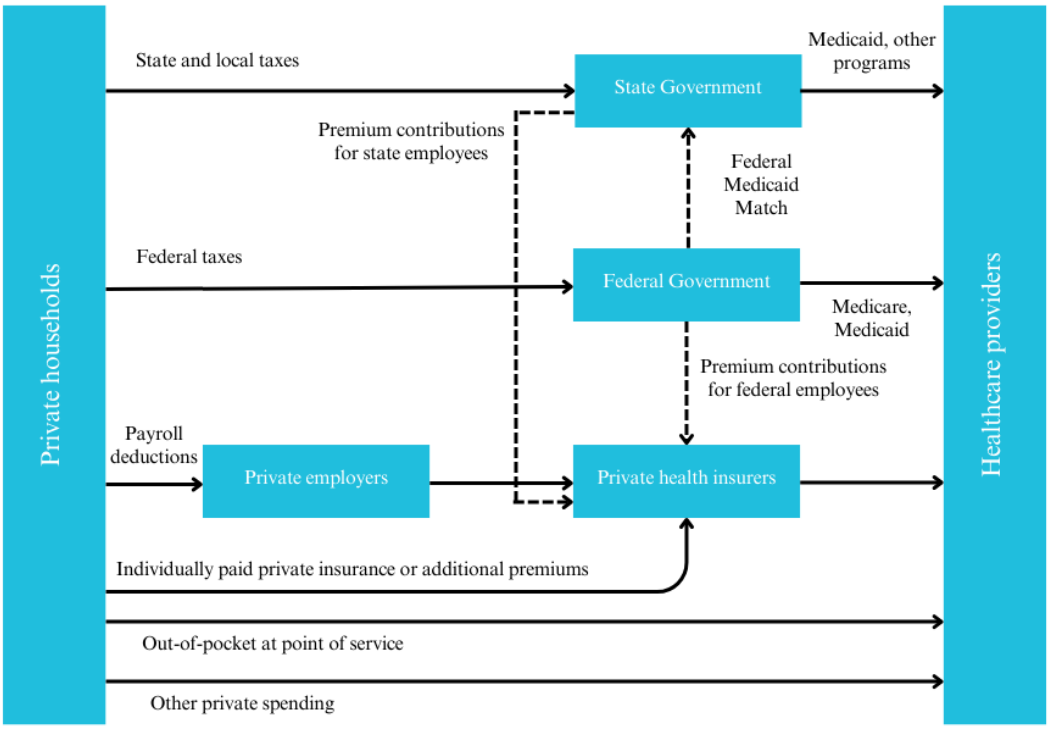


Figure 19-1: Healthcare: Payment Flows[977]

19.1.2. Industry challenges

IoT is used in a variety of ways in the healthcare industry including to improve the quality of healthcare services delivery and safety to patients and care receivers. The healthcare industry faces several challenges that constrain the growth of the industry. Four key challenges, which are relevant to the Internet of Things in healthcare are:

- Rising healthcare costs
- Access to healthcare
- Chronic disease management
- Healthcare workforce shortage

[976] "How Many Americans Don't Have Health Insurance?", Simply Insurance, October 2023. Link

[977] "The Money Flow From Households to Health Care Providers", Economic, Reinhardt U., September 2011. Link

© Strategy of Things, 2025. All rights reserved.

Each of these is discussed below.

19.1.2.1. Rising healthcare costs

Figure 19-2 below shows previous and forecasted U.S. healthcare costs.

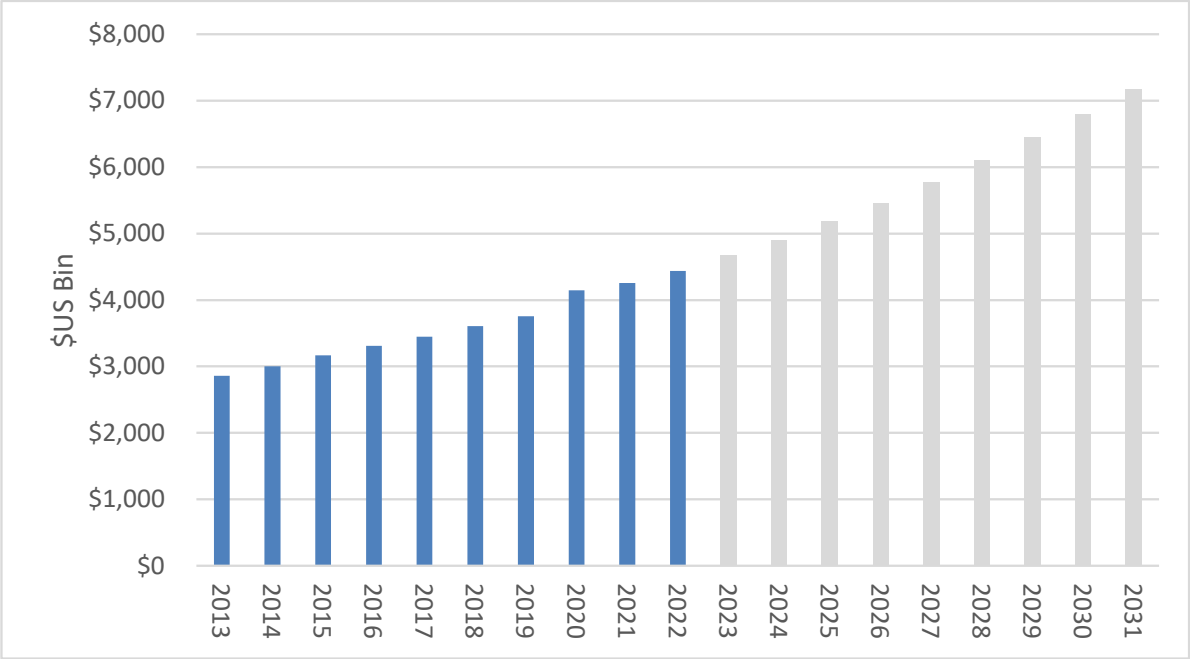


Figure 19-2: Healthcare: Current and Forecasted Costs[978]

The increase in healthcare spending is a function of two issues.

- The amounts of services used.[979] In the past two years, NHE rose by 9.7% in 2020 and 2.7% in 2021.[980] Most of this increase was attributed in 2020 to spending and services related to the COVID-19 pandemic.[981] The smaller growth rate in 2021 was attributed to a decrease in spending on pandemic related spending and services.[982]
- The cost of services provided. Over the past twenty years, the cost of healthcare services has steadily increased and outpaced the Consumer Price Index. During the time period 2003 to 2023, the CPI has risen an average of 2.5% per year, while the CPI for medical

[978] "Table01 National Health Expenditures and Selected Economic Indicators", CMS.gov, Centers for Medicare & Medicaid Services, September 2023. Link

[979] "Why are Americans paying more for healthcare?" Peter G. Peterson Foundation, July 14, 2023. Link

[980] "NHE Fact Sheet, 2021", Centers for Medicare & Medicaid Services. Link

[981] "National Health Expenditures, 2020: Spending Accelerates Due to Spike in Federal Government Expenditures Related to the COVID-19 Pandemic", Apoorva Rama, AMA Policy Perspective, May 2022. Link

[982] "National Health Expenditures, 2021: Decline in Pandemic-Related government spending results in 9-percentage point decrease in total spending growth", Apoorva Rama, AMA Policy Perspective, 2023. Link

© Strategy of Things, 2025. All rights reserved.

care has risen by an average of 3.2%.[983]

An analysis conducted by the Commonwealth Fund to examine why the United States spends more than other countries found that sixty percent of the "excess" spending was attributed to several factors. These include administrative costs of insurance (15% of excess), administrative costs by care providers (15%), wages for physicians and nurses (15%), prescription drugs (10%) and medical machinery and equipment (< 5%).[984]

These rising costs are evidenced by the Milliman Medical Index (MMI). This index examines data from health insurance claims and "estimates healthcare costs for both individuals and families who receive coverage from employer-sponsored preferred provider organization (PPO) plans."[985] The MMI showed an annual healthcare cost increase of 4.8% from 2021 to 2022 and a 5.6% increase from 2022 to 2023. For individuals, the MMI determined costs went from $6,472 per person in 2021 to $7,221 in 2023. For a family of four, the MMI determined costs went from $28,310 in 2021 to $31,065 in 2023.[986]

The effect of NHE increases is felt by healthcare receivers. Out of pocket payments paid by healthcare receivers rose by an average of 4.8% annually from $353.5 billion ($1,103 per capita) in 2015 to $433.2 billion ($1,315 per capita) in 2021. These payments are projected to rise by 4.3% annually to $659.3 billion ($1,877 per capita) by 2031.[987]

Providers also feel the rising costs of healthcare. In a 2023 survey of 150 senior healthcare leaders, "lowering the total cost of care" was ranked fourth as an industry challenge. It was selected by 34% of the healthcare leaders, behind growth (49%), system modernization (39%) and workforce challenges (35%).[988]

According to an analysis conducted by the Peter G. Peterson foundation, the higher amounts of per capita healthcare spending did not provide patients in the United States with better health outcomes when compared to other countries which spent less.[989] The analysis considered average life expectancy, obesity rate, infant mortality rate and diabetes admission rate in arriving at this conclusion.

Some of the factors that contribute to this high level of spending include:

- An aging population
- Chronic disease

---

[983] "Why are Americans paying more for healthcare?" Peter G. Peterson Foundation, July 14, 2023. Link

[984] "High U.S. health care spending: where is it all going?" A. Turner, G. Miller, E. Lowry, The Commonwealth Fund, October 4, 2023. Link

[985] "Charted: America's rising healthcare costs," Daily Briefing, Advisory Board, June 1, 2023. Link

[986] ibid.

[987] "Table 5 Personal Health Expenditures by Source of Funds," NHE Fact Sheet Downloads, NHE, September 6, 2023. Link

[988] "C-suite check-in: Building a modern, sustainable health system," R. Linnander, M. Kinney, R. Woods, Optum Advisory, July 2023. Link

[989] "Why are Americans paying more for healthcare?" Peter G. Peterson Foundation, July 14, 2023. Link

© Strategy of Things, 2025. All rights reserved.

- Administrative costs
- Prescription drug costs

Each of these is discussed below.

An aging population. As Americans age, their need for medical services rises. According to the U.S. Census Bureau, the American population is getting older with a median age of 38.9 years, an increase of 0.2 years between 2021 and 2022.[990] Between 2000 and 2021, the national median age increased by 3.4 years.[991] Older adults, older than 65, are one of the fastest growing groups, rising from 55.7 million in 2020 to an expected 80.8 million in 2040.[992]

As people age, they are more likely to experience health issues and use healthcare services. Twenty percent of adults aged 65 and older reported that their overall state of health was "fair" or "poor."[993] Adults aged 65 and older are disproportionally affected by chronic conditions and diseases including arthritis, diabetes, cancer and heart disease.[994] The National Council on Aging reports that nearly 95% of older adults have at least one chronic condition, while nearly 80% have two or more.[995]

People over 55 accounted for over half (56%) of total healthcare spending in 2019.[996] The total personal healthcare spending per capita for people 65 to 84 has been rising steadily, from $11,921 in 2002 to $20,503 in 2020.[997] This spending jumps significantly for those ages 85 and up, from $24,055 in 2002 to $35,995 in 2020. Per capita out-of-pocket spending for adults ages 64 to 84 rose from $1,909 in 2002 to $2,525 in 2020.[998] For adults 85 and up this spending increases to $5,038 in 2002 to $6,160 in 2020.

[990] "America is getting older," Press Release Number CB23-106, U.S. Census Bureau, June 22, 2023. Link

[991] "Nation continues to age as it becomes more diverse," Press Release Number CB22-112, U.S. Census Bureau, June 30, 2022. Link

[992] "Get the facts on older Americans," National Council on Aging, December 12, 2022. Link

[993] "How do health expenditures vary across the population?" J. Ortaliza, M. McGough, E. Wager, G. Claxton K. Amin, Peterson0FF Health System Tracker, November 12, 2021. Link

[994] "Get the facts on older Americans," National Council on Aging, December 12, 2022. Link

[995] "The inequities in the cost of chronic disease: why it matters for older adults," S. Silberman, National Council on Aging, April 21, 2022. Link

[996] "How do health expenditures vary across the population?" J. Ortaliza, M. McGough, E. Wager, G. Claxton K. Amin, Peterson KFF Health System Tracker, November 12, 2021. Link

[997] "Table 7 Total Personal Health Care Spending by Sex and Age Group," NHE Fact Sheet Downloads (Age and Sex Tables), NHE, September 6, 2023. Link

[998] ibid. Table 7-1.

© Strategy of Things, 2025. All rights reserved.

Chronic diseases: Around six in ten Americans have at least one chronic condition, such as diabetes, heart disease or cancer.[999] In 2020, 90% of the nation's $4.1 trillion in national health care spending was for people with chronic and mental health conditions.[1000]

- Heart disease and strokes kill more than 877,500 Americans every year at a cost for the healthcare system of $216 billion.[1001]
- Every year, 1.7 million Americans are diagnosed with cancer with over 600,000 dying. Cancer healthcare costs are rising and projected to cost $240 billion by 2030.[1002]
- More than 37 million Americans have diabetes and another 96 million have or are pre-diabetic. In 2017, the estimated cost of diagnosed diabetes was $327 billion in medical costs and lost productivity to the U.S. economy.[1003]

Adults diagnosed with chronic conditions have higher healthcare spending than those without a chronic condition. For example, the 2019 average adult total health spending for someone diagnosed with a stroke was $20,202 compared to an overall non-stroke average of $6,879.[1004] For cancer, the average spending for someone diagnosed versus a non-cancer diagnosis is $15,765 and $6,341. Similarly, for diabetes, the average spending is $16,301 versus a non-diabetes average of $5,333.

Preventive care for citizens reduces the risk of developing chronic diseases and associated complications leading to lower healthcare costs and improved patient outcomes. In 2015, however, only 8% of U.S. adults aged 35 or older received all recommended, high-priority, appropriate clinical preventive services and nearly 5% received none.[1005] Many times, people forgo these services due to cost considerations. The U.S. public's failure to undergo preventive care practices can cost up to $111 billion annually.[1006]

Labor costs. The 203 Commonwealth Fund analysis attributed 15% of the excess healthcare spending difference between the U.S. and other countries to wages for physicians and nurses.[1007]

---

[999] "Physical Activity Helps Prevent Chronic Diseases", CDC, National Center for Chronic Disease Prevention and Health Promotion (NCCDPHP). Link

[1000] "Health and Economic Costs of Chronic Diseases ", CDC, NCCDPHP. Link

[1001] ibid.

[1002] ibid.

[1003] ibid.

[1004] "How do health expenditures vary across the population?" J. Ortaliza, M. McGough, E. Wager, G. Claxton K. Amin, Peterson KFF Health System Tracker, November 12, 2021. Link

[1005] "Health Care industry insights: Why the use of preventive services is still low," S. Levine, E. Malone, A. Lekiachvili and P. Briss. Prev Chronic Dis 2019;16:180625. Link

[1006] "Almost 25% of healthcare spending is considered wasteful. Here's why." Peter G. Peterson Foundation. April 3, 2023. Link

[1007] "High U.S. health care spending: where is it all going?" A. Turner, G. Miller, E. Lowry, The Commonwealth Fund, October 4, 2023. Link

© Strategy of Things, 2025. All rights reserved.

The healthcare workforce shortage along with the pandemic have been key contributing factors to rising costs. The extent and causes of the labor shortage are further discussed in Section 19.1.2.4.

While workforce shortages were a problem before the pandemic, they were exacerbated during the pandemic. Prior to the pandemic, labor costs were more than 50% of a hospital's expenses.[1008] The American Hospital Association reported that hospitals experienced a 19.1% increase in labor expenses per adjusted discharged patient from pre-pandemic 2019 to 2021.[1009] Management consultancy McKinsey & Co. estimated that U.S. NHE could be $590 billion higher than the projected $5.8 trillion forecasted for 2027, of which $148 billion is due to "elevated clinical labor inflation rates linked to a shortage of clinical staff."[1010]

An analysis conducted by healthcare improvement company, Premier Inc., found that hospitals are paying $24 billion more per year for qualified clinical labor than before the pandemic. This translates to an increase of eight percent per patient per day and $17 million increase in additional annual labor costs during the pandemic.[1011] In addition, overtime hours increased 52% and use of agency labor was up 132% for full time and part-time workers. These labor options added more than 50% to the typical employee's hourly rate.[1012]

Administrative costs: As discussed in Section 19.1.1, the U.S. spends more money annually on healthcare than any other country.[1013] An analysis by the Commonwealth Fund attributed 60% of the excess healthcare spending, relative to other countries, to a variety of factors discussed previously in this section. Of this 60%, administrative costs accounted for half (30%). This includes administrative costs for insurance (15%) and care providers (15%).[1014]

A 2019 report from independent, non-partisan policy institute Center for American Progress showed that administrative costs represented a higher percentage of U.S. healthcare spending than other high-income countries. For example, administrative costs were 8.3% of U.S. healthcare expenditures in 2016, as compared to France (5.7%), Austria (4.8%) and Germany (4.2%).[1015] An analysis from the Peter G. Peterson Foundation echoed these findings. The United

---

[1008] "Massive growth in expenses and rising inflation fuel continued financial challenges for America's hospitals and health systems," Guide/Report, American Hospital Association, April 2022. Link

[1009] ibid. Figure 1.

[1010] "The gathering storm: The uncertain future of U.S. healthcare," A. Fleron and S. Singhal. McKinsey & Company. September 16, 2022. Link

[1011] "PINC AI Data Shows Hospitals Paying $24B More for Labor Amid COVID-19 Pandemic," M. Alkire, D. Miller and B. Cloyd, PINC, October 6, 2021. Link

[1012] ibid.

[1013] See Note 961

[1014] "High U.S. health care spending: where is it all going?" A. Turner, G. Miller, E. Lowry, The Commonwealth Fund, October 4, 2023. Link

[1015] "Excess administrative costs burden the U.S. healthcare system," E. Gee, T. Spiro, Center for American Progress, April 8, 2019. Link

© Strategy of Things, 2025. All rights reserved.

States' administrative costs per capita of $1,055 are at least three times higher than Germany ($306), France ($299) and Switzerland ($297).[1016]

The U.S. healthcare system is built around the individual's desire for "choice." This desire creates a system with multiple payers and results in complexity in billing and non-care expenses such as marketing costs related to plan choice.[1017]

> *A broader way of thinking about high administrative costs in the U.S. health care system is that they reflect the way in which the system deals with the inherent problems with health care markets. Specifically, because health care expenditures are uncertain, individuals need insurance. Without any countervailing force, insurance distorts market outcomes, causing utilization and prices to increase.*[1018]

The complex and fragmented nature of the U.S. healthcare system requires a variety of supporting administrative activities. These activities account for 15% to 25% of total national healthcare expenditures.[1019] Of the 2021 NHE of $4.3 trillion, administrative costs represented $645 billion to $1.1 trillion. The Center for American Progress estimates that administrative costs amount to $569 billion,[1020] [1021] building off an analysis[1022] conducted in 2003 and accounting for medical care inflation.

Administrative costs in the U.S. healthcare system consist of two main components, billing and insurance related (BIR) costs and hospital and physician practice administration costs.

- BIR costs include the health insurance and providers overhead costs for claims submission, reconciliation and payment processing. It is reflected in consumers' insurance premiums and providers' reimbursements.
- Practice administration accounts for medical recordkeeping, hospital management, care quality management activities and fraud and abuse management programs.[1023]

An analysis conducted by the Center for American Progress estimates BIR costs of $469 billion for 2019.[1024] Of that amount, the analysis determined that $248 billion are excess administrative

---

[1016] "Almost 25% of healthcare spending is considered wasteful. Here's why." Peter G. Peterson Foundation. April 3, 2023. Link

[1017] "Administrative expenses in the U.S. health care system: Why so high?" M. Chernew and H. Mintz, JAMA, October 20, 2021. Link

[1018] See note 1017

[1019] See note 1017

[1020] "Excess administrative costs burden the U.S. healthcare system," E. Gee, T. Spiro, Center for American Progress, April 8, 2019. Link

[1021] In 2018 dollars.

[1022] "Costs of Health Care Administration in the United States and Canada," S. Woolhandler, T. Campbell and D. Himmelstein. The New England Journal of Medicine. August 21, 2003. Link

[1023] See note 1020

[1024] See note 1020

© Strategy of Things, 2025. All rights reserved.

costs. For healthcare providers, the CAP report cited several research studies that showed that BIR costs were 25% of hospital expenditures and 25% of physician revenues. These administrative costs varied on a "per encounter" basis depending on the type of visit. Costs ranged from $20 for a primary care visit, $62 for an emergency room visit to $215 for an in-patient surgery visit.

Prescription drug costs. The rising cost of prescription drugs is a key contributor to the increase in overall U.S. healthcare spending. Between 2015 and 2021 spending for prescription drugs rose 21%, from $312 billion ($978 per capita) to $378 billion ($1,147 per capita). Spending is projected to grow 57% to $591.8 billion ($1,685 per capita) by 2031, an average annual growth rate of 4.6%.[1025] While there are several reasons for the increase in spending for prescription drugs, such as the number and types of drugs prescribed, pricing and price increases are the major drivers.[1026]

The American Hospital Association (AHA), citing a study by GoodRx, reported that drug companies increased the price of about 810 brand and generic drugs that they reviewed by an average of 5.1% in January 2022.[1027] A study by the Kaiser Family Foundation (KFF) reported that half of the 3,911 drugs covered by Medicare had price increases greater than the rate of inflation between July 2019 and July 2020. Seventeen percent, or 668, of the covered drugs had price increases above 7.5%.[1028]

A report from the Assistant Secretary for Planning and Evaluation's Office of Health Policy highlighted that the number of drugs experiencing price increases grew from 3,263 in 2016 to 3,840 in 2022.[1029] [1030] In January 2016, the average increase was 13% ($100) while in January 2022, the increase was 10% ($150). While some price increases were adjustments for inflation, several of the price increases significantly exceeded the inflation rate. For example, during the period July 2021 to July 2022, there were 1,216 drugs whose average price increase of 31.6% exceeded the general inflation rate of 8.5%.[1031]

There are several factors that contribute to the rise in drug prices. One of the most significant factors is the introduction and dispensing of brand name drugs. These drugs are protected by

---

[1025] "Table 2 - National Health Expenditure Amounts and Annual Percent Change by Type of Expenditure: Calendar Years 2015-2031", NHE Fact Sheet Downloads, NHE, Centers for Medicare and Medicaid Services, September 6, 2023. Link

[1026] "Why are prescription drug prices rising and how do they affect the U.S. fiscal outlook?" Peter G. Peterson Foundation, November 14, 2019. Link

[1027] "Massive Growth in Expenses and Rising Inflation Fuel Continued Financial Challenges for America's Hospitals and Health Systems," American Hospital Association, April 2022. Link.

[1028] "Prices Increased Faster Than Inflation for Half of all Drugs Covered by Medicare in 2020," J. Cubanski and T. Neuman, KFF, February 25, 2022. Figure 1. Link

[1029] See note 1028

[1030] Prescription drug prices increases occur in January and July of each year. For 2016, there were 2650 drugs reporting price increases in January and 613 in July. For 2022, there were 3,239 drugs with price increases in January and 601 in July.

[1031] ibid.

© Strategy of Things, 2025. All rights reserved.

patents and "gives the manufacturer monopolistic control over a given market and the ability to increase prices without competition."[1032] These brand name drugs represent 10% of the prescriptions dispensed and 79% of prescription drug spending.[1033] Prices on some brand-name drugs have increased by over 60% since 2014.[1034] According to the Peterson-KFF Health System Tracker some specialty drugs are more expensive in the U.S. than in other countries. For example, the list price of Harvoni, used to treat chronic Hepatitis C is 132% more than in Switzerland and 89% more than in the U.K. Similarly, the list price of Humira that treats rheumatoid arthritis, Crohn's disease and ulcerative colitis is 265% higher than Switzerland and 423% higher than the U.K.[1035]

Other factors cited as contributors to rising drug prices include "a lack of transparency in drug prices, less competitive drug markets stemming from mergers and acquisitions among manufacturers and limited ability of other parties, such as Medicare, to negotiate drug prices."[1036]

19.1.2.2. Access to quality healthcare

Access to quality healthcare is often seen as a right and is a key determinant of health and well-being. Many people in the United States face barriers to accessing quality, affordable and timely healthcare services. These barriers disproportionately affect vulnerable and underserved populations, such as racial and ethnic minorities, low-income groups, rural residents, older adults and people with disabilities or chronic conditions. Some of these barriers include:

- **Affordability.** A 2021 West Health and Gallup survey of 3,753 U.S. adults found that 18% of Americans (46 million people), were unable to afford quality healthcare.[1037] Black and Hispanic adults were most affected with 29% and 21% respectively, unable to pay, compared with 16% of white adults.

  The ability to afford healthcare varies by age. Adults in the 18-49 age group were least likely to afford healthcare with 27% of non-white and 20% of white adults unable to pay. Among adults 50 to 64, 26% of non-whites and 15% of whites reported they are unable to pay. Adults older than 65 have the best access, with only 16% of non-whites and 8% of white adults unable to pay.

  Those households with the least income are most affected. For example, 35% of adults with an annual income under $24,000 are unable to pay. In contrast, only 7% of those with an income over $180,000 are unable to pay.

  Rising healthcare costs lead to cutting back on something else to pay for care. A 2021

[1032] See note 1026

[1033] ibid.

[1034] ibid.

[1035] "What are the recent and forecasted trends in prescription drug spending?" E. Wager, I. Telesford, C. Cox and K. Amin, Peterson-KFF Health System Tracker. September 15, 2023. Link

[1036] See note 1026

[1037] "In U.S., an estimated 46 million cannot afford needed care," D. Witters, Gallup, March 31, 2021. Link

© Strategy of Things, 2025. All rights reserved.

Gallup-West Health survey found that 12% of Americans cut back on food, while 11% cut back on over the counter drugs to pay for healthcare.[1038] One quarter of those earning less than $24,000 cut back on food and drugs to pay for healthcare.

- **Lack of insurance coverage.** While the number of uninsured Americans have decreased since 2013 there are still people who lack insurance. The U.S. Department of Health and Human Services reported that 25.3 million, or 7.7% of Americans did not have insurance in the first quarter of 2023.[1039] The uninsured rate varies by age groups, with 11% of adults aged 18 to 64 and 4.2% of children 0 to 17 years having no insurance.[1040]

  The uninsured rate varies by income level. It is highest, at 17%, for those under the Federal Poverty Level (FPL). It decreases as income rises, from 15.8% for those making between 100% to 200% of FPL to 3.3% for those making over 400% of FPL.[1041]

  Despite the continuing decrease, the Congressional Budget Office (CBO) predicts that the uninsured rate will increase in the future as Medicaid and Affordable Care Act marketplace subsidies and policies expire. For example, the CBO projects that 10.4% of Americans under 65 will be uninsured in 2027 and 10.1% in 2033.[1042]

- **Geographic location**: According to the Washington Post, the federal government has designated 80% of rural areas in the U.S. as "medically underserved." These "medical deserts" are home to 20% of the U.S. population, but only 10% of the doctors. [1043] The patient-to-primary care physician ratio is 39.8 per 100,000 people in rural areas. In contrast, this ratio is 53.3 per 100,000 in urban areas.[1044] Exacerbating this shortage is that the number of rural physicians is expected to decline by 23% over the next decade, while the number of urban doctors remains flat.[1045]

  Access to healthcare is difficult for these rural residents. As an illustrative example, 159 of the 254 counties in Texas have no general surgeons. 121 counties have no medical

---

[1038] ibid.

[1039] "National uninsured rate reaches an all-time low in early 2023 after the close of the ACA open enrolment period," HP-2023-20, Assistant Secretary for Planning and Evaluation, Office of Health Policy, U.S. Department of Health and Human Services, August 3, 2023. Figure 1. Link

[1040] ibid. Figure 2.

[1041] ibid. Figure 4.

[1042] "US projected to hit record-low uninsurance rate this year," R. Pifer, HealthcareDive, May 24, 2023. Link

[1043] "'Out here, it's just me': In the medical desert of rural America, one doctor for 11,000 square miles," E. Saslow, Washington Post, September 28, 2019. Link

[1044] "Top challenges impacting patient access to healthcare," S. Heath, Patient Engagement Hit, February 22, 2022. Link

[1045] See note 1043

© Strategy of Things, 2025. All rights reserved.

specialists, and 35 counties have no doctors.[1046] To access healthcare, "Individuals in rural areas travelled an average of 40.8 miles to their radiation treatment while those in urban areas travelled about 15.4 miles"[1047]

According to the CDC, Americans living in rural areas face health disparities when compared to their urban counterparts. These residents are "more likely to die from heart disease, cancer, unintentional injury, chronic lower respiratory disease and stroke than their urban counterparts. Unintentional injury deaths are approximately 50 percent higher in rural areas than in urban areas, partly due to greater risk of death from motor vehicle crashes and opioid overdoses. In general, residents of rural areas in the United States tend to be older and sicker than their urban counterparts."[1048]

There are a variety of reasons for these disparities, including less access to healthcare and lack of insurance.[1049] In particular, home healthcare, hospice and palliative care, mental health, substance use disorder, reproductive, obstetric and maternal health and oral health services are difficult to access.[1050]

- **Transportation issues.** Around 3.6 million people in the U.S. do not receive appropriate health care due to transportation issues.[1051] Transport issues include lack of vehicle access, inadequate infrastructure, long distances, lengthy travel times and costs. These issues may lead to missed or delayed health care appointments, increased health expenditures and overall poorer health outcomes.[1052]

  While transportation issues affect urban and rural communities, residents in rural communities are more affected given that the limited number of healthcare providers and healthcare locations may be distant. These communities often have an older population who have chronic conditions requiring multiple visits to outpatient healthcare facilities.[1053] Unlike urban areas with public transit options, public transportation services are often not available in rural areas. This lack of a public or private transportation infrastructure limits access to healthcare services.

[1046] See note 1043

[1047] "Top challenges impacting patient access to healthcare," S. Heath, Patient Engagement Hit, February 22, 2022. Link

[1048] "About Rural Health", Public Health Infrastructure Center, U.S. Centers for Disease Control and Prevention, May 9, 2023. Link

[1049] ibid.

[1050] "Healthcare access in rural communities," Rural Health Information Hub, November 21, 2022. Link

[1051] "Social Determinants of Health Series: Transportation and the Role of Hospitals", American Hospital Association, 2023. Link

[1052] ibid.

[1053] "Healthcare access in rural communities," Rural Health Information Hub, November 21, 2022. Link

© Strategy of Things, 2025. All rights reserved.

- **Cultural and linguistic differences**: In 2021, there were approximately 25.7 million, or 8% of people older than 5, living in the United States who have Limited English proficiency (LEP).[1054] Language barriers are a significant cause of healthcare inequities and impacts 1 in 12 patients seeking healthcare. [1055]

  Non-elderly persons with LEP are more likely to be uninsured (29%) compared to their English proficient (9%) counterparts.[1056] This is because people with LEP are typically employed in lower wage jobs and industries that often do not offer employer sponsored coverage. If coverage is offered, persons with LEP may have difficulty affording coverage.[1057]

  LEP people face several barriers to accessing quality healthcare. Healthcare policy and research firm reported that "Studies have found that language barriers between providers and patients may result in decreased patient satisfaction with health care; lack of comprehension of health care information, leading to increased adverse effects; reduced medication adherence; excessive ordering of medical tests by providers; higher rates of medical errors; and decreased primary care utilization".[1058]

  In 2021 A KFF survey of 778 Hispanic adults found that among the 334 who completed the survey in Spanish, 35% (of the 334) said it is difficult to find a doctor who explains things in a way they can understand compared with 17% (of the 444) of those who completed the survey in English and one-third (33% of 778) said it was very or somewhat difficult to find a doctor who speaks their preferred language or provides an interpreter when needed."[1059]

  Patients with LEP have longer hospital stays and are at higher risk of surgical delays and readmissions. Hispanic people with LEP report reduced access to care and fewer preventive services compared to English proficient Hispanic people. For Asian American people with LEP, language barriers are one of the most significant challenges to accessing care, particularly among older Asian Americans.

19.1.2.3. Chronic disease management

Chronic diseases are long-term conditions that require ongoing medical attention and affect a patient's quality of life. The management of these diseases is a challenge for the American

[1054] "Overview of health coverage and care for individuals with limited English proficiency (LEP)," S. Haldar, D. Pillai and S. Artiga. KFF, July 7, 2023. Link

[1055] "Language barriers in healthcare: A preventable obstacle to health equity", Jeenie. Link

[1056] See note 1054

[1057] See note 1054

[1058] See note 1054

[1059] See note 1054

© Strategy of Things, 2025. All rights reserved.

healthcare industry. These diseases are prevalent and are expected to increase over the next several decades among all age groups.

Section 19.1.2.1 discussed the high spending levels in treating chronic diseases that contribute to the rising national health expenditures in the United States. Despite spending levels that far exceed those of other countries, Americans are not obtaining better health outcomes.[1060]

Some challenges to chronic disease management include:

- **Patient adherence.** For example, a patient with diabetes must "watch what they eat, monitor their blood sugar levels, take their medications, maintain a routine of moderate exercise and some must self-administer insulin injections multiple times a day."[1061]

  Successful health outcomes are achieved if patients adhere to these prescribed treatments. Several barriers, however, hinder successful outcomes. The more complex the disease, the more challenging patient adherence. This complexity increases for those patients suffering multiple chronic conditions.

  McKinsey & Company cites several studies quantifying the impact of non-compliance. Fifty to sixty percent of patients miss doses, take the wrong doses or prematurely stop treatment in the first year. Non-adherence leads to an estimated 125,000 deaths and $290 billion in additional spending annually. An additional 10% of hospitalizations can be avoided.[1062]

  The World Health Organizations cites several factors for non-adherence, including type of diagnosis, type of therapy, socioeconomic and cost concerns, individual traits, health care providers and insurance systems, lack of education and involvement in the treatment decision-making process.[1063]
- **Care coordination.** Patients managing chronic conditions often require treatment by multiple care providers. The ability to provide coordinated care and treatment through "team-based" care is crucial for successful patient health outcomes.

  The Institute for Healthcare Improvement defined team-based care as "the provision of comprehensive health services for individuals, families and/or their communities by at least two health professionals who work collaboratively along with patients, family caregivers and community service providers on shared goals within and across settings to achieve care that is safe, effective, patient-centered, timely, efficient and equitable."[1064]

[1060] "Why are Americans paying more for healthcare?" Peter G. Peterson Foundation, July 14, 2023. Link

[1061] "Overcoming patient barriers to chronic disease management," A. Warnock, Managed Healthcare Executive, January 18, 2022. Link

[1062] "Improving patient adherence through data-driven insights," J. Hichborn, S. Kaganoff, N. Subramanian, Z. Yaar. McKinsey & Company, December 14, 2018. Link

[1063] "Why people are noncompliant with treatment," T. Torrey, VeryWell Health, March 31, 2023. Link

[1064] "Team-based care: optimizing primary care for patients and providers," C. Hupke, Institute for Healthcare Improvement, May 16, 2014. Link

© Strategy of Things, 2025. All rights reserved.

Coordinated care is "deliberately organizing patient care activities and sharing information among all of the participants concerned with a patient's care to achieve safe and more effective care" and requires that all patient information and treatments are known ahead of time and communicated to the right people at the right time.[1065] Effective care coordination leads to reduced hospital readmissions, [1066] greater adherence and lowered costs.[1067]

Coordinating care, however, is challenging due to the fragmented nature of the healthcare industry. A 2023 survey conducted by Harris Poll for the American Academy of Physician Associates (AAPA) reported that U.S. adults spent the equivalent of one eight-hour workday per month to coordinate healthcare for themselves or others. In addition, two-thirds (65%) of adults feel managing healthcare is "overwhelming and time consuming."[1068]

As a result, a majority (61%) of those surveyed only seek healthcare when they are sick. Patients who were unable to get an appointment in the same week had to wait for just under a month to get an appointment. Just over two-fifths (44%) of adults have skipped or delayed care that they needed over the past two years. Nearly two-thirds (60%) of those skipping or delayed care experienced some kind of impact.[1069]

- **Information sharing.** Timely and accurate communication among healthcare providers, insurance companies and patients are critical to successful patient outcomes. This is important in the treatment of chronic conditions where multiple providers and caregivers need to work together in a coordinated manner.

  The Office of the National Coordinator (ONC) for Health Information Technology, however, found that 65% of 1,524 physicians engaged in some form of electronic exchange (send, receive, or query) of patient health information with providers outside their organization in 2019.[1070] Only 10% of physicians engaged in all four domains of exchange (send, receive, find and integrate).[1071] Three quarters of those who engaged in Health Information Exchange (HIE) reported benefits. These benefits include improving

[1065] "Care Coordination", Agency for Healthcare Research and Quality. Link

[1066] "Care coordination program improves outcomes, cuts readmissions," H. Nelson, Patient Engagement HIT, February 18, 2021. Link

[1067] "5 care coordination strategies for Medicare ACO success," J. LaPointe, Revcycle Intelligence, April 16, 2019. Link

[1068] "U.S. adults spend eight hours monthly coordinating healthcare, find system 'Overwhelming'," Press Release, American Academy of Physician Associates, May 17, 2023. Link

[1069] ibid.

[1070] "Interoperability among office-based physicians in 2019", ONC Data Brief No. 59, Office of the National Coordinator for Health Information Technology, July 2022. Figure 1. Link

[1071] ibid. Figure 3.

© Strategy of Things, 2025. All rights reserved.

care quality, care coordination and reduced duplicate test ordering.[1072]

The electronic exchange of information increases with the size of the physician's practice. Those practices employing 50 or more physicians have access to and use electronic information more than smaller and solo practices. For example, while the national average of physicians who have access to information from outside sources at the point of care is 36% and use that information is 26%, large offices report access of 55% and information use of 44%. In contrast, only 23% of solo physicians have access to information and 13% use that information.[1073]

There are some challenges to the electronic exchange of information. The top three barriers included difficulties exchanging information with providers who use a different Electronic Health Record (EHR) developer (reported by 85% of those who use HIE), using multiple systems or portals (73%) and providers in referral networks who lack the capability to exchange information electronically (71%).[1074]

19.1.2.4. Healthcare workforce shortage

In an open letter the American Hospital Association (AHA) suggests that the current labor shortage is "a national emergency that demands immediate attention from all levels of government and workable solutions."[1075] The letter cites an estimated shortage of 3.2 million healthcare workers in critical, although lower-wage jobs such as medical assistants, home health aides and nursing assistants, by 2026. [1076]

The Association of American Medical Colleges forecasts a shortage of between 54,100 and 139,000 physicians by 2033. This includes a shortage of 21,400 to 55,200 primary care physicians and 33,700 to 86,700 non-primary care specialist physicians by 2033.[1077]

In addition, 200,000 new Registered Nurses (RNs) will need be hired each year to meet expected demand and replace the retiring workforce.[1078] Figure 19-3 below shows the expected physician shortages by 2033.

[1072] Ibid. Table 1.

[1073] Ibid. Figure 4.

[1074] ibid. Table 1.

[1075] "AHA Letter Re: Challenges Facing America's Health Care Workforce as the U.S. Enters Third Year of COVID-19 Pandemic," American Hospital Association, March 1, 2022. Link

[1076] "US healthcare labor market," T. Bateman, S. Hobaugh, et al., Mercer, 2021. Link

[1077] "New AAMC Report Confirms Growing Physician Shortage," Press Release, AAMC, January 20, 2020. Link

[1078] "Fact Sheet: Strengthening the Health Care Workforce," Fact Sheet, American Hospital Association, November 2021. Link

© Strategy of Things, 2025. All rights reserved.

Medical Areas	Shortage Range
Primary care	Between 21,400 and 55,200 physicians
Nonprimary care specialties	Between 33,700 and 86,700 physicians
• Surgical specialties	Between 17,100 and 28,700 physicians
• Medical specialties	Between 9,000 and 17,800 physicians
• Other specialties (i.e., pathology, radiology, psychiatry	Between 17,100 and 41,900 physicians

Figure 19-3: Healthcare: Physician Shortage[1079]

The workforce shortage is caused by the prevalence of chronic conditions and an aging population and as discussed in Appendices 19.1.2.3 and 19.1.2.4. Other factors include:

- **COVID-19**: The pandemic increased the demand for healthcare services, exposing the workforce to high levels of stress and reducing the availability of foreign-trained workers. An estimated 1.5 million health care jobs were lost in the first two months of COVID-19 as restrictions on non-emergency services were implemented.[1080] A 2021 Washington Post-Kaiser Family Foundation survey found that nearly 30% of health care workers are considering leaving their profession and nearly 60% reported impacts to their mental health stemming from their work during the COVID-19 pandemic.[1081]
- **High turnover**: Healthcare professionals are leaving the workforce at high rates for a variety of reasons, including retirement, stress and factors related to the pandemic. The U.S. Bureau of Labor Statistics reported that 2.1 million workers have quit their healthcare jobs between May 2023 and August 2023.[1082] The AHA reported that more than half of all nurses were 50 years of age or older and 30% were 60 years of age or older.[1083] The annual turnover rate of hospital certified nursing assistants (CNAs) was 27.7%, double the turnover rate of nurses and physician assistants.[1084]
- **Limited supply of incoming professionals.** While the number of medical school graduates has increased over the past two decades, the number of Medicare-funded residency slots has remained frozen at the levels imposed by Congress in 1996. This

[1079] "New AAMC Report Confirms Growing Physician Shortage," Press Release, AAMC, January 20, 2020. Link

[1080] "Staff Shortages Choking U.S. Health Care System", U.S. News, Johnson, S., July 2022 Link

[1081] "Burned out by the pandemic, 3 in 10 health-care workers consider leaving the profession," W. Wan, Washington Post, April 22, 2021. Link

[1082] "Table 4. Quits levels and rates by industry and region, seasonally adjusted", Economic News Release, U.S. Bureau of Labor Statistics, October 3, 2023. Link

[1083] "Fact Sheet: Strengthening the Health Care Workforce," Fact Sheet, American Hospital Association, November 2021. Link

[1084] ibid.

© Strategy of Things, 2025. All rights reserved.

resulted in 3,100 applicants that did not receive residency slots in 2019.[1085]

Similarly, the American Association of Colleges of Nursing reported that U.S. nursing schools turned away 91,938 qualified applications from baccalaureate and graduate nursing programs in 2021. Key reasons include "insufficient number of faculty, clinical sites, classroom space, clinical preceptors as well as budget constraints."[1086]

- **Low compensation.** Over 7 million people work in low-paid, essential healthcare jobs, including healthcare support (e.g., orderlies, medical assistants, pharmacy aides), direct care (e.g., home health workers, nursing assistants, personal care aides, etc.) and healthcare service (janitors, food preparation, housekeepers in hospitals and nursing homes).

  The median pay for these jobs was $13.48 per hour in 2019, below the living wage.[1087] Nearly 20% of healthcare workers live in poverty and more than 40% rely on public assistance. In contrast, the median pay of registered nurses was $35.17 per hour, while physicians and surgeons had a median pay of over $100 per hour.[1088]

19.2. IoT in the healthcare industry

The Internet of Things is transforming healthcare by changing the way medical services are delivered, monitored and managed to create significant improvements in patient health outcomes.

For example, wearable IoT health devices, such as smart watches, empower people to continuously track their vital signs, activity levels and certain chronic conditions. This monitoring facilitates early detection of health issues, enables timely interventions and encourages preventive measures, ultimately contributing to improved patient well-being.

The data collected from the devices may be paired with AI algorithms to provide physicians with additional insights that are used to prescribe highly individualized treatments. This is a new approach to tailoring disease prevention and treatment that accounts for differences in people's genes, environments and lifestyles to provide the right treatments to the right patients at the right times.[1089]

When legacy medical devices were connected, their use of propriety manufacturer-specific technologies limited their ability to interoperate and scale. In contrast, the integration of medical devices with standardized IoT technologies holds the promise of many different types of devices

---

[1085] ibid.

[1086] "Fact Sheet: Nursing Shortage," American Association of Colleges of Nursing, October 2022. Link

[1087] "Living Wage Calculator", MIT, EDU. Link

[1088] "Essential but undervalued: Millions of health care workers aren't getting the pay or respect they deserve in the COVID-19 pandemic," M. Kinder, Brookings Institute, May 28, 2020. Link

[1089] "Precision Medicine", U.S. FDA, September 27, 2018. Link

© Strategy of Things, 2025. All rights reserved.

that connect with each other and the Internet, interoperate and combine data to deliver patient care in innovative ways.

Healthcare IoT devices range from consumer devices, such as wearable fitness trackers to connected medical devices used in hospitals such as local and remote patient monitoring equipment and infusion pumps. IoT devices used in clinical settings are referred to as Internet of Medical Things (IoMT) and are subject to FDA regulations.[1090]

IoT plays a key role in addressing some of the healthcare industry's top challenges such as rising annual healthcare expenditures. The use of IoT helps to reduce some of these expenditures by enhancing care delivery, facilitating early diagnosis and improving patient health outcomes.

IoT enables remote patient monitoring and decentralized clinical trials.[1091] Remote patient monitoring enables clinicians to develop more accurate diagnoses, detect the onset of diseases earlier and intervene earlier when patient conditions deteriorate. This allows for more effective treatments and reduces the number of future treatment visits. In addition, it keeps patients out of the hospital which reduces costs and increases patient satisfaction.

Wearable health trackers enable users to monitor their vital signs and empowers them to maintain a healthy lifestyle and take preventative measures such as exercise and diet. This leads to healthier individuals with reduced use of medication and doctor visits.

Access to quality healthcare is a challenge for people living in rural communities, those who are disabled and those without access to transportation. In other instances, patients may have rare conditions without geographic access to specialists. The challenge is magnified for those suffering from chronic conditions that require regular visits to multiple doctors.

Sensors integrated with IoT technologies enable the remote monitoring of patients outside of doctor offices or medical facilities. Paired with video cameras, doctors can review patient health conditions to diagnose and prescribe treatment during virtual doctor visits. Furthermore, continuous remote monitoring can alert doctors to a patient's abnormal or deteriorating condition and allows them to intervene and prescribe treatment.

IoT facilitates the management and treatment of chronic diseases. These conditions require sustained treatment and monitoring. Additionally, care coordination between multiple caregivers is often required. Treatment usually requires patients to adhere to a care plan and success depends on patients doing certain activities or taking medication on a regular basis.

Remote patient monitoring can track the patient's health conditions over time to see if treatment is efficacious and doctors can be proactively notified of abnormal or deteriorating conditions.

Patient non-adherence to medication is a common problem. IoT based medication tracking reminds patients to take their medicine at the appropriate dosages and times supporting their recovery.[1092]

[1090] IoT devices used outside of clinical may also be subject to FDA regulations as long as they are classified as medical devices.

[1091] "The Medical Internet of Things", Thales. Link

[1092] "IoT and Health: Keeping track of your meds," Tele2. Link

© Strategy of Things, 2025. All rights reserved.

The ongoing healthcare workforce shortage is a major challenge for Healthcare Delivery Organizations (HDO) in delivering treatment and care. This shortage means patients may not be able to see doctors in a timely manner or doctors may not be able to spend quality time treating patients.

IoT technologies help HDOs alleviate some of the problems by becoming more efficient and productive with the existing resources and workers. The pairing of medical devices with IoT and AI technologies can facilitate the diagnosis of patient conditions by efficiently analyzing large amounts of data collected to provide doctors with insights that lead to treatments.

Wearable health trackers facilitate the treatment of patients with intermittent conditions, such as heart arrhythmia, which often occurs outside of doctor appointments. The ability of smart watches to capture this information in real time and share it during an appointment helps doctors prescribe effective treatments while reducing the number of office visits.

The value provided by IoT in the healthcare industry is reflected in market adoption. The global IoT market for healthcare was around $71.84 billion in 2020 and is expected to grow at least 4-fold to $446.52 billion by 2028.[1093]

Many of these IoT devices will be used in hospitals. Industry analyst Juniper Research projected that 7.4 million connected IoMT devices will be deployed in hospitals globally by 2026 or about 3,850 devices per smart hospital. This number represents a 131% increase over 2021. Nearly 1 in 5, or 21%, will be deployed in hospitals in the United States.[1094] According to Deloitte, 68% of medical devices produced are expected to be connected.[1095]

19.2.1. IoT use cases

Figure 19-4 shows a representative set of healthcare use cases organized into four categories. These categories are:

- **Healthcare provider.** The use of IoT involved in the delivery of healthcare services to the patient.
- **Medical equipment.** The integration of IoT with medical equipment such as diagnostic, imaging, surgical and therapeutic.
- **Managed healthcare.** The use of IoT to support healthcare delivery services.
- **Drugs.** The use of IoT to support and manage medication usage, inventory and supply chain and trials.

[1093] "Internet of things (IoT) in healthcare market size, share & COVID-19 impact analysis." Fortune Business Insights. Link

[1094] "Smart Hospitals to Deploy Over 7 Million Internet of Medical Things," Juniper Research, January 2022. Link

[1095] "10 internet of things (iot) healthcare examples", ordr. Link

© Strategy of Things, 2025. All rights reserved.

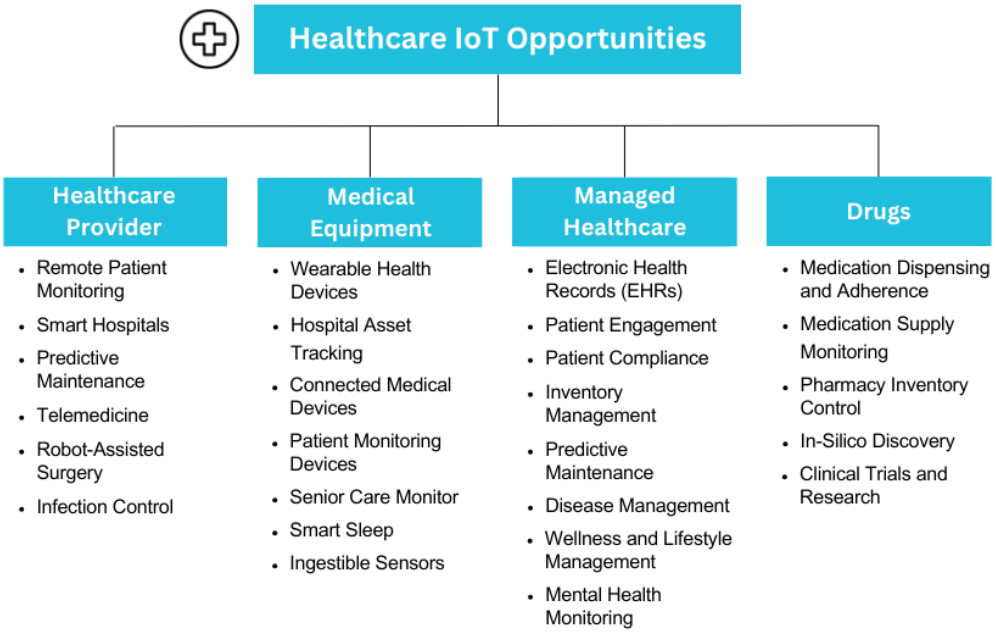


Figure 19-4: Healthcare: Use Case Categories and Selected Use Cases

19.2.1.1. Use case and industry challenges alignment

The healthcare industry faces several challenges, some of which are described in Section 19.1.2. Figure 19-5 below shows the fit between the proposed use case subcategories and the documented industry challenges.

© Strategy of Things, 2025. All rights reserved.

Challenge	Role of IoT	Use case examples
Rising healthcare costs	Help control rising healthcare costs by enabling remote patient monitoring and telemedicine, reducing the need for hospital visits and stays.	• Predictive maintenance • Hospital asset tracking • Inventory management • Predictive maintenance • Pharmacy inventory control • Medication supply monitoring • Electronic Health Records (EHRs)
Access to healthcare	Improve access to healthcare by enabling remote consultations and treatments, making healthcare services accessible to people in remote areas or those with mobility issues.	• Telemedicine • Connected medical devices • Patient engagement • Wellness and lifestyle management • Patient compliance • Patient monitoring devices • Senior care monitor • Wearable health devices
Chronic disease management	Wearable health monitors can provide continuous data on a patient's health, enabling better management of chronic diseases through timely interventions.	• Remote patient monitoring • Infection control • Smart sleep • Ingestible sensors • Disease management • Mental health monitoring • Medication dispensing and adherence

© Strategy of Things, 2025. All rights reserved.

Challenge	Role of IoT	Use case examples
Healthcare workforce shortage	Address workforce shortages in healthcare by automating routine tasks, such as patient monitoring and data collection, freeing up healthcare professionals to focus on more complex tasks.	• Smart hospitals • Robot-assisted surgery • In-silico discovery • Clinical trials and research

Figure 19-5: Healthcare: Use Case and Industry Challenges Alignment

19.2.1.2. IoT use case details

Figure 19-6 below provides details for each case use as shown in Figure 19-4.

Category	Use case	Definition
Healthcare provider	Remote Patient Monitoring	A form of telehealth that allows providers to monitor and manage patients' chronic conditions.
	Smart Hospitals	Hospitals which optimize, redesign and transform clinical processes as part of smart clinics, smart hospital management system.
	Predictive Maintenance	Uses regular, continuous inspections to assess the need for maintenance to prevent breakdown.
	Telemedicine	Allows a person to seek a doctor's advice about nonemergency situations that do not require an in-office visit.
	Robot-assisted surgery	Allows doctors to perform many types of complex procedures with more precision, flexibility and control than is possible with conventional techniques.
	Infection Control	Infection control prevents or stops the spread of infections in healthcare settings.

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Definition
Medical Equipment	Wearable Health Devices	These are devices that patients attach to their bodies to collect health and fitness data, which they may provide to doctors, health providers, insurers and other relevant parties.
	Hospital Asset Tracking	Hospital asset tracking systems are used for medication, tools and equipment monitoring. They can substantially decrease the loss of hospital assets, cut asset search time, provide real-time data on the assets' use, help monitor medication storage conditions and plan equipment maintenance.
	Connected Medical Devices	Connected medical devices are new medical instruments that provide detailed information on status.
	Patient Monitoring Devices	These devices include weight scales, pulse oximeters, blood glucose meters and blood pressure monitors.
	Senior Care Monitor	Using technology to monitor the health and well-being of seniors. It can include wearable devices that track vital signs, fall detection systems and remote monitoring tools.
	Smart Sleep	Wearable devices that track sleep patterns, smart mattresses and apps that provide insights and recommendations for better sleep.
	Ingestible Sensors	Tiny sensors that can be swallowed and used to monitor various aspects of health from within the body. They can track medication adherence, monitor vital signs or provide images of the gastrointestinal tract.
Managed Healthcare	Electronic Health Records (EHRs)	Digital versions of a patient's medical history maintained by healthcare providers. They include key clinical data like demographics, progress notes, medications, vital signs, past medical history, immunizations, laboratory data and radiology reports.
	Patient Engagement	Patients actively participate in their healthcare. This includes understanding their treatment options, making informed decisions about their care and taking an active role in managing their health.

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Definition
	Patient Compliance	Patients follow the care plan prescribed by their healthcare providers. It includes taking medications as prescribed, following recommended lifestyle changes and attending follow-up appointments.
	Inventory Management	Tracking and managing medical supplies and equipment.
	Predictive Maintenance	Using data analysis to predict when medical equipment might fail so that maintenance can be performed in advance. This helps to prevent equipment downtime and improve patient care.
	Disease Management	A coordinated approach to healthcare for patients with chronic diseases. It involves educating patients on how to manage their disease, monitor their condition and prevent complications.
	Wellness and Lifestyle Management	Helping individuals make healthy lifestyle choices to prevent disease and improve overall health. It can include nutrition counseling, exercise programs and stress management techniques.
	Mental Health Monitoring	Monitoring an individual's mental health. It can include self-reporting tools, wearable devices that track physiological indicators of stress or mood and telehealth services for remote counseling.
Drugs	Medication Dispensing and Adherence	Strategies to ensure that patients take their medications as prescribed. It can include pill dispensers with alarms, medication reminder apps and programs that provide education about the importance of medication adherence.
	Medication Supply Monitoring	Tracking the supply of medications to prevent shortages or overstocking. It can include inventory management systems that track point of medication usage and alert staff when supplies are low.
	Pharmacy Inventory Control	Like medication supply monitoring but specific to pharmacies. This involves tracking the stock of medications in a pharmacy to ensure that there is enough supply to meet patient demand.
	In-silico Discovery	The use of computer simulations or computational models to discover new drugs or understand biological phenomena.

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Definition
	Clinical Trials and Research	These are studies conducted with patients to evaluate new treatments or interventions.

Figure 19-6: Healthcare: Use Case Details

© Strategy of Things, 2025. All rights reserved.

19.2.2. Market views of IoT in healthcare

To understand market views on IoT and to inform on our gaps discovery and analysis, our research team conducted a survey of 450 people, from adopters to solution providers, across the nine industries studied. Survey respondents were asked their opinion on the importance of IoT for the healthcare industry over the next 5 to 10 years. Figure 19-7 below shows an expected relative high impact of IoT, as compared to other industries.

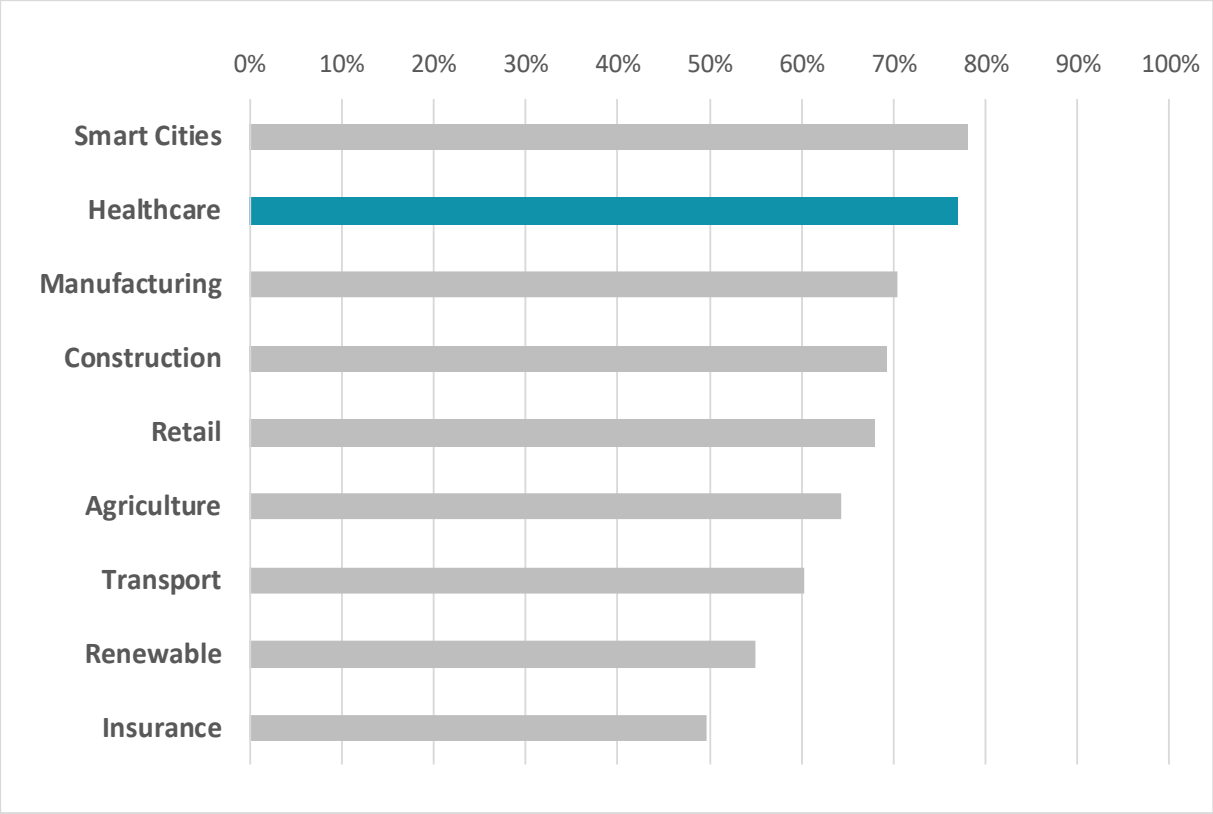


Figure 19-7: Healthcare: Importance of IoT

Survey respondents were asked to rate the impact of these use case categories on the healthcare industry.[1096] Figure 19-8 below shows the percentage of responses in each impact category for each use case category. Overall, this shows a bias to a moderate to high impact of the use case categories in healthcare.

[1096] In your view, what will be the impact of these use cases in healthcare over the next 5-10 years?

© Strategy of Things, 2025. All rights reserved.

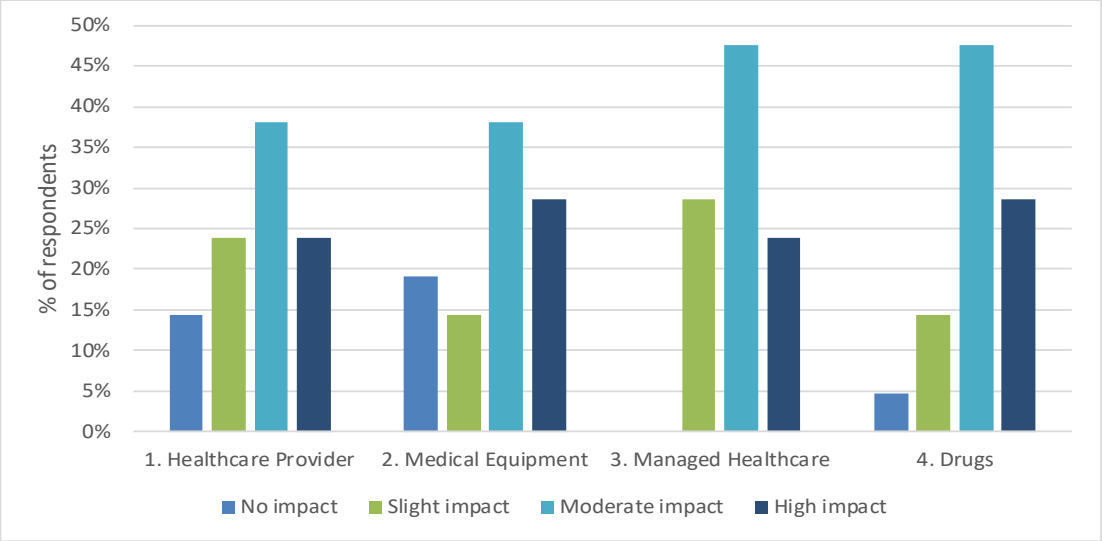


Figure 19-8: Healthcare: Use Case Category Impact

In addition, respondents were asked about their confidence in suppliers delivering the services required to operationalize these use case categories.[1097] Figure 19-9 below shows the percentage of responses in each confidence category for each use case category. Overall, their responses indicate some confidence in the ability of suppliers to deliver the necessary services.

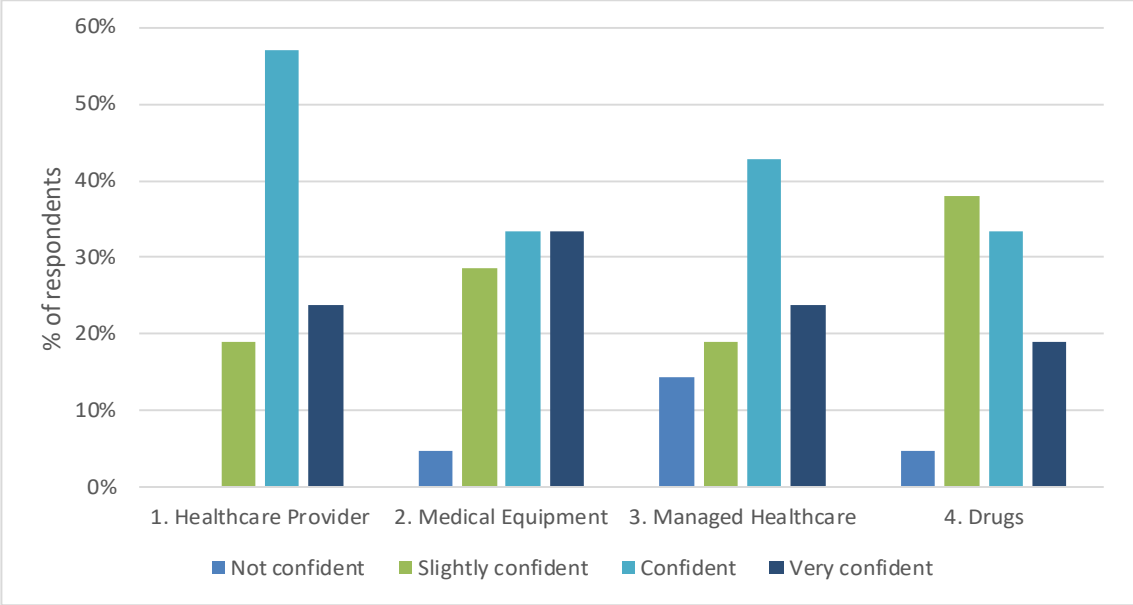


Figure 19-9: Healthcare: Confidence in Suppliers Delivering

[1097] How confident are you that suppliers will deliver the services that healthcare organizations need from these technologies over the next 5-10 years?

© Strategy of Things, 2025. All rights reserved.

19.3. IoT gaps and findings in healthcare

A combination of interviews, secondary research and surveys were conducted to identify and understand the opportunities and challenges to the development and adoption of IoT. Each research method approached the challenges from a different perspective.

For example, the survey targeted a large audience but asked specific questions that supported the economic analysis. The interviews targeted a small number of people who provided deeper insight and context to supplement the information already collected. Finally, the desk research, consisting of a review of online news articles, published research reports, vendor and government white papers, blogs, webinars, videos and other content, provided a broad overview of the application of IoT in the industry.

In our survey, respondents were asked to choose the most important technology areas to operationalize IoT in their industry. Figure 19-10 below shows respondent's selections of the top 10 IoT technologies and the percentage of respondents who chose that technology.[1098] The survey results are not seen as a technology gaps list, but rather an indication of what is important to the respondents. This information partially informs the gap selection process.

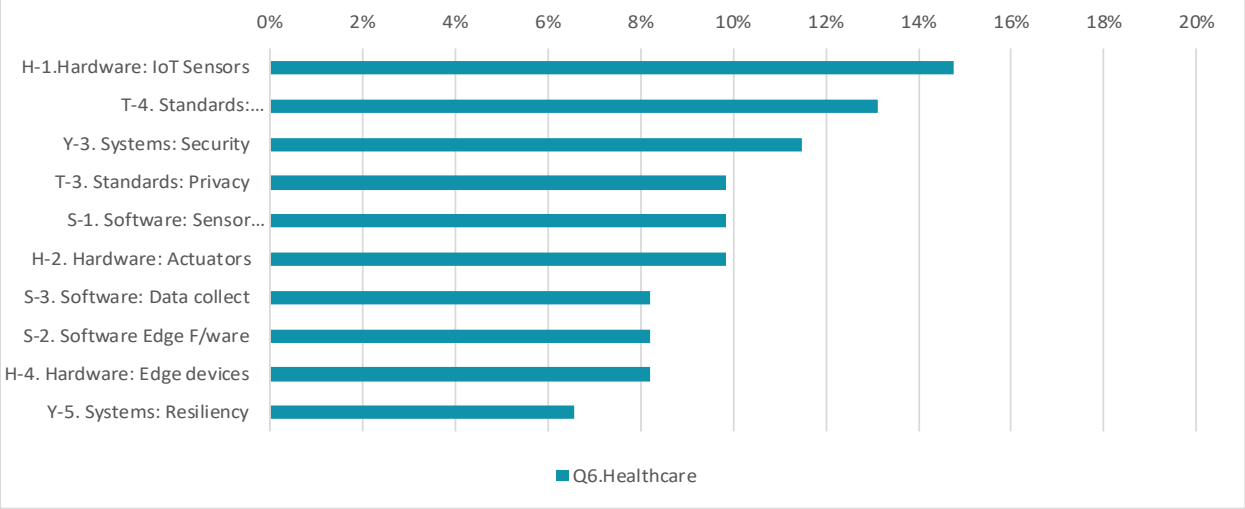


Figure 19-10: Healthcare: Top 10 Most Important Single Technologies

[1098] Respondents were asked to choose up to 5 out of the 25 technologies listed.

© Strategy of Things, 2025. All rights reserved.

19.3.1. Top technology challenges

Based on the approach described above, the following three IoT technology challenges were identified as listed below:

- Cybersecurity
- Interoperability
- Artificial Intelligence

Each of these is discussed below:

19.3.1.1. Challenge #1: Cybersecurity

Cybersecurity is a major concern for connected healthcare devices and IoMT. Cyberattacks may expose sensitive and private patient data, disrupt the operations of medical devices and put patients' lives at risk and disrupt the operations of healthcare providers.

A 2023 report from Asimily stated that these attacks are responsible for a 20% increase in patient mortality and cost healthcare providers or Health Delivery Organizations (HDO) an average of $10.1 million per incident. For example:

- Nearly two-thirds, 64% of 641 organizations surveyed, suffered operational delays and 59% had longer patient stays.[1099] A woman sued an Alabama hospital for providing "severely diminished" care during childbirth, citing the impact of a ransomware attack that locked down hospital systems, preventing crucial tests, leading to brain damage and the subsequent death of her baby nine months later due to an undetected umbilical cord entanglement.[1100]
- A study of 200,000 infusion pumps, medical devices that deliver fluids and medicine to a patient's body in a controlled manner, found that 75% of the units scanned had known cybersecurity vulnerabilities. Six of the top ten vulnerabilities were considered critical and two more were considered high risk.[1101]

The Asimily report indicated that the average healthcare provider or HDO experienced 43 attacks a year. Of those cyberattacks, 44% of HDOs suffered a data breach caused by a third party.[1102]

[1099] "Total Cost of Ownership Analysis on Connected Device Cybersecurity Risk," Asimily Report, 2023. Link

[1100] "Baby died because of ransomware attack on hospital, suit says," K. Collier, NBC News, September 30, 2021. Link

[1101] "Know Your Infusion Pump Vulnerabilities and Secure Your Healthcare Organization," A. Das, Unit 42, Palo Alto Networks, March 2, 2022. Link

[1102] "Total Cost of Ownership Analysis on IoMT Cybersecurity Risk , August 2023. "Link

© Strategy of Things, 2025. All rights reserved.

The average medical device has 6.2 vulnerabilities. This challenge is exacerbated by the fact that more than 40% of medical devices are near end-of-life and poorly or unsupported by the device manufacturers.[1103]

The same report identified the top cyberattack strategies used were "ransomware attacks that spread to devices and disrupt services, third-party introduced malware that impacts device performance and devices communicating with unknown IP addresses to enable remote breaches."[1104]

These cyberattacks put HDOs at financial risk as hospitals often have low operating margins. For example, the median operating margin was 0.4% in March 2023.[1105] This suggests that fixing and recovering from a cyberattack could put smaller HDOs out of business.

Nearly one third, 30%, of rural U.S. hospitals are at heightened financial risk. Reliance on cyber insurance to offset the financial impacts of a cyberattack has limited effectiveness as insurers are introducing coverage limits and capping payouts.[1106]

A 2023 Cybersecurity Risk analysis reported that the healthcare industry has an average loss exposure (probable likelihood and probable financial impact) of $5.5 Million per attack scenario.[1107]

> These scenarios include insider misuse, web application attack, system intrusion, insider error, ransomware, social engineering and denial of service attacks. Extracted from Section 14.3.1

IoMT and medical devices face several cybersecurity challenges. These include

- **Update risk**: Medical devices have long operational lives ranging from 10 to 30 years. The software that operates these devices may have update cycles that vary from months to years. Many devices are built on embedded system platforms that have been customized by the manufacturers, are built on platforms with limited computing resources and are memory limited such that a quick patch in reaction to a cybersecurity vulnerability is not realistic.[1108] Devices with fewer frequent updates are at higher risk of outdated software which is susceptible to the cybersecurity vulnerabilities.[1109]

[1103] See note 1102

[1104] See note 1102

[1105] "Hospital margins crawl into black for March, report finds," N. Schwartz, Beckers CFO Report, May 12, 2023. Link

[1106] "More Than 30% of Rural Hospitals Are at Risk of Closure, Report Warns , Med City News ", July 2023. Link

[1107] "2023 Cybersecurity Risk Report", RiskLens, 2023. Link

[1108] Ken Fuchs, IEEE 11073 Standards Committee Chair, IHE DEV Domain Co-Chair.

[1109] "Unpatched and Outdated Medical Devices Provide Cyber Attack Opportunities," Private Industry Notification 20220912-001, Federal Bureau of Investigation Cyber Division, September 12, 2022. Link

© Strategy of Things, 2025. All rights reserved.

- **Limited authentication**: Many medical devices, especially legacy and early generation models, were not designed with cybersecurity protections.[1110] For example, many devices collect and access patient data without requiring user authentication or credentials.[1111]

  This "free" access to the patient data and other information stored on the network makes medical devices an entry point for cybercriminals.[1112] While the FDA implementation guidance on cybersecurity requirements for medical device premarket submissions went into effect on October 1, 2023, it does not apply retroactively to devices submitted for review.
- **Small HDO risk**: Legacy devices continue to be in use and are often purchased by smaller HDOs who are also less able to address cybersecurity issues.[1113] A study found that small U.S. hospitals suffer 53% of the data breaches compared to 10% for large hospitals and 36% for medium size hospitals.[1114]
- **Resource constrained medical devices.** Wearables and other medical devices are small, low power and lightweight to avoid impeding other bodily functions and to extend battery life. As a result, medical devices often have limited capabilities to perform computation, security and encryption tasks. As a result, these devices have limited to no cybersecurity capabilities.[1115]
- **Networks not properly configured for cybersecurity.** A hospital's network connects a variety of computers, servers, IP phones, medical devices and mobile devices. Network segmentation, also known as virtual local area networks, is a cybersecurity best practice that isolates devices in one network segment from those in another segment.

  A study by Forescout, a cybersecurity software company, found that nearly half of the HDOs surveyed (49%) had 10 zones (network segments) or less.[1116] An insufficient number of segments means that a device that is introduced locally can potentially allow a

[1110] On October 1, 2023, the FDA implementation guidance on cybersecurity requirements for medical device premarket submissions went into effect. The Guidance outlines the implementation of new Section 524B of the Federal Food, Drug and Cosmetic Act (FDCA), which requires that manufacturers submitting premarket submissions for cyber devices meet specific cybersecurity requirements.

[1111] User authentication (logins, passwords) can get in the way of device usability, especially in areas such as an OR or ICU and therefore is not practical in all cases.

[1112] "What Poor Cybersecurity and a Lack of Digital Hygiene Means for Medical IoT in Healthcare," P. Howe, The Journal of mHealth, December 22, 2022. Link

[1113] "Next steps toward managing legacy medical device cybersecurity risks," Mitre Corporation, November 2023. P. 6. Link

[1114] "Patient safety and the Internet of Medical Things (IoMT)," K. Stockdale, OR Manager, November 17, 2021. Link

[1115] "The Unique Cyber Vulnerabilities of Medical Devices," R. Pallardy, Information Week, November 14, 2023. Link

[1116] "Network segmentation is a security best practice, but is adoption lagging in healthcare?" D. Wolf, Forescout blog, October 16, 2019. Link

© Strategy of Things, 2025. All rights reserved.

lateral cyberattack to other medical and non-medical systems and devices in the network.

While industry is actively developing and implementing solutions to alleviate these concerns, there are opportunities for research to address emerging threats, improve the resilience of healthcare systems and ensure the privacy and security of sensitive medical data.

Protection of medical data remains a priority because of the sensitivity of medical records. Research opportunities exist in encryption, secure networks and authentication and access controls to prevent access to collected, transmitted or stored data. Some examples of opportunities include:

- Lightweight encryption algorithms designed to work with resource constrained IoMT devices that provide strong cybersecurity.[1117]
- Alternative approaches to cryptography such as "friendly jamming" that can be used with existing resource constrained devices and do not require extra computing power.[1118]
- Development of lightweight quantum safe algorithms that are suitable for use on resource constrained IoT devices[1119]
- Integration of blockchain with IoMT to enhance data security and management[1120]
- The use of privacy enhancing technologies in protecting patient data collected through IoMT and other medical devices.[1121]
- The use of AI in combating cyberattacks, such as intrusion detection, on IoMT devices.[1122]

19.3.1.2. Challenge #2: Interoperability

There is a wide range of healthcare and medical devices in use from consumer wearable fitness trackers, ambulance-mounted equipment and clinical grade mobile and stationary devices. The ability of these devices to communicate and exchange information with each other and medical

[1117] "LSEA-IOMT: On the Implementation of Lightweight Symmetric Encryption Algorithm for Internet of Medical Things (IoMT)," S. Saif, P. Das and S. Biswas. Lecture Notes in Networks and Systems, vol 519. Springer, Singapore. Link

[1118] "Securing Internet of Medical Things with Friendly-jamming schemes," X Li, H. Ning Dai, et al. Computer Communications, Vol 160, pp 431-442. July 1, 2020. Link

[1119] "Post-Quantum Cryptography: Securing IoT Networks for the Future," H. Ravilla, LinkedIn Post, June 23, 2023. Link

[1120] "Blockchain-Assisted Cybersecurity for the Internet of Medical Things in the Healthcare Industry," M. Alkatheiri and A. Alghamdi, Electronics 2023, 12(8), 1801. Link

[1121] "How Privacy-Enhanced Technologies (Pets) are Transforming Digital Healthcare Delivery," P. Nivarthi, K. S. American Scientific Research Journal for Engineering, Technology and Sciences, 90(1), 351–361. 2022. Link

[1122] "Artificial intelligence for IoMT security: A review of intrusion detection systems, attacks, datasets and Cloud–Fog–Edge architectures," M. Hernandez-Jaimes et al, Internet of Things Volume 23, October 2023, 100887. Link

© Strategy of Things, 2025. All rights reserved.

systems is essential to timely and responsive care, automation of manual processes and operational efficiency.[1123]

As an example, a patient with a chronic health condition could wear various IoMT devices such as a continuous glucose monitor or a wearable ECG monitor. These devices continuously collect health data, which is transmitted to a home health hub. The hub aggregates these data and integrates it into the patient's Electronic Health Records (EHR) system. Healthcare providers access this EHR through a platform, allowing them to remotely monitor the patient's health in real-time.

If any anomalies are detected, alerts are triggered, enabling timely interventions and adjustments to the patient's treatment plan. This scenario is possible if the home health hub, the EHR system and the healthcare provider platform support the same standards, to allow seamless communication and exchange of information.

Attaining interoperability is challenging. The Deloitte Center for Health Solutions, in a 2018 report, identified three barriers hindering interoperability. These are:[1124]

- Privacy and security challenges associated with widespread health information exchange. Concerns regarding violations of the Health Information Portability and Accountability Act (HIPAA) hindered the development of interoperability.
- Lack of incentives for the private sector to develop interoperability.
- Lack of adoption of standards based EHR systems.

For example, patient data are often stored in silos, with different systems using incompatible formats. This results in medical records that are "notoriously balkanized in EHR frameworks, wherein a patient's health information may be spread across wearable devices used in the home, outpatient clinics and hospital care resulting in any one clinician seeing only a portion of a patient's full picture of health or illness."[1125]

In addition, healthcare and medical devices come from a variety of manufacturers and employ different and proprietary data formats and communication protocols. While HDOs have addressed this situation through the use of middleman organizations that convert data from one proprietary protocol to another, this approach adds cost and complexity to the process of integrating medical devices.[1126] Developing standards for medical devices is complicated as device identity standards vary across device classes because of the wide range of technologies used in patient care from automated blood pressure cuffs to ventilators and the varying technical complexity used in their manufacture.

[1123] "The case for medical device interoperability," V. Gowda, H. Schulzrinne and B. Miller. JAMA Health Forum, January 14, 2022. Link

[1124] "Medtech and the Internet of Medical Things: How connected medical devices are transforming health care," Deloitte Center for Health Solutions, July 2018. Figure 9. Link

[1125] See note 1123

[1126] Ken Fuchs, IEEE 11073 Standards Committee Chair, IHE DEV Domain Co-Chair.

© Strategy of Things, 2025. All rights reserved.

Interoperability can be modeled along a continuum from data to communication on to semantic and workflow. Different medical devices may be at different places on this continuum, ranging from basic interoperability that covers data to plug-and-play workflow interoperability.[1127]

While many medical devices can communicate today, they do so with "dysfunctional interoperability" as proprietary protocols make it difficult to extract the information.[1128]

In a clinical practice, interoperability concerns lead to poor safety, poor prioritization, lost and missing data, inefficiency, reluctance to standardize processes, inability to measure and improve care and failure to transfer and disseminate successes.[1129]

One significant consequence of poor interoperability is patient safety. Poor interoperability slows healthcare systems from "early detection and prevention of adverse events, such as medication errors, lack of patient monitoring or assessment and patient deterioration."[1130]

A 2013 analysis by the West Health Institute found that medical device interoperability would help to mitigate waste and could lead to $35 billion in annual savings across the U.S. healthcare system. This includes:[1131]

- $2 billion in cost savings from avoidable adverse events including drug errors, diagnostic errors and failures to prevent injuries.
- $3 billion in cost savings from redundant testing.
- $12.4 billion in cost avoidance from clinician time spent manually entering information.
- $17.8 billion in cost avoidance from increased hospital length of stay.

A majority (93%) of those savings are realized by healthcare providers, with the remaining 6% realized by payers and 1% by patients.[1132]

There are ongoing industry efforts to develop consensus standards including:

- Integrating the Healthcare Enterprise (IHE) promotes the coordinated use of established standards such as DICOM and HL7 to address specific clinical needs in support of optimal patient care.
- Devices Domain which seeks to enable the integration of healthcare devices, typically via translators, with other IT solutions such as Electronic Health Records (EHR).
- Service-oriented Working Groups in Health Level 7 International (HL7) looking at Fast Healthcare Interoperability Resources (FHIR).

[1127] "Medical device interoperability. A safer path forward." Priority Issues from the 2012 AAMI-FDA Summit. AAMI. 2012. P. 11. Link

[1128] Ken Fuchs response comment to article in Note 1123. Link

[1129] See note 1127 P. 11. Link

[1130] See note 1129 p. 9.

[1131] "The value of medical device interoperability," West Health Institute, 2013. Link

[1132] See note 1131. Figure 3.

© Strategy of Things, 2025. All rights reserved.

In addition, there are several efforts around open health device interoperability standards, including the Association for the Advancement of Medical Instrumentation (AAMI) 2700 series looking at high level architectures, AAMI/UL (Underwriters Laboratories) 2800 looking at process-oriented interoperability and ISO/IEEE 11073 which covers point of care medical device communication.

The Deloitte report suggested that "open platforms, based on open data standards is the direction of travel that needs to be followed to enable payers, providers and technology vendors to finally come together to make data more available to one another."[1133] While some efforts led to commercial adoption of standards (e.g. IHE Devices), the adoption of open interoperability standards at the device level has "fallen flat."[1134] This is attributed to the continued use of legacy devices, a lack of a business case for device manufacturers to move away from proprietary solutions and a lack of healthcare providers asking for open interoperable interfaces.

The Digital Imaging and Communications in Medicine (DICOM) standard, a widely used international standard for the exchange, storage and communication of medical images, represents a rare example of a successful adoption of an open standard in the healthcare industry.

Continued efforts from industry stakeholders, regulatory bodies and healthcare organizations to attain interoperability across the healthcare industry are needed to realize patient outcomes, operational efficiencies and economic benefits.

While industry is developing standards, some have called upon the U.S. Food and Drug Administration to facilitate the development of an industry wide medical IoT harmonization initiative. These include retooling of existing interoperability efforts and security standards (e.g., HTTPS, W3C, Web of Things) to accommodate the specific functions of medical devices and address cybersecurity concerns" instead of creating new IoT-specific standards.[1135] Other representative opportunities to advance interoperability include:

- Development of standards for medical device and system security. Interoperability to reduce the potential for medical devices and systems, as well as the data they store, transmit, or share, to be breached or compromised.[1136]
- Address gaps targeting specific needs in existing standards. There is significant variability across clinical, health IT and organizational practices, which makes it difficult to develop "universally applicable" technical standards.[1137]
- Address interoperability challenges between different IoMT platforms with semantic web technologies.[1138]

[1133] See note 1124. P21.

[1134] See note 1128

[1135] See note 1123

[1136] See note 1127. P. 14.

[1137] See note 1127. P. 14.

[1138] "A Semantic Interoperability Approach to Heterogeneous Internet of Medical Things (IoMT) Platforms," I. Villanueva-Miranda, H. Nazeran and R. Martinek, 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services, September 2018. Link

© Strategy of Things, 2025. All rights reserved.

- Use AI-based systems to facilitate interoperability. AI algorithms can process and translate data from one system into a format compatible with another, extract meaningful information from unstructured data sources and convert to structured data.[1139]

19.3.1.3. Challenge #3: AI

AI is well suited for applications that require analyzing large amounts of data leading to diagnoses and predictions.[1140] The United States Government Accountability Office (GAO), in its technology assessment report on AI in healthcare, identified five categories of clinical applications where AI can augment patient care. These are:[1141]

- Predicting health trajectories
- Recommending treatments
- Guiding surgical care
- Monitoring patients
- Supporting population health management

As an example, the pairing of glucose monitoring with an AI-powered mobile application has allowed for highly personalized and effective care.[1142] The application employs an AI algorithm to "evaluate blood sugar data, identify concerning trends and recommend steps to help patients keep their glucose levels within a healthy range."[1143]

While AI offers significant benefits for patient care, its adoption is slow with less than 5% of healthcare organizations using AI tools.[1144] Slowing the adoption of AI in healthcare are several technical and non-technical challenges. Some of the technical challenges associated with the integration of AI and IoMT include:

- **Limited access to high quality data.** AI algorithms depend on data for training, building, refining and validating models. These data, however, come from disparate and siloed sources such as imaging and diagnostic systems, electronic health records and other databases. Adding to the challenge is that the data from different sources are not

[1139] "How AI untangles interoperability challenges," ClearStep. Link

[1140] "AI in healthcare is here, but uptake is slow," T. Dai, A. Ching, et al., Johns Hopkins University, November 18, 2022. Link

[1141] "Artificial Intelligence in Health Care," Technology Assessment GAO -21-7SP, United States Government Accountability Office and National Academy of Medicine, November 2020. P. 9. Link

[1142] "Revolutionizing healthcare: the integral role of AI and IoT in shaping modern medicine," R. Saluja. Forbes, February 14, 2024. Link

[1143] "Artificial intelligence, diabetes experts combine forces for blood sugar management study," F. White, OHSU, January 10, 2023. Link

[1144] See note 1140

© Strategy of Things, 2025. All rights reserved.

fully interoperable and are in various formats that are not easily aggregated and reconciled.[1145]

- **Biased data.** The AI algorithms may not yield the intended outcomes as the underlying training data may not be representative of the patient population being treated. For example, the data may come from a subset of the population instead of a more representative group. In addition, the dataset may not be sufficient size for certain patient subgroups. Finally, data based on documentation and clinical reasoning of previous patients are less accurate or may differ across sites.[1146] The bias in the data may lead to incorrect or inappropriate treatment recommendations, leading to non-optimal, ineffective or unsafe outcomes.
- **Lack of transparent and explainable models.** The results and outcomes from the AI algorithms may not be easily explainable based on the underlying decision-making or inference patterns.[1147] The models may not always be peer reviewed nor shared with others because of intellectual property concerns. The inability to explain outcomes makes it difficult for physicians, regulators and others to determine whether a model is safe, usable and supports efficacious outcomes.
- **Data Privacy.** The data collected from IoMT and medical devices contain sensitive patient data. These data are used to develop AI models, as well as used by AI models to treat patients. The data, however, may be accessed by cybercriminals or shared, sold and used without the patient's consent. Some data, while anonymized, may potentially be reconstituted and allow patients to be identified.[1148] These concerns may lead patients to withhold data or forgo certain treatments.
- **High resource requirements.** Some advanced AI algorithms, especially deep learning models, can be computationally intensive. These resource-intensive AI applications may not be able to operate on IoMT devices with limited processing power and energy resources.
- **Limited ability to scale into clinical practices.** AI models may not always be effectively or easily integrated into existing clinical workflows and practices. Models developed in one setting may not easily be transferrable to another setting.[1149] For example, models developed for a high resource hospital may recommend treatments and access to specialists not available in rural or community hospitals. In other cases, the model may need to be retrained in the new setting though the cost of retraining may be high.

Several research opportunities are needed to address these challenges. Examples include:

- **AI explainability and interpretability.** Rapid advances in AI were made possible using "black box" approaches, such as deep learning. These "black box" models, however,

[1145] See note 1141. P. 22.

[1146] See note 1141. P. 24.

[1147] See note 1141. P. 26.

[1148] See note 1141. P. 28.

[1149] See note 1141. P. 25.

© Strategy of Things, 2025. All rights reserved.

produce decisions and outcomes that are not easily explained as compared to their less powerful and accurate "white box" counterparts (linear and decision tree methods). Development of methods and tools (explainable AI) that explain and interpret machine learning and AI models is required to build trust in the decisions and recommendations.[1150]

- **Addressing AI bias.** The development of strategies and techniques to identify and remove bias in datasets is critical to the development of "fair" AI algorithms. This includes methods for preprocessing the data used to train the models, as well as designing "fair and accountable" algorithms.[1151] Another area of research is developing "technical ways of defining fairness, such as requiring that models have equal predictive value across groups or requiring that models have equal false positive and false negative rates across groups."[1152]
- **Addressing interoperability challenges that hinder access to data.** The inability to source and standardize data hinders the development of AI algorithms. The data required comes from a variety of sources such as medical devices and IoMT to EHR systems.

19.3.2. Other challenges

In addition to the technology challenges for further consideration, our research has identified other challenges that impact IoT adoption. These challenges did not meet the criteria for research consideration because they were either not a technology challenge or a technology related challenge that can be addressed by current marketplace offerings or capabilities. These are:

- Regulatory compliance challenges
- Consumer IoT device privacy

Each of these is discussed below.

19.3.2.1. Regulatory compliance challenges

Medical and IoMT devices are subject to several regulations. While these regulations are intended to create products that are safe and secure, compliance poses challenges for healthcare providers, health delivery organizations, IoMT manufacturers and third-party vendors and service providers.

The two most important regulations that cover IoMT are HIPAA and FDA medical device regulations. Each of these is discussed below.

[1150] "Explainable AI: A Review of Machine Learning Interpretability Methods," P. Linardatos, et al., Entropy (Basel). 2021 Jan; 23(1): 18. Published online 2020 Dec 25. Link

[1151] "Artifical Intelligence and Bias: Challenges, Implications and Remedies," A. Min, October 2023Journal Of Social Research 2(11):3808-3817. Link

[1152] "What Do We Do About the Biases in AI?" J. Manyika, J. Silberg, B. Presten., Harvard Business Review, October 25, 2019. Link

© Strategy of Things, 2025. All rights reserved.

- **HIPAA.** Healthcare organizations in the United States are required by the Health Insurance Portability and Accountable Act of 1996 (HIPAA) to "protect the confidentiality of patient health information which is generated or maintained in the course of providing health care services."

  This includes the use and disclosure of "Protected Health Information" (PHI) related to the patient's health, the services rendered and the payment for these services, as well as the management of electronic protected health information (EPHI) and the prevention of access to that information by unauthorized persons.[1153]

  Breaches of unsecured PHI must be disclosed to the affected individuals, the Secretary and the media if appropriate.[1154]
- **FDA medical device regulations.** The U.S. Food and Drug Administration (FDA) regulates medical devices, including the Internet of Medical Things (IoMT), to ensure their safety and effectiveness.

  Before a medical device can be introduced into the market, manufacturers must apply to be reviewed and approved by the FDA. Class II devices[1155] must "demonstrate that the device to be marketed is as safe and effective, that is, substantially equivalent, to a legally marketed device (section 513(i)(1)(A) FD&C Act)"[1156] while Class III devices[1157] must show "sufficient valid scientific evidence to assure that the device is safe and effective for its intended use(s)."[1158]

  Long-held concerns about the medical device cybersecurity have led to the implementation of a new requirement, which took effect on October 1, 2023, that mandates device manufacturers to include in their application "plans to monitor, identify and address, in a reasonable timeframe, all post-market cybersecurity vulnerabilities and exploits through coordinated vulnerability disclosures and response plans."[1159]

IoMT devices collect, transmit and store PHI. Healthcare organizations using IoMT technologies must ensure that these devices comply with HIPAA requirements for PHI protection. This

---

[1153] "HIPAA Basics Overview," University of Wisconsin, Milkwaukee. Link

[1154] "Breach Notification Rule," U.S. Department of Health and Human Services. Link

[1155] The FDA defines Class II devices as "devices for which general controls are insufficient to provide reasonable assurance of the safety and effectiveness of the device." Examples include catheters, blood pressure cuffs, contact lens, syringes, blood transfusion kits.

[1156] "Premarket Notification 510(k)." U.S. Food & Drug Administration. Link

[1157] The FDA defines class III devices as products which "usually sustain or support life, are implanted or present a potential unreasonable risk of illness or injury." Examples include pacemakers, defibrillators, high frequency ventilators. 10% of products regulated by the FDA fall are Class III devices.

[1158] "Premarket Approval (PMA)." U.S. Food & Drug Administration. Link

[1159] "Oct. 1 Deadline for FDA Medical Device Cyber Standards: How Providers Should Prepare," First Health Advisory, August 17, 2023. Link

© Strategy of Things, 2025. All rights reserved.

requires ensuring privacy through informed patient consent, implementing robust security safeguards and establishing Business Associate Agreements (BAAs) with third-party vendors.

As the variety of IoMT devices scale in healthcare networks, the complexity and challenge of complying with government regulations grows in proportion. Non-compliance with HIPAA can be costly, with penalties ranging from $137 per violation up to $68,928 for a Tier 1 violation "lack of knowledge" to $68,928 to $2,067,813 per violation for a Tier 4 violation "willful neglect and not corrected after 30 days."[1160] In addition to financial penalties, data and security breaches lead to lost productivity, brand and reputational loss and reduced consumer goodwill.[1161]

Healthcare networks contain IoMT and medical devices at various levels of cybersecurity vulnerability risk. While medical devices approved after October 1, 2023, will be more secure, millions of older devices lack advanced security protections.

Legacy and older devices are the most vulnerable as they may not have the current firmware updates or be incorrectly configured. While modern IoMT devices may be more cybersecure, new vulnerabilities are regularly discovered. Finally, a healthcare delivery organization may have incorporated all the updates and current practices, but its third-party vendors and contractors may be negligent.

As new devices are added to the network, healthcare delivery organizations must understand what information is being collected, how it is used, shared, transmitted and stored. Complying with these regulations requires that healthcare delivery organizations establish infrastructure and capabilities that allow them to stay current with both regulations and firmware updates. They will also need to implement changes to operational systems and administrative processes and train staff, vendors and partners in best practices. Urban healthcare delivery organizations, with their larger pool of capabilities and resources are better prepared than smaller and rural community organizations to comply with these regulations.

19.3.2.2. Consumer IoT device privacy

The increasing popularity of consumer healthcare IoT apps and wearable devices, such as fitness trackers, has allowed users to monitor their health and physical activities. These wearable devices are becoming more sophisticated, with some monitoring sleep patterns, heart rates and rhythms. Data from these wearable devices may be used to inform healthcare providers, leading to better care outcomes.

A 2023 Morning Consult survey of 2,201 U.S. adults reported that over one-third (35%) are using wearable healthcare devices, an eight percent increase from the December 2018 survey.[1162] Along with this increase in wearers, nearly one-third (30%) of users indicated they were concerned about data privacy.

[1160] "What are the penalties for HIPAA violations?" The HIPAA Journal. Link

[1161] "Update: Privacy and security of protected health information," Deloitte Center for Health Solutions. Issue Brief. P. 6. Link

[1162] "Over a Third of Adults Use Health Apps, Wearables in 2023, Up From 2018," A. Vaidya, mHealth Intelligence, February 23, 2023. Link

© Strategy of Things, 2025. All rights reserved.

The Software Advice 2023 Consumer Wearables Survey of 876 U.S. patients who use personal wearable fitness devices reported that 91% of patients are interested in sharing data from their personal health tracking devices with doctors. The remaining 9% who are not interested in sharing cited a number of reasons. For example, two-thirds (63%) cited privacy reasons for keeping the data private and 41% cited concerns about security breaches.[1163]

These concerns are not unfounded. Researchers uncovered a fitness tracker data breach that exposed 61 million records of user data. The exposed data included the user's name, gender, age and geographic location.[1164]

In addition to health information, wearable devices collect other information that may be sensitive. For example, one well-known fitness app published a map that shows all the sports activity locations and routes of its users, including sensitive locations of military bases and spy outposts.[1165]

Privacy concerns, applicable to both IoMT devices and consumer health IoT devices, are apparent in several ways, including:

- **Data Ownership and Control.** When patients and consumers use wearable health monitors, questions arise about whether the data belongs to the patient or consumer, the device manufacturer or the healthcare provider.
- **Consent Mechanisms.** Healthcare IoT devices and systems collect large volumes of data, making it difficult for patients to control their information. Patients and consumers lack the information and the tools to manage what information and data they want to share.[1166]
- **Data Retention and Deletion.** Healthcare organizations and wearable device manufacturers must establish clear policies for data retention and deletion to ensure that patient data collected by IoT devices is not retained longer than necessary. Failure to manage data retention can increase the risk of unauthorized access and privacy breaches.
- **Third-Party Sharing.** Sharing patient data with third-party service providers, such as IoT device manufacturers or cloud service providers, raises privacy concerns. In addition, sharing increases the risk of data breaches, unauthorized access and misuse of patient and consumer information. The security and privacy practices of these third parties may not be at the same level as the healthcare organization's standards.[1167]

[1163] "Do Personal Health Trackers Belong in the Doctor's Office? Patients Say Yes." L. Morris, Software Advice, October 24, 2023. Link

[1164] "Report: Fitness Tracker Data Breach Exposed 61 Million Records and User Data Online," J. Fowler, Website Planet, 2021. Link

[1165] "Fitness tracking app Strava gives away location of secret U.S. army bases," A. Hern, The Guardian, January 28, 2018. Link

[1166] "Can You Trust IoT in Healthcare? Analyzing IoT Security Risks in Healthcare," S. Jones, Webmedy, July 28, 2023. Link

[1167] See note 1166

© Strategy of Things, 2025. All rights reserved.

While wearable IoT technologies help facilitate better consumer and patient health outcomes, they present opportunities for advancing the business interests of device makers. For example, recent advances have enabled measurement of a person's health and biological reaction to environmental stimuli, allowing more accurate inferences about a person's emotional condition. In turn, these data could be used for business applications, such as emotional marketing."[1168] Another concern is that the information may be combined with information from other sources to create outcomes that may not be beneficial to the consumer. For example, insurance companies may "use data from wearables to price insurance or to infer the user's suitability for credit or employment."[1169]

The HIPAA Act applies to medical equipment and devices used to diagnose, treat and care for patients in both clinical and non-clinical settings. Unlike medical devices used by healthcare providers, consumer wearable companies are not subject to HIPAA regulations.[1170] This regulation applies to "covered entities" such as health plans, healthcare clearinghouses and healthcare providers who transmit information electronically[1171] and their 3rd party business associates who perform activities that involve the use or disclosure of protected health information for a covered entity.[1172]

As the data collected from wearable devices are generated by the consumer and not from "covered entities" and their business associates,[1173] it is not covered by HIPAA.

While HIPAA does not apply to consumer wearable devices, health apps and connected devices that collect or use consumers' health information are subject to compliance with the Federal Trade Commission's Health Breach Notification Rule. In the event of a breach, they must notify consumers when their health data has been breached.[1174]

In light of these challenges, privacy and human rights advocates are calling for better data privacy protections as "current legal framework and ethical oversight are not sufficient."[1175] One advocate suggested that the "core difficulty with tech wearables, when it comes to privacy and human rights, is the amount and nature of the data that users surrender to their device "and that

---

[1168] "Wearables: Where do they fall within the regulatory landscape?" G. Tomimbang, International Association of Privacy Professionals. Link

[1169] See note 1168

[1170] See note 1168

[1171] "The HIPAA definition of covered entities explained," S. Alder, The HIPAA Journal, January 1, 2023. Link

[1172] "Business Associates", U.S. Department of Health and Human Services. Link

[1173] "Wearables: Where do they fall within the regulatory landscape?" G. Tomimbang, International Association of Privacy Professionals. Link

[1174] "FTC Warns Health Apps and Connected Device Companies to Comply With Health Breach Notification Rule," Press Release, Federal Trade Commission. September 15, 2021. Link

[1175] "Putting Our Bodies Online: The Privacy Risks of Tech Wearables," M. Lamensch, Centre for International Governance Innovation, August 11, 2021. Link

© Strategy of Things, 2025. All rights reserved.

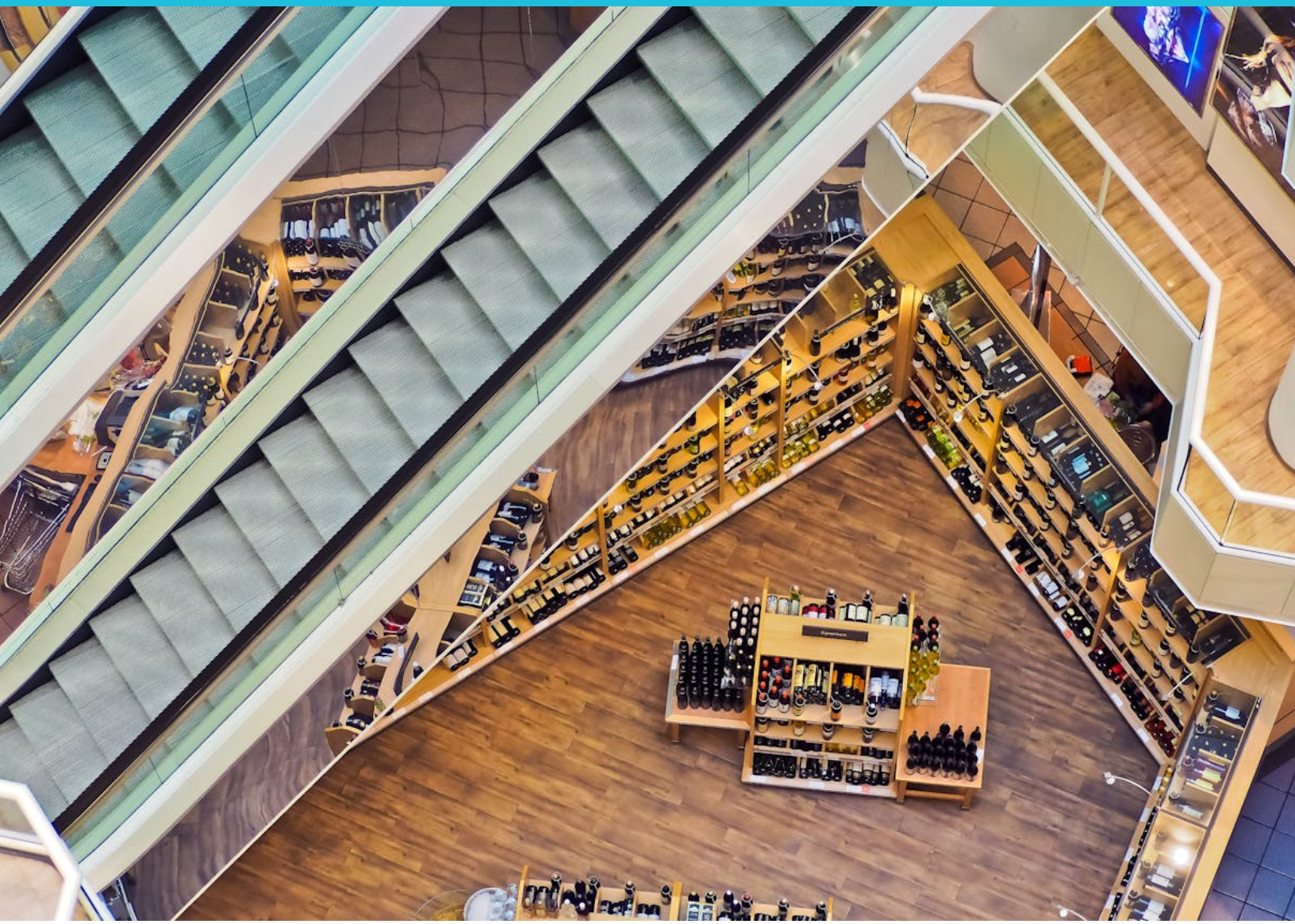
”the experience with Apple, Google, Facebook and others is that they are not competent at protecting privacy and hide behind opaque terms of services.”[1176]

> *It is increasingly obvious that more and better guardrails are urgently needed. Tech companies that sell fitness and health devices or apps are not subject to the same level of oversight and privacy laws as companies that sell medical devices — and they should be. Similarly, in a clinical context, our data is heavily protected, which is not the case for the health and behavioural data shared through a phone app or wearable device*[1177]

[1176] See note 1175

[1177] See note 1175

© Strategy of Things, 2025. All rights reserved.



Appendix: Retail

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

© Strategy of Things, 2025. All rights reserved.

20. Appendix: Retail

This section describes the research findings for IoT technology infrastructure in the U.S. retail industry. The topics discussed here cover:

- Industry overview
- Use of IoT in retail
- IoT challenges in retail

20.1. Industry overview

The retail industry in the United States is a significant sector of the economy, covering a range of businesses involved in the sale of goods and services directly to consumers. It plays an important role in driving consumer spending, employment and overall economic growth.

20.1.1. Key facts

Retail sales in the United States totaled $5.57 trillion in 2020, representing a growth of 3.1% over 2019 sales of $5.4 trillion.[1178] In Q4 of 2020, the retail industry contributed $1.26 trillion dollars[1179] in value to the American economy, representing 5.86% of the Gross Domestic Product (GDP). In Q4 of 2021, the retail industry's contribution to GDP grew to $1.434 trillion dollars,[1180] or 5.97% of the total GDP. When its indirect and induced contributions are factored in, the total impact of U.S. retail was $3.9 trillion or 18.7%[1181] of the overall U.S. GDP.

The largest subsectors within retail are food services and drinking places ($458.7 B, 28.9% of total retail GDP), motor vehicles and parts ($212.2 B, 13.4%), non-store retail ($158.6 B, 10%), food and beverage ($156.4 B, 9.86%) and general merchandise ($151 B, 9.52%).

Online sales have been rising since 2000, rising from 0.6% of all retail sales in Q4 2000 to a high of 16.4% in Q2 2020.[1182] The online sales subsector was the fourth fastest growing in terms of job growth, growing at 5.7% between 2010 and 2018.[1183]

The U.S. retail industry is the second largest employer of Americans after healthcare. U.S. retailers employed 32.1 million people in 2018 with 21.1 million (65.8%) of retail workers employed at firms with 50 or more people.[1184] The retail industry created an additional 19.8

[1178] Annual Retail Trade Survey: 2020. Link

[1179] Q4 2020 seasonally adjusted annual rate, Bureau of Economic Analysis. Link

[1180] Q4 2021 seasonally adjusted annual rate, ibid

[1181] Table 5, "The Economic Impact of the U.S. Retail Industry", PWC and National Retail Federation report, May 2020. Link

[1182] E-Commerce Retail Sales as a Percent of Total Sales, FRED economic research. Link

[1183] ibid, Page 16

[1184] Table E-4, "The Economic Impact of the U.S. Retail Industry", PWC and National Retail Federation report, May 2020. Link

© Strategy of Things, 2025. All rights reserved.

million jobs indirectly.[1185] Retailers created $1.04 trillion in total labor income, with $680.6 million (65.4%) coming from businesses employing 50 people or more.[1186] The three sectors employing the most Americans in retail in 2018 were food services and drinking places (12.8 million), food and beverage (3.265 million) and general merchandise (3.152 million).[1187]

There were 3,611,704 retail businesses in the United States in 2018.[1188] Of this, 3,557,920 or 98.5% were small businesses employing 50 people or less. 3,279,058 (90.8%) of the retail businesses employed fewer than 11 people.

20.1.2. Industry challenges

The U.S. retail trade faces several challenges that constrain the growth and advance of the industry. Five key challenges that are relevant to the Internet of Things in retail are:

- Inventory management
- Labor shortages
- Shrinkage
- Profitability
- Retailer resilience

Each of these is discussed below.

20.1.2.1. Inventory management

Inventory management is a foundational capability for successful retailing. The ability to understand and forecast demand and then place the right inventory at the right outlets and locations at the right time enables the fulfillment of shopper needs. More importantly, it allows retailers to convert inventory into cash for operations, purchase more inventory and free up storage and merchandising space for new higher demand items.

Despite its importance, inventory management continues to be a challenge for retailers. Inventory shortages lead to customer dissatisfaction and lost sales. Inventory overstocks consume valuable space in stores and warehouses for in-demand goods, tie capital that could be used to purchase in-demand inventory and require discounting to draw down stock levels and free up cash.

A 2019 survey of national and large regional retailers reported that the top inventory management challenges were item level inventory accuracy (55%), reducing out of stock inventory (45%) and reducing over stock inventory (39%). Other challenges included real time

[1185] ibid, Page 13

[1186] ibid, Table 7

[1187] ibid, Table 4

[1188] Table E-4, "The Economic Impact of the U.S. Retail Industry", PWC and National Retail Federation report, May 2020. Link

© Strategy of Things, 2025. All rights reserved.

inventory visibility (36%) and applying mark downs to move excess inventory (27%).[1189] A separate survey of over 200 senior retail decision-makers reported that 46% of respondents attribute inventory markdowns to overbuying and buying the wrong types of products.[1190] These challenges are exacerbated by changing customer demands, supply chain inefficiencies, shrinkage and outdated processes and systems.

In addition, unforeseen events such as the COVID-19 pandemic exposed supply chain vulnerabilities in many retailers. For example, many retailers have disparate fulfillment processes for e-commerce and physical store channels. Some retailers stored 30% of the total inventory in the warehouse for e-commerce orders, while the remaining 70% was distributed to physical stores. With physical stores closed, customers went online to place orders. While warehouse inventory stocks were quickly sold out, outdated processes, systems and lack of stock visibility kept retailers from tapping into the remaining inventory located in the closed stores, resulting in lost sales, inventory write-offs and dissatisfied customers.[1191] Omni-channel inventory management is a critical capability, yet less than half of the retailers (48%) have a "few advanced systems and processes" in place to support this.[1192]

Omni channel inventory management adds a new level of complexity to retailers as online orders can be picked up from stock in physical stores instead of warehouses and store visits can result in delivery orders fulfilled from warehouse stocks. This model is more dynamic than traditional inventory management methods and improper planning will result in depletion of safety stock, degradation in store presentation and out of stock situations in individual locations.[1193]

20.1.2.2. Labor shortages

Although the retail industry is the second largest private sector employer of Americans in the United States and supports nearly a quarter of the U.S. workforce,[1194] it faces several labor and workforce challenges. A survey of 50 executives in the retail industry, conducted by management consultancy Deloitte, found that 70% of respondents reported labor as the number one challenge in 2022.[1195]

For example, in December 2022, there was a net shortage of 976,000 positions.[1196] At the store level, 74% of respondents to the Deloitte survey specified that a shortage of customer-facing workers is one of their main challenges.[1197] The Deloitte survey also reported that nearly half the

---

[1189] "Sharpening Omnichannel Inventory Management to A Razor's edge," J. Skorupa, Retail Info Systems, April 16, 2019. Link

[1190] "Hidden Costs of Poor Inventory Management," J. Andrews, TotalRetail, April 5, 2019. Link

[1191] "How the Pandemic Exposed Major Cracks in Retailers' Inventory Management Practices," G. Drenik, Forbes, Feb 23, 2022. Link

[1192] See note 1189

[1193] Inventory Management Challenges: Omni-Channel Replenishment, NTS Retail. Link

[1194] "State of Retail", National Retail Federation. Link

[1195] "2022 retail industry outlook", R. Sides and L. Skelly, Deloitte, 2022. Link

[1196] Job Openings and Labor Turnover Survey, Bureau of Labor Statistics. Link

[1197] See note 1195

© Strategy of Things, 2025. All rights reserved.

respondents expect a shortage in IT and analytics positions and 56% expect shortages in hourly supply chain, distribution and logistics positions.[1198]

A 2023 Forrester Research study commissioned by technology platform provider WorkJam reported a similar finding, with 63% of retail companies operating with a deficit of customer-facing employees.[1199] As retail becomes more digital and e-commerce sales become an increasing part of retail sales with 14.7% of sales in 4Q-2022,[1200] a digital labor force to support these capabilities and operations is required.

The COVID-19 pandemic accelerated some long running labor trends. In the three years prior to the COVID-19 pandemic, the retail industry experienced a loss of 200,000 jobs due to online competition and from changes in consumer preferences and demand. During the pandemic, the retail industry lost almost 800,000 jobs during 2020 as many retailers engaged in contactless shopping, e-commerce and curbside pickups.[1201]

The pandemic also contributed to the "Great Resignation" across several industries. The "Great Resignation" is an economic trend in which workers voluntarily left their jobs in large numbers about a year after the start of the pandemic.[1202] There are several reasons for quitting, including low pay, lack of advancement opportunities, work environment, childcare needs and lack of flexibility.[1203] While these reasons were not unique to the retail trade the voluntary quit rate doubled from 2.2% in April 2020 to 4.4% in November 2021.[1204] At its peak, 714,000 workers, corresponding to a 4.7% rate, left their jobs in retail in August 2021.[1205]

One impact of the labor shortages is higher wages. According to data provided by Magnit, a workforce management platform provider, the average hourly pay rate for retail associates increased by 22%, from $15.70 in 2018 to $19.21 in 2022. While the average hourly pay rate for warehouse associates increased only 9% from $20.28 in 2018 to $22.06 in 2022, their pay was higher than those of their retail associate counterparts. In some states, Magnit estimates that there are 50% to 250% more warehouse workers than retail workers.[1206]

[1198] See note 1195

[1199] "New Survey Finds 63% of Retailers Are Short Frontline Staff, but Only 8% Plan to Invest in Improving the Frontline Employee Experience This Year", Business Wire, January 16, 2023. Link

[1200] "Quarterly Retail E-Commerce Sales, 4th Quarter 2022", U.S. Census Bureau News, U.S Department of Commerce, February 17, 2023. Link

[1201] "Retail Trade Employment: Before, During and After the Pandemic," D. Dorfman, Beyond the Numbers: Employment & Unemployment, vol. 11, no. 4 , U.S. Bureau of Labor Statistics, April 2022. Link

[1202] "Great Resignation", Wikipedia. Link

[1203] "Majority of Workers Who Quit A Job In 2021 Cite Low Pay, No Opportunities for Advancement, Feeling Disrespected," K. Parker and J. Menasce-Horowitz, Pew Research Center, March 9, 2022. Link

[1204] "The "Great Resignation" in perspective," Maury Gittleman, Monthly Labor Review, U.S. Bureau of Labor Statistics, July 2022. Link

[1205] "Job Openings and Labor Turnover Survey", Bureau of Labor Statistics. Link

[1206] "Hiring Retail Workers This Holiday Season: 2 Things You Should Know", R. Gagnon, Magnit blog, November 7, 2022. Link

© Strategy of Things, 2025. All rights reserved.

20.1.2.3. Shrinkage

According to the 2022 Retail Security Survey, conducted by the National Retail Federation in partnership with the Loss Prevention Research Council and Appriss Retail, the average shrinkage rate was 1.4% of retail sales in 2021. This translates to $94.5 billion in losses for American retailers and represents a 4.1% increase from the 2020 shrinkage rate.[1207]

One industry consultant estimated that "for every $330 worth of products stolen, a retailer has to sell an incremental $300,000 worth of goods to break even."[1208] Target, a major national retailer, attributed inventory shrinkage as a factor in its 3rd quarter 2022 operating income margin rate decline of 50% over the same period from the previous year.[1209] This corresponded to a reduction of $400 million year to date, after 3 quarters, compared to the previous year.[1210]

The impact of shrinkage and theft extends beyond retailers. A study, conducted by the Retail Industry Leaders Association and Buy Safe America Coalition, provided additional insight on the broader economic impact of retail theft. Examining data from the largest retailers, the study reported $68.9 billion of product stolen by organized and professional theft rings in 2019. This corresponds to $125.7 billion in lost economic activity and 658,375 fewer jobs and almost $39.3 billion in lost wages and benefits to workers. In addition, this theft costs federal and state governments nearly $15 billion in lost tax revenues.[1211]

Beyond the economics of shrinkage is the increased potential for violence against retail employees. A study found that 86% of respondents reported verbal threats of bodily harm, 76% reported physical assaults, 76% reported threatening use of a weapon and 40% reported the use of a weapon to cause harm.[1212]

External theft, including organized retail theft, represented the largest contributor at 37% of shrinkage. Internal theft and process/control failures represented the second and third largest contributors at 28.5% and 25.7% respectively.[1213] These three categories accounted for 92% of the shrinkage.

Not all shrinkage occurred in the retail outlets. Survey respondents reported shrinkage also occurred in the supply chain. For example, nearly half, or 47.4%, of losses occurred while shipments were "en route from distribution centers to stores." Cargo shrinkage at stores was reported by 42.1% of respondents, while losses "en route from manufacturers to distribution

---

[1207] "2022 Retail Security Survey", National Retail Federation and Loss Prevention Research Council, Page.9. Link

[1208] "Shoplifting is Surging Across America With Dangerous and Costly Consequences," P. Kavilanz, CNN Business, January 7, 2022. Link

[1209] "Target Corporation Reports Third Quarter Earnings," Target Press Release, November 16, 2022. Link

[1210] "Target: 'Organized retail crime' has driven $400 million in extra profit loss this year," B. Sozzi, Yahoo News, November 16, 2022. Link

[1211] "The Impact of Organized Crime and Theft In the United States," John Dunham and Associates, Retail Leaders Industry Association, November 18, 2021. Link

[1212] Ibid.

[1213] See note 1207

© Strategy of Things, 2025. All rights reserved.

centers" was reported by 35.1%. Shrinkage losses also occurred at distribution centers (31.6%), third-party centers (31.6%) and "en route between stores" (29.8%).[1214]

20.1.2.4. Profitability

Profitability is a constant challenge in the retail industry. In Q4 2022, the average annual Trailing Twelve Month (TTM) gross margins and net margins for retailers were 24.71% and 2.53%, respectively.[1215]

Within the retail industry, profitability margins vary by segment. In the same quarter, the quarterly gross and net margins for department and discount retailers were 33.07% and 3.7% respectively.[1216] In contrast, specialty retailers reported 40.79% and 6.56% for gross and net margins. Pharmacy services and retail drugstores reported low margins of 4.45% and 0.84% for gross and net margins.

A 2018 analysis, conducted by the American Enterprise Institute, provided a more relatable perspective on profitability. Using data sourced from the New York University (NYU) Stern database,[1217] General Retail businesses reported an average net margin of 2.3%.[1218] The study determined that the corresponding date of first profit for those businesses would be December 23. This is the date when sales exceed the company's annual operating expenses of labor, leases, cost of goods, utilities, taxes, marketing and other costs. The retailer then has 8.4 days to generate profit before the end of the year.[1219]

Retailer profitability is impacted by cost of goods sold, unsold inventory, labor costs, shrinkage, taxes and other operating expenses. There are several contributing factors to the retail industry's low profits. Some retailers, such as WalMart and Target, employ a low margin, high volume business model. For example, WalMart reported a net margin of 1.91% on $611.29 billion of TTM revenue and $11.68 billion of TTM net income on January 31, 2023.[1220] The internet and e-commerce have made it easier to compare prices exacerbating the low margins. Finally, many retail purchases are considered discretionary, creating a high price elasticity of demand limiting the retailer's ability to raise prices.[1221]

While retail industry profitability has always been subjected to these factors, the COVID-19 pandemic exacerbated many of them. For example, sales from e-commerce channels and retailers were growing before the pandemic and further accelerated during the pandemic where physical transactions and visits were discouraged. E-commerce sales grew from 1.3% of total retail sales

---

[1214] See note 1207

[1215] "Retail Sector Profitability - Profitability Information & Trends," CSI Market. Link

[1216] "Profitability by Industry within Retail Sector", CSI Market. Link

[1217] "Margins by Sector (US)", NYU Stern database. Link

[1218] "The Typical U.S. Firm Doesn't Earn A Profit Until the Second Week of December and for Retailers It's at the End of the Month," M. Perry, AEI, November 18, 2018. Link

[1219] Ibid.

[1220] "WalMart Net Profit Margin 2010-2023", Macrotrends. Link

[1221] "What is A Good Profit Margin for Retailers," S. Ross, Investopedia, September 30, 2022. Link

© Strategy of Things, 2025. All rights reserved.

in Q1-2002 to 11.9% by Q1-2020. This increased to 16.4% in Q2-2020, before dropping back down to 14.7% in Q4-2022.[1222]

An analysis of 250 retailers in six European countries found that pre-tax margins were expected to drop from 6.4% in 2016 to 3.7% in 2025, assuming e-commerce penetration at pre-COVID levels. These margins, however, are forecasted to fall 3.2%, by 2025, due to the pandemic accelerated e-commerce takeup.[1223]

While the adverse effects of the pandemic are beginning to ebb, some of the changes brought about by the pandemic are likely to stay.

> *... the margins are already brutally thin. And the selling side, the consumer side, is incurring all kinds of new costs that even a few short years ago they didn't have to deal with such as having to do with the fulfillment of orders that were generated online and picked up in the store... All kinds of new costs are eroding what little margin they have. So retail is in a kind of a profitability crisis mode.*
>
> *Brian Kilcourse, Co-founder, RSR Research*[1224]

20.1.2.5. Retailer resilience

Retailers face three types of disruptive forces. Competition and changing customer preferences, cyclical forces such as inflation, recessions and rare and unpredictable "black swan" events, such as the COVID-19 pandemic of 2020 and the Global Financial Crisis of 2008.

While disruptive events and forces are part of any business, retailers are especially vulnerable. Low profit margins, averaging 2.53% in Q4 2022, along with significant debt mean that retailers have little financial cushion to weather disruptive forces or make new investments.

In times of uncertainty and recession, retailers that sell mostly discretionary goods, cater to middle and lower-income consumers or have weak balance sheets will be most vulnerable to store closings and bankruptcies.[1225] For example, during the Great Recession from late 2007 to 2009,[1226] annual retail sales growth was 0.5% and -3.6% for 2008 and 2009, respectively.[1227] During that time, there were 328, 441 and 407 retailer bankruptcy filings reported in 2007, 2008

[1222] "E-commerce Retail Sales ss A Percent of Total Sales," FRED Economic Data, Federal Reserve Bank of St. Louis, February 17, 2023 (updated). Link

[1223] "An Analysis of 250 Retailers Shows What Online Shopping Does to Profit Margins," M. Bain, Quartz, July 1, 2021. Link

[1224] Research interview, RSR Research, April 20, 2023

[1225] "These Retail Chains May Not Survive A Recession," N. Meyersohn, CNN, October 13, 2022. Link

[1226] "Great Recession," Wikipedia. Link

[1227] "10 Years After the Financial Crisis, Americans Are Still Looking for A Deal," L. Thomas and L. Hirsch, CNBC, September 18, 2018. Link

© Strategy of Things, 2025. All rights reserved.

and 2009, respectively.[1228] There were approximately 15,000 major chain store closings during this three year period.[1229]

Besides financial challenges, operational issues reduce retailer resilience. For example, e-commerce is both a positive and negative disrupter for retailers. While e-commerce expands a retailer's market reach it also provides challenges. A report by micro-fulfillment center service provider, Fabric, found that 81% of consumers will purchase an item if it can be delivered that same day. That same report found that retailers lack the operational capacity to keep up with and fulfill online orders. As a result, retailers lost an average of 22% of sales in 2021 and expect to lose nearly 30% in 2022.[1230]

Exacerbating this is that 33% of those consumers are not willing to pay a premium for same day delivery, while 37% will only pay a premium between $1 and $4.[1231] Residential courier delivery rates have increased by 71% from 2016 to 2021,[1232] further pressuring retailers who are unable to pass the higher costs to customers. According to a 2022 survey of global retail leaders, almost 40% of respondents agreed that their e-commerce operations are not meeting profit targets, while 27% said e-commerce is hurting overall profitability and 25% said it is not profitable at all.[1233]

A 2020 survey by Bain & Company and Microsoft of 70 retailers showed investments in three key areas are required to improve responsiveness and speed. These were omnichannel supply management, predictive planning and flexible operations.[1234] These findings were echoed by management consultancy Deloitte in 2023, who analyzed top performing retailers for common behaviors. They found that retail leaders "prioritize investments in marketing and merchandising, omnichannel capabilities, digital transformation and supply chain."[1235] According to management consultancy McKinsey and Company 2022 report, most retailers have embarked on digital transformation initiatives but are in the middle of their journey for both technology architecture and operating model transformations.[1236]

20.2. IoT in the retail industry

[1228] "As Pandemic Stretches On, Retail Bankruptcies Approach Highest Number In A Decade," M. Repko and L. Thomas, CNBC, August 3, 2020. Link

[1229] "A Tsunami of Store Closings is About to Hit the U.S. — and It's Expected to Eclipse the Retail Carnage of 2017," H. Peterson, January 1, 2018. Link

[1230] "The 3 Biggest Last-Mile Challenges the Retail Industry is Facing Today," Fabric 2022 retail report. Link

[1231] ibid.

[1232] ibid.

[1233] "Retailers Grapple With E-Commerce's Drag on Profits", D. Howland, Retail Dive, June 14, 2022. Link

[1234] "Retailers plan to invest in supply chain resilience," M. Vu and K. Goldman, Bain & Company, November 20, 2020. Link

[1235] "2023 Retail Industry Outlook," N. Handrinos and L. Skelly, Deloitte, 2023. Link

[1236] "The Tech Transformation Imperative In Retail," R. Bick et al, McKinsey & Company, May 20, 2022. Link

© Strategy of Things, 2025. All rights reserved.

The retail industry is in a long running technology driven evolution. The Internet and e-commerce, also known as Retail 3.0,[1237] delivered innovations that have changed how customers find and buy products and interact with retailers and brands.

A survey of 1,501 shoppers, conducted by the Consumer Technology Association in 2020, reported that 57% of respondents indicated that online shopping offers more inventory and a wider choice of products. Furthermore, 55% indicated that online shopping allows them to discover more products compared to in-store, while 53% said that online shopping was less time consuming than in-store shopping.[1238] Similarly, it provided retailers with new channels to reach, market, sell and build relationships with customers.

Industry leaders are evolving to omni-channel retail, also known as Retail 4.0,[1239] where the disparate physical and digital channels integrate to create one seamless experience and interaction for customers. One example of this is a customer ordering online and picking up at the store or visiting the store to "touch and feel" the goods and place the order and then have it delivered to their home or workplace.

The evolution to Retail 4.0 was accelerated by the COVID-19 pandemic. A 2022 Consumer Technology Association survey of 1,621 shoppers reported that 40% indicated that having both a physical "brick and mortar" store and an online store is important or very important.[1240]

IoT is expected to make a significant impact on the retail industry and contribute to its ongoing transformation. IoT sensors collect data, some of which have not been previously collected and analyzed, to create actionable insights and capabilities that mitigate some of the industry challenges.

For example:

- Radio Frequency Identification (RFID) and asset tracking devices provide retailers with real time location information of their stock to facilitate omni-channel inventory management.[1241] This helps retailers reduce shrinkage in stores and warehouses and become more agile to demand changes by optimizing the distribution of inventory.
- Bluetooth beacons installed at various locations within a store provide retailers with insights into shopper movement patterns within a store leading to increased sales through improved store layouts and more effective merchandise placement.[1242] In addition, beacons can detect and send personalized marketing promotions directly to a shopper's mobile phone to increase in-store sales.[1243]

[1237] "Retail 4.0: the Future of Retail Grocery In A Digital World," P. Desai et al, McKinsey & Company. Link

[1238] "COVID-19 Impact: Retail Innovations," Consumer Technology Association Research Report, October 2020.

[1239] See note 1237

[1240] "Retail innovations: 2022," Consumer Technology Association Research Report, August 2022.

[1241] "Why Retail Asset Tracking is Key to Better Stock Control," Comparesoft, December 2022. Link

[1242] "IoT in Retail," K. Kimachia, Enterprise Networking Planet, December 5, 2022. Link

[1243] "7 Innovative Ways Retailers Are Using Beacon Technology," C. Forsey, Hubspot, October 11, 2018. Link

© Strategy of Things, 2025. All rights reserved.

- Smart shelves detect empty shelves and prompt employees to restock thereby minimizing lost sales.[1244] Sensors embedded in high value products, such as tools, are activated at checkout, to discourage theft and protect retailer profitability.[1245]
- Self-checkout kiosks partially alleviate the impact of retail labor shortages by allowing select customers to pay on their own, freeing up the existing cashiers to process those customers with many or complex items to complete the purchase.

The COVID-19 pandemic was a powerful change agent. A 2022 industry survey conducted by retail industry analyst firm, RSR Research, of 104 large American retailers with sales of $500 million and above reported the top overall business challenges driving interest in IoT included competitive differentiation (43%), maintaining margins (41%), operations cost reduction (40%) and operations speed and agility (34%).[1246]

The use cases that retailers deemed as "very important" centered around inventory accuracy and stock management (82%), fraud and loss prevention (80%), fulfillment center process automation (65%), supply chain process automation (63%), loyalty and personalization (62%) and brand protection and anti-counterfeiting (62%).[1247]

> *The supply chain is logically where you might start with some of these things, because that's the inflow of merchandise, which is the huge expense to retailers. It's probably the most highly engineered set of business processes that retailers have and profitability is built in the supply chain.*
>
> *Brian Kilcourse, Co-founder, RSR Research*[1248]

In contrast, prior to the pandemic, retailer interest in IoT focused on customer facing activities. The IoT use cases with "a lot of value" are those that supported tracking of customer flow nearby the store (89%), improving wait time to service (83%), dwell time monitoring (80%), in-store customer flow (77%) and inventory management (74%).[1249] The top business challenges driving IoT interest included operations speed and agility (41%), customer interaction outside of store (37%), technological capability disparity between retailer and consumers (32%) and maintaining margins (32%).[1250]

[1244] "Smart Shelves: What Retailers Should Know About the Emerging Trend," E. Smith, BizTech, January 6, 2022. Link

[1245] "Lowe's Employs RFID, Blockchain to Combat Retail Theft," N. Silberstein, Retail Touchpoints, December 16, 2022. Link

[1246] "A Deep Dive into Retailers' Views About Rfid and the Internet of Things", B, Kilcourse and S. Rowen, Retail Systems Research Benchmark Report, April 2022. Link

[1247] Ibid.

[1248] See note 1224

[1249] "The Internet of Things: Finally Finding A Home In Retail?", P. Rosenblum and S. Rowen, Retail Systems Research Benchmark Report, October 2019. Link

[1250] ibid.

© Strategy of Things, 2025. All rights reserved.

To better understand what this means, complementary data from a 2019 survey conducted by retail analyst firm, RSR Research was used. Their research data showed that[1251]:

- 68% "strongly agree" that IoT will drastically change the way companies do business in the next 3 years.
- 52% "strongly agree" that IoT will have a dramatic impact on consumer products in the next 3 years.
- 50% "strongly agree" that "My company has no idea how IoT will impact our own operations in the next 3 years."

This suggests that there is still a lack of understanding or awareness of the value and capabilities provided by IoT. Analysts from RSR Research attributed this gap to a "fundamental disconnect between how the retail industry sees the opportunities versus how the technology world sees them."[1252] This is further supported by survey data showing the top organization inhibitors that stand in the way of taking advantage of IoT. These include[1253]:

- 46% of retail winners, (those with annual sales growth of 4.5% or higher "have not identified a business case to support specific use-cases for the IoT."
- 44% of retail winners reported "Business leadership doesn't understand the benefits of IoT."

20.2.1. IoT use cases

The retail use cases are organized into four categories as shown below in Figure 20-1. Some use cases, such as asset tracking, may appear across multiple categories. The list of IoT use cases represent a range of applications across the various retailing activities. The retail IoT use case categories are:

- **Distribution and logistics.** The IoT applications in retail distribution and logistics include those that support operational processes that manage how inventory is transported and managed from manufacturers and producers to distribution centers, warehouses and stores.
- **Point of Sales/Store Operations.** These IoT applications support activities involved in the management and operation of the retail store. These activities may include stock planning, merchandising, stocking, theft prevention and processing transactions.
- **Consumer experience.** The IoT applications enhance the consumer experience and interactions while shopping, from finding merchandise, obtaining information to interacting with store personnel.
- **Post sale.** The IoT applications enable the retailer to provide support to the customer after the goods have been sold. This may range from after sales and product support to

[1251] ibid. Figure 1.

[1252] ibid. Page 1.

[1253] ibid. Figure 11.

© Strategy of Things, 2025. All rights reserved.

other interactions with the customer.

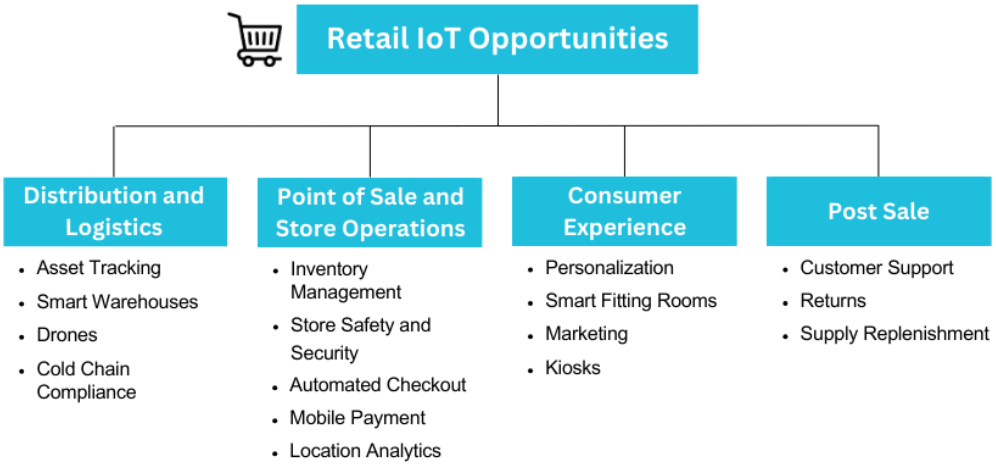


Figure 20-1: Retail: Use Case Categories and Selected Use Cases

20.2.1.1. Use case and industry challenges fit

The retail industry faces several challenges, some of which are described in Section 20.1.2. Figure 20-2 below shows the fit between the proposed use case subcategories and the documented industry challenges.

© Strategy of Things, 2025. All rights reserved.

Challenge	Role of IoT	Examples
Labor shortage	Mitigate labor shortages by automating routine tasks such as inventory tracking and checkout processes.	• Drones (in warehouses) • Store safety and security • Automated checkout • Smart fitting rooms and mirrors • Kiosks
Inventory management	Provide real-time inventory tracking, reducing overstock and out-of-stock situations	• Asset tracking • Smart warehouses • Drones in warehouses • Cold chain compliance • Inventory management • Store safety and security • Returns tracking and management • Supply replenishment
Shrinkage	Reduce shrinkage by providing real-time tracking of goods and alerting staff to potential thefts. Smart shelves and RFID tags can help identify when items go missing.	• Asset tracking • Inventory management • Store safety and security

© Strategy of Things, 2025. All rights reserved.

Challenge	Role of IoT	Examples
Profitability	Improve inventory management, reducing shrinkage and automating routine tasks. Additionally, IoT can provide customer data that can be used to improve marketing and sales strategies.	• Asset tracking • Inventory management • Automated checkout • Mobile payment • Location analytics • Personalization • Smart fitting rooms and mirrors • Marketing • Kiosks • Customer support • Supply replenishment
Retailer resilience	Enhance resilience by providing real-time data that can be used to quickly respond to changing market conditions.	• Asset tracking • Inventory management

Figure 20-2: Retail: Use Case Alignment with Industry Challenges

20.2.1.2. IoT use case details

Figure 20-3 below provides details on each of the use case subcategories as shown in Figure 20-1.

Category	Use case	Definition
Distribution and logistics	Asset tracking	Supply chain tracking of inventory shipments from transit to storage locations such as warehouses and distribution centers.

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Definition
	Smart warehouses	A variety of applications, including real time inventory management, shelf and bin sensors and warehouse robotics
	Drones	Drones for automated management and counting inventory stored in warehouses.
	Cold chain compliance	Monitor and verify compliance of perishable goods during transit and storage.
Point of Sales/Store Operations	Inventory management	Real time tracking of stock levels in stores and shelves using RFID and other sensors.
	Store safety and security	Cameras and sensors used for theft prevention, foot traffic monitoring, room occupancy, checkout queues and shopping cart tracking.
	Automated checkout	Kiosks or stations that allow for cashier-less or self-checkouts.
	Mobile payment	Point of sales systems using Near Field Communications (NFC) that allow for payment from smart watches, phones, tablets and other mobile devices.
	Location analytics	Tracking of shopper traffic patterns within a store to optimize store design, stock placement and marketing messages.
Customer Experience	Personalization	Bluetooth or Ultra-Wide Band (UWB) beacons detect customer devices to send personalized messages or display content on digital signage.
	Smart fitting rooms/mirrors	Fitting rooms/mirrors equipped with RFID readers that sense customer items, provide information, virtual fittings, etc.

© Strategy of Things, 2025. All rights reserved.

Category	Use case	Definition
	Marketing	IoT applications that provide couponing, personalized marketing content and other information to customers in stores or nearby.
	Kiosks	Computer stations that allow customers to interact with them to obtain information such as price checks, item location, product information and wayfinding
Post Sales	Customer support	Various IoT applications that monitor product usage and condition, solicit customer input or interact with company support staff. For example, an IoT help button.
	Returns	Tracking of stock in transit that is returned by the customer throughout the reverse logistics process.
	Supply replenishment	Sensors that detect when supply is low and add to shopping list or automatically place orders on behalf of customers. For example, eggs in a refrigerator, printer toner cartridges

Figure 20-3: Retail: Use Case Details

© Strategy of Things, 2025. All rights reserved.

20.2.2. Market views of IoT in retail

To understand market views on IoT and to inform on our gaps discovery and analysis, our research team conducted a survey of 450 people, from adopters to solution providers, across the nine industries studied. Our survey asked respondents about their opinion on the importance of IoT for the retail industry over the next 5 to 10 years. Figure 20-4 below shows respondents expected IoT to have a relative medium impact (68%), as compared to other industries.

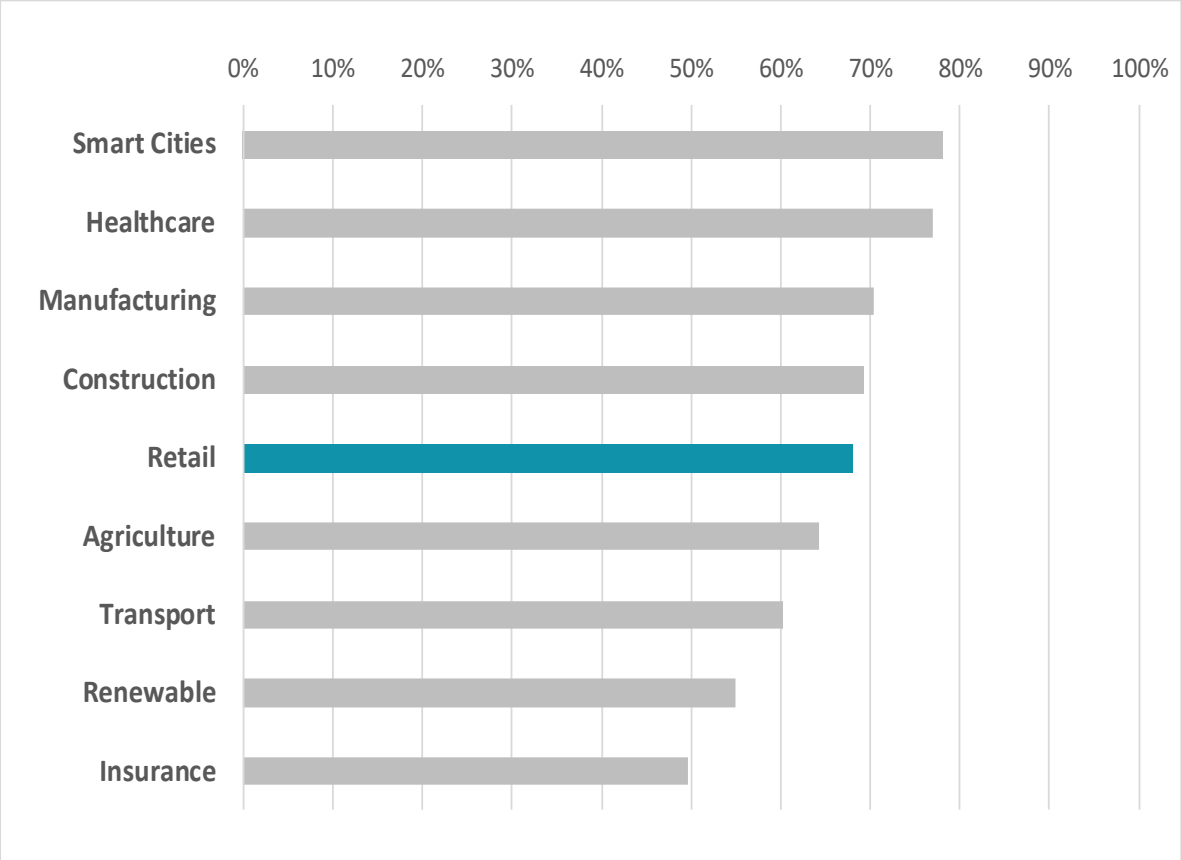


Figure 20-4: Retail: Importance of IoT

In support of the use case analysis, survey respondents were asked to rate the impact of these use case categories on the retail industry.[1254] Figure 20-5 below shows the percentage of responses in each impact category for each use case category. Overall, shows a bias to a moderate to high impact of the use case categories in retail.

[1254] In your view, what will be the impact of these use cases in retail over the next 5-10 years?

© Strategy of Things, 2025. All rights reserved.

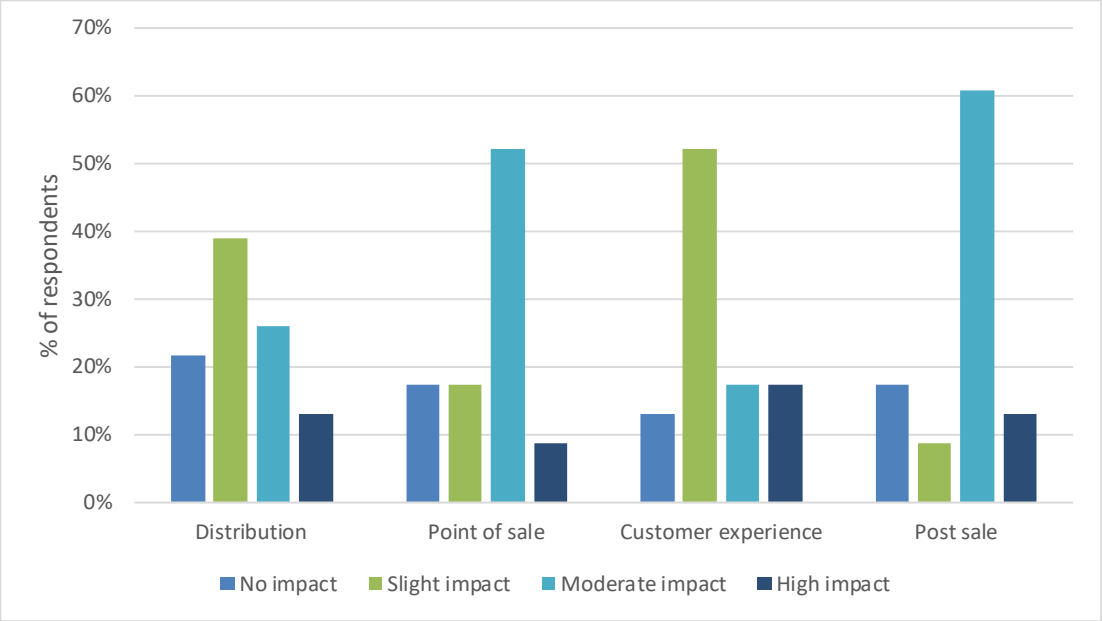


Figure 20-5: Retail: Use Case Category Impact

In addition, respondents were asked about their confidence in suppliers delivering the services required to operationalize these use case categories.[1255] Figure 20-6 below shows the percentage of responses in each confidence category for each use case category. Overall, their responses indicate modest confidence in the ability of suppliers to deliver the necessary services.

[1255] How confident are you that suppliers will deliver the services that retail organizations need from these technologies over the next 5-10 years?

© Strategy of Things, 2025. All rights reserved.

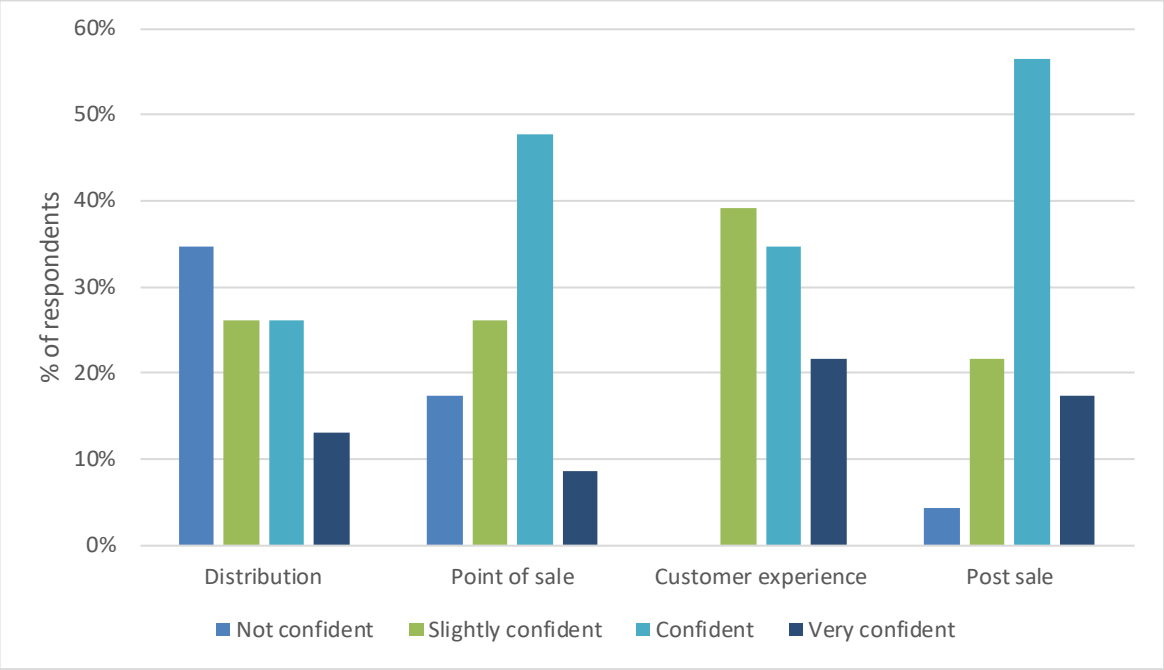


Figure 20-6: Retail: Confidence in Suppliers Delivering

20.3. IoT gaps and findings in retail

A combination of interviews, secondary research and surveys were conducted to identify and understand the opportunities and challenges to the development and adoption of IoT. Each research method approached the challenges from a different perspective.

- The survey targeted a large audience but asked specific questions that supported the economic analysis.
- The interviews targeted a small number of people who provided deeper insight and context to supplement the initial information collected.
- The desk research, consisting of a review of online news articles, published research reports, vendor and government white papers, blogs, webinars, videos and other content, provided a broad overview of the application of IoT in the industry.

In the survey, respondents were asked to choose the most important technology areas to operationalize IoT in their industry. Figure 20-7 below shows respondent's selections of the top 10 IoT technologies and the percentage of respondents who chose that technology.[1256] The survey results are not seen as a technology gaps list, but rather an indication of what is important to the respondents. This information partially informs the gap selection process.

[1256] Respondents were asked to choose up to 5 out of the 25 technologies listed.

© Strategy of Things, 2025. All rights reserved.

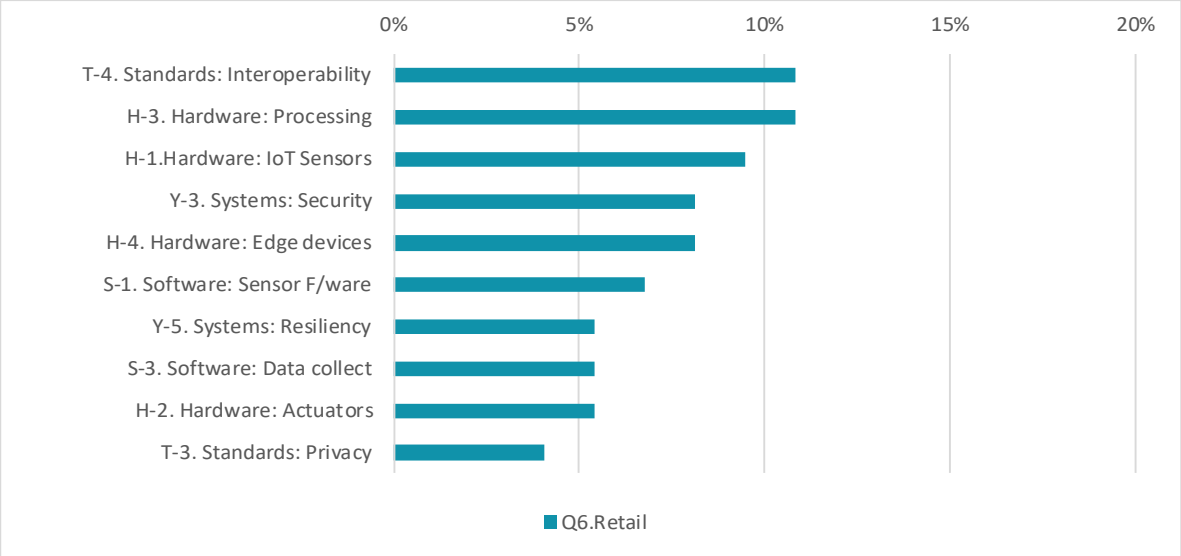


Figure 20-7: Retail: Top 10 Most Important Single Technologies

20.3.1. Top technology challenges

Using this approach three challenges were selected for further consideration. These are:

- Low-cost sensors
- Privacy enhancing technologies
- Artificial intelligence

20.3.1.1. Challenge # 1: Low-cost sensors

Low-cost sensors and devices are key enablers to IoT adoption in the retail industry. As discussed in Section 20.1.2.4, retailers operate with low profitability margins. These low margins hinder the ability of retailers to invest in IoT and other initiatives.

> *One of the biggest challenges that retailers have in adopting IoT is that their free cash flow to invest in these things is very, very limited.*
>
> *Brian Kilcourse, Co-founder, RSR Research*[1257]

RFID is the most common IoT technology in the retail industry. Its applications include inventory tracking on individual items, theft prevention and product marketing. According to a 2021 survey of 120 retail executives worldwide conducted by management consultancy

[1257] See note 1224

© Strategy of Things, 2025. All rights reserved.

Accenture, 93% of North America respondents are adopting RFID.[1258] Research analyst firm, IDTechEx, estimated that there are 10 billion RFID tags used for apparel tagging in retail.[1259]

While apparel tagging is one of the largest by volume applications of RFID, IDTechEx estimates that it has only penetrated 10% of the total addressable market for apparel goods.[1260] One of the reasons is the expense of RFID systems.[1261]

While passive RFID sensors may cost ten cents, the accompanying readers may cost anywhere from $3,000 for a single handheld reader and up to $20,000 for a fixed position passive reader.[1262] Depending on the application, the size and type of the store, retailers may need multiple readers which lead to an expensive system. With the low profitability margins and cash tied up in inventory, retailers have limited ability to purchase these systems.

Despite its popularity, RFID is only well suited for a small number of applications. Other IoT technologies, such as beacons, condition sensors and cameras and robotics support use cases not possible with RFID. For example, an appliance retailer could offer a remote monitoring service on its products by installing an IoT device with multiple sensors that alert the owner when the appliance needs to be serviced. These devices, however, are significantly more expensive than RFIDs.

In the manufacturing section of this report, it was noted that while the cost of sensors has been dropping steadily from $1.30 in 2004 to $0.38 in 2020,[1263] the cost of the semiconductors in the IoT devices in 2017 was $85.[1264] For retailers to adopt and launch this service at scale with these technologies, the upfront cost of the IoT device must come down as there is limited ability to pass the cost on to the customer.

> *You have a typical retailer P&L and the thing that jumps out is that the operating income line for a retailer might be a nickel on every dollar they put in the register. The operating income from a tech company is going to be 20 to 25 cents. The difference is that the 20 cents difference is all put into R&D and that is one of the things you'll never see in any retailer P&L So that makes them risk averse and look for cashflow positive analyses in the 12 to 18 month timeframe*

[1258] "A New Era for RFID in Retail," J Sain, Accenture, 2021. Link

[1259] "RFID Forecasts, Players and Opportunities 2019-2029," R. Das, IDTechEx. Link

[1260] See note 1259

[1261] "After Years of Hype, RFID is Still Struggling to Catch on in Retail," A. Hensel, Modern Retail, January 14, 2020. Link

[1262] "Simple Cost Analysis for RFID Options – Choice Must Fit the Organization's Needs and Budget," T. Watson, April 28, 2015, IAITAM.org website. Link

[1263] See note 434

[1264] See note 435

© Strategy of Things, 2025. All rights reserved.

Brian Kilcourse, Co-founder, RSR Research[1265]

Despite the significant value provided by IoT, the initial technology cost remains an issue. Further research and development on significantly lower cost IoT sensors and devices is needed.

One promising area is non-silicon thin film sensors that offer the potential for high volume, low cost IoT applications. This technology is currently the subject of interdisciplinary research at Purdue University through its Scalable Manufacturing of Aware and Responsive Thin Films (SMART) consortium.[1266]

20.3.1.2. Challenge # 2: Privacy enhancing technologies

Privacy issues slow the use of IoT technologies in retail and other consumer facing environments. IoT solutions that retailers use must balance the need for collecting and using data with the customers' need for privacy.

The use of IoT technologies and the data they collect enable retailers to understand their customers better and offer a variety of personalized services and experiences not previously possible. For example, facial recognition systems provide retailers with a literal view of the customer along with foot traffic types, average shopping times, peak traffic hours and demographics as well as moods and behavior. Other applications enabled by facial recognition include more effective VIP and loyalty programs, security and theft prevention and customer authentication for payment systems.[1267]

A 2021 survey of 3,000 businesses and consumers, conducted by customer data platform maker Twilio Segment, reported that 44% of consumers will take their business elsewhere if brands fail to offer a personalized experience. Furthermore, 60% of consumers are likely to become repeat buyers after a personalized experience and more than a third will return to shop with a brand following a good experience, even if there are cheaper or more convenient options available elsewhere.[1268]

At the same time, consumers, businesses and legislators are becoming increasingly sensitive to privacy. A 2019 survey of 4,272 American adults conducted by the Pew Research Center reported that 81% of respondents stated that "potential risks of companies collecting data about them outweighed the benefits", 79% stated that they are "very/somewhat concerned about how companies use the data collected."[1269]

These concerns are justified. In one widely reported incident in 2022, a company used its facial recognition technology to identify and deny a ticket holder entry to an entertainment event. The

---

[1265] See note 1224

[1266] Scalable Manufacturing of Aware and Responsive Thin Films, Purdue University. Link

[1267] "How Facial Recognition Will Change Smart Retail," FaceMe Market Insights, February 15, 2023. Link

[1268] "Why Brands Must Embrace Personalization Before It's Too Late," K. Wong, Ad Age, June 9, 2021. Link

[1269] "Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information," B. Auxier et al., Pew Research Center, November 15, 2019. Link

© Strategy of Things, 2025. All rights reserved.

ticket holder was barred because she worked for a law firm that engaged in litigation with the company, even though she was not involved in the specific case.[1270]

In another instance, a class action lawsuit was filed against a retailer because customers at its New York city stores were not notified that they were being monitored by biometric sensors as required by law.[1271] The enactment of the California Consumer Privacy Act of 2018[1272] and the rollout of App Tracking Transparency[1273] in Apple iOS 14.5 in 2021 are examples of some of the responses to privacy concerns.

Privacy Enhancing Technologies (PETs) are a "broad set of technologies that protect privacy by removing personal information, by minimizing or reducing personal data or by preventing undesirable processing of data while maintaining the functionality of a system."[1274] Some examples of these technologies include:[1275]

Cryptographic algorithms

- Homomorphic encryption which enables computation on encrypted data.
- Secure multi-party computation which enables computation from multiple encrypted data sources.
- Differential privacy which adds statistical noise to data.
- Zero knowledge proofs which allow information to be validated without revealing the underlying data proofs.

Data masking

- Obfuscation which replaces sensitive information with distracting or misleading data.
- Pseudonymization where identifier fields are replaced with fictitious data and data collection minimization.
- Communication anonymizers which replaces online identity with one-time untraceable identity.

Artificial intelligence and machine learning algorithms

[1270] "Madison Square Garden Uses Facial Recognition to Ban its Owner's Enemies," K. Hill and C. Kilgannon, New York Times, December 22, 2022. Link

[1271] "Amazon Sued for Not Telling New York Store Customers About Tracking Biometrics," K. Collier, NBC News, March 16, 2023. Link

[1272] "California Consumer Privacy Act (CCPA): What You Need to Know to Be Compliant," M. Korolov, CSO, July 7, 2020. Link

[1273] "Why Apple's New Privacy Feature is Such A Big Deal," C. Gartenberg, The Verge, April 27, 2021. Link

[1274] "National Strategy to Advance Privacy-Preserving Data Sharing and Analytics," Fast-track action committee on advancing privacy-preservation data sharing and analytics, Networking and information technology research and development subcommittee, National Science and Technology Council Report, March 2023. Link

[1275] "Top 10 Privacy Enhancing Technologies & Use Cases in 2023," C. Dilmegani, AI Multiple, July 21, 2020. Link

© Strategy of Things, 2025. All rights reserved.

- Synthetic data generation which uses artificially created data.
- Federated learning which trains algorithm across multiple decentralized edge devices.

Other

- Trusted execution environments[1276] which uses a secure area on a device to execute select operations in isolation.
- Zero party data[1277] based on data that a customer intentionally shares.

> PETs help mitigate some of the concerns but have limited adoption. PETs are seen as a gap because of "the need for more research and development, limited technical expertise, perceived and possible risks, financial cost and the lack of generalizable solutions."
>
> Continuing research and development are necessary to address some challenges and accelerate these privacy enhancing technologies. For example, the National Strategy to Advance Privacy-Preserving Data Sharing and Analytics report cites cryptographic technologies having initial success for real world adoption in simple applications. They still, however, have "scalability and efficiency challenges that need to be addressed in the context of a broader set of threat model."
>
> In addition, PET technologies lack consensus standards. While some standards development is underway for homomorphic encryption and zero knowledge proofs, the same report cites "more standards that specify foundational cryptographic primitives and other Privacy Preserving Data Sharing and Analytics (PPDSA) technologies would facilitate adoption and trust in solutions." Finally, the National Strategy to Advance Privacy-Preserving Data Sharing and Analytics report[1278] notes that "there are no widely adopted standards for data formats, application programming interfaces or system architectures that are necessary to facilitate the interoperability and deployment of PPDSA technologies." See Section 17.3.1

Similarly, while Forbes magazine called Zero Party Data (ZPD) the "new oil,"[1279] it has some limitations. Because these data come from a subset of customers willing to share, they may not be representative of the overall customer base. Customers may intentionally provide misleading or incomplete information or do so unintentionally due to the way the information was requested or fall victim to social and cognitive biases in responding to the requests.[1280] New artificial

---

[1276] "The New Generation of Privacy Preserving Technologies," R. Potter, CapGemini Expert Perspectives, June 13, 2022. Link

[1277] "Straight From the Source: Collecting Zero-Party Data From Customers," S. Liu, Forrester Research Blog, July 30, 2020. Link

[1278] See note 1274

[1279] "Zero-Party Data is the New Oil," V. Gozman, Forbes, March 14, 2022. Link

[1280] "Zero Party Data Between Hype and Hope," A. Polonioli, Frontiers in Big Data, Volume 5 2022, August 30, 2022. Link

© Strategy of Things, 2025. All rights reserved.

intelligence and machine learning algorithms will be required to address these biases and extract insights and learnings.

20.3.1.3. Challenge # 3: Artificial Intelligence

As IoT adoption increases in the retail industry, it is expected to generate a "tsunami of data" that retailers are not prepared to manage. A 2022 survey by RSR Research reported that, organizationally, 24% of retailers did not "have the skills to manage the analytics and predictive modeling required to take advantage of IoT data."[1281] The same report found that, technically and operationally, retailers struggled with:[1282]

- Combining IoT data with existing data infrastructure (47%).
- Determining the best response to specific data events or exceptions (36%).
- Representing IoT data in a meaningful way that enables insights (31%).
- Dealing with so much data from so many different sources in real time (30%).

> *One of the things that we hear a lot when we survey retailers is, 'I can barely make sense of the data that I'm already collecting… an enormous amount of information I'm collecting on the customer side.' And I think one of the areas where a lot of people who are in the quote, unquote, IOT space, fall down on, is they talk about all these possibilities. And they talk about once you're collecting all this information, you'll be able to do smarter and more intelligent things. … And retailers are just thinking, 'All I'm going to have is more data that I can't turn actionable'*
>
> *Steve Rowen, Managing Partner, RSR Research*[1283]

Artificial Intelligence (AI) technologies are poised to transform the industry by helping retailers make sense of data, create insights and act on those insights in both real time and autonomously. A 2019 survey of 168 decision-makers in enterprise retail organizations, conducted by Microsoft for its 2020 IoT Signals report, found that 44% of respondents stated that "AI is a core component of their IoT solutions." Furthermore, the report found that those retailers using AI said that they are "able to use their IoT solutions more quickly and more fully" and "plan to use IoT even more in the future than those not integrating AI."[1284]

[1281] See note 1246 Figure 13.

[1282] ibid. Figure 14.

[1283] Research interview, RSR Research, April 20, 2023

[1284] "IoT Signals Retail Report: IoT 's Promise for Retail Will Be Unlocked Addressing Security, Privacy and Compliance," S. George, Microsoft Azure blog, January 13, 2020. Link

© Strategy of Things, 2025. All rights reserved.

A 2023 survey of 1,420 global IT decision-makers across a variety of industries, conducted by Coleman Parkes Research for Rackspace Technology, found that 71% of the retail industry respondents indicated AI and machine learning lead their business and IT strategies.[1285]

A survey of 150 retailers, conducted by management consultancy KPMG, found that 81% of respondents reported the use of AI in operations was moderately functional or fully functional at scale.[1286]

The areas where AI can play a significant role include:[1287]

- Automating the shopping experience
- Inventory management
- Enhancing customer service
- Analyzing customer behavior
- Personalizing the shopping experience
- Optimizing pricing strategies

> *The big innovation in the last several years, five or six years, has been AI. And the reason it's so important is because it can sift through huge data links in a much, much more efficient way than we used to be able to do it. And that is a key enabler*
>
> *Brian Kilcourse, Co-founder, RSR Research*[1288]

To support AI and ML in retail industry operations, several key data technology capabilities are needed. These include:[1289]

- Intelligent data filtering (81%)
- Event-based alerting and exception management (72%)
- Real-time streaming data processing (71%)
- Predictive analytics (69%)
- Analytics at the edge (69%)
- Descriptive statistics (57%)
- Machine learning (57%)

[1285] "Exclusive: How important is AI in retail?" D. Berthiaum, Chain Store Age, February 28, 2023. Link

[1286] "Thriving in an AI world," S. Krishna et al, KPMG, May 2021. Link

[1287] "The Impact of Artificial Intelligence on the Retail Industry," Segwitz, January 28, 2023. Link

[1288] See note 1224

[1289] See note 1246 Figure 18

© Strategy of Things, 2025. All rights reserved.

These data capabilities are partially enabled by some of the key IoT technology requirements reported in our survey shown in Figure 20-7. For example, respondents to our survey identified processing, edge devices and data collection as key technology requirements enabling IoT in the retail industry.

Several technology infrastructure gaps, however, slow the adoption of AI in the retail industry. A 2019 global survey of 161 retailers of various sizes that have implemented AI in their organizations by research firm IDC reported the following technology infrastructure gaps:[1290]

- Trustworthiness/bias in the data (27% of respondents.
- Selection of the right algorithms (23%).
- Lack of adequate volumes of quality training data (22%).
- Explainability of algorithms (21%).
- Access to computing resources (19%).

The issue of overall AI trustworthiness was reported in another survey, which found only 33% of respondents in retail strongly trusted AI/ML results, while 35% slightly trusted the results. Nearly half of the respondents, 47%, believe that there are only "slightly enough checks and balances in place to avoid the negative consequences of AI/ML." One of the reasons for these attitudes may be attributed to algorithm and model failures, with 59% of respondents citing it as one of their greatest AI/ML challenges.[1291] This theme was echoed in the 2021 KPMG survey, which reported that 45% of retail respondents cited potential bias as one of their top two risks for AI.[1292]

In Section 20.3.1.2, privacy concerns were identified as a technology infrastructure gap slowing IoT adoption. Privacy concerns limit what data can be collected and how it is managed and used. This in turn impacts algorithm development and model training. To ensure relevance and accuracy of outcomes, new algorithms will need to be developed that can analyze limited sets of data that customers are willing to share under a "zero party data" protocol. In addition, synthetic data may be needed to train algorithms and improve their accuracy.[1293]

To users in the retail industry, AI is a black box with data from IoT and other sources coming in and actionable insights, recommendations and automated process activations going out. For example, inventory levels and Point of Sale (POS) data are inputs into an AI algorithm, which will output what new inventory to order, how much to order, what outlets and quantities it is to be distributed to and at what price.

The decision process used by the AI model is not visible, transparent or easily explainable to decision-makers. This lack of explainability compromises trust and contributes to one of many

[1290] "Barriers and Challenges to AI Adoption in Retail", J. Duke, IDC Perspective, 2019. Link

[1291] "Exclusive: How Important is AI in Retail?" D. Berthiaum, Chain Store Age, February 28, 2023. Link

[1292] "Thriving in an AI world," S. Krishna et al, KPMG, April 2021. Link

[1293] See note 1279

© Strategy of Things, 2025. All rights reserved.

reasons why 55% of retail decision-makers encountered pushback or scrutiny about the penetration of AI/ML in their organization.[1294]

While the adoption and integration of IoT technologies into all aspects of retail operations is poised to make a significant impact, the ability of AI technologies to analyze and act on the "tsunami of data" collected will accelerate the disruption and transformation of the industry. The growing use of AI, however, may also lead to potential outcomes and decisions that are "biased, discriminatory, exclusionary or otherwise unfair."[1295] Continued investments in AI research and development are necessary to overcome some of the challenges slowing AI adoption and accelerate the scaling of IoT.

20.3.2. Other challenges

In addition to the technology infrastructure challenges, our research has identified other challenges that impact IoT adoption. These challenges did not meet the criteria for research consideration because they were either not a technology challenge or a technology related challenge that can be addressed by current marketplace offerings or capabilities.

These challenges include:

- Digital skills
- Legacy technology infrastructure

20.3.2.1. Digital Skills

In a 2021 cross industry survey of 437 global organizations, Gartner Research reported that 64% of respondents identified talent availability as the primary risk factor for the deployment of emerging technologies, a sixteen time increase over the 2020 figure.[1296]

IoT solutions require integration into a retailer's processes and systems. This includes integrating inventory and supply chain management, back-office Enterprise Resource Planning (ERP), customer management, stores and payment processing. Data from the IoT applications are then collected, integrated, processed and analyzed to drive appropriate insights and actions. A lack of key digital and analytics skills, however, slows the ability of the industry to adopt and scale IoT.

In addition to the more traditional technology skills such as software development, networking and managing customer facing and back-office systems, IoT applications require several new skills. These include IoT architecture and design, sensor and device integration, data analytics, cybersecurity and cloud and edge computing.

Based on an analysis of job descriptions posted by IT functions across the United States in the beginning of July 2021[1297] Gartner identified systems integration, machine learning, data

---

[1294] See note 1291

[1295] "Artificial Intelligence Could Lead to Extinction, Experts Warn," C. Vallance, BBC, May 31, 2023. Link

[1296] "The Gartner 2021-2023 Emerging Technology Roadmap Findings," L. Ramos et al., Gartner Webinar, 2021. Page. 14. Link

[1297] ibid. p. 38

© Strategy of Things, 2025. All rights reserved.

integration, cloud architecture and environments, artificial intelligence and data engineering as some of the critical in-demand skills.

Microsoft, in a 2019 survey of 168 decision makers across enterprise retail organizations, reported that a lack of technical knowledge was one of the top three concerns of U.S. retailers.[1298] Management consultancy Deloitte reported that nearly half of the 50 senior retail executives surveyed, expect a shortage in skilled workers for IT and analytics.[1299] RSR Research, in its 2022 research report, found that 24% of surveyed respondents did not have "the skills to manage the analytics and predictive modeling required to take advantage of IoT data."[1300]

This shortage is exacerbated by competition for the same talent from businesses in other industries. Realizing the value provided by IoT technologies requires a workforce capable of building, integrating and using these solutions. A shortage of key technology skills threatens to slow down digital transformation initiatives in retail.

20.3.2.2. Legacy technology infrastructure

From e-commerce and omnichannel operations to changing customer requirements, personalization and supply chain complexity, digital technology is a vital capability for retail industry performance and success.[1301]

Legacy systems and existing infrastructures are major barriers to business transformation in the retail industry. Many retailers have well-established IT infrastructures that are compatible with or support the requirements needed to integrate, deploy and operate IoT applications. According to RSR Research, however, in its April 2022 report, 38% of 104 retailers surveyed indicated that their "existing infrastructure is not capable of supporting Internet of Things."[1302] The report also found the following infrastructure related challenges in connecting IoT to the infrastructure.[1303]

- Combining IoT data with existing data infrastructure (47%).
- Connecting emerging IoT technologies to existing infrastructure (45%).
- Dealing with so much data from so many different sources in real time (30%).
- The lack of interoperability between different IoT based technologies (26%).
- Public concern over privacy issues/security breaches (15%).
- Connecting nascent IoT technologies to existing infrastructure (13%).

[1298] "IoT Signals Retail Report: IoT 's Promise for Retail Will Be Unlocked Addressing Security, Privacy and Compliance," S. George, Microsoft Blog, January 2020. Link

[1299] See note 1195 p. 6

[1300] See note 1246 Figure 13.

[1301] "The Tech Transformation Imperative in Retail," R. Bick et al., McKinsey & Company, May 2022. Link

[1302] See note 1246 Figure 13.

[1303] "Legacy System Key Barrier in Digital Transformation: Study," CXO Today, January 2019. Link

© Strategy of Things, 2025. All rights reserved.

A 2018 cross industry survey, conducted by technology consultancy Infosys, reported that 41% of respondents indicated "legacy systems" as the biggest barrier to digital transformation. Legacy systems slow business transformation in several ways. These include:[1304]

- Increasing cybersecurity risks because they are not designed to address modern threats.
- Preventing the realization of new value because of performance, scalability and inability to be modified or upgraded.
- Reducing the attraction and retention of technical talent because of a shrinking talent pool for outdated systems and desire to work in a more modern technology environment.
- Increasing the risks of poor data management and governance due to outdated methodologies and lack of compliance with standards and regulations.
- Slowing innovation by diverting resources away from new value creation to service these systems.

Modern systems provide retailers with capabilities that facilitate operations and digital transformation initiatives. Management consultancy McKinsey estimates that most of the retailers who have started technology transformation initiatives are stuck in the "emerging" phases.[1305] There are, however, many companies that have not upgraded their systems for a variety of reasons. These reasons include:[1306] [1307]

- "If it ain't broke, don't fix it" attitude
- Risk of operational disruption
- Legacy system complexity
- Large investment needed

[1304] "Five Ways Your Legacy Systems Hold Your Business Back," P. Godwal, IEEE Computer Society, August 18, 2022. Link

[1305] See note 1301, Exhibit 2.

[1306] Ibid.

[1307] "Why Legacy IT is Holding Back Retailers," L. Nguyen, Builder.ai, June 9, 2021. Link

© Strategy of Things, 2025. All rights reserved.

Appendix: Renewable Energy

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

© Strategy of Things, 2025. All rights reserved.

21. Appendix: Renewable Energy

This section describes the research findings for IoT technology infrastructure in the renewable energy industry. The topics discussed here are:

- Industry overview
- Use of IoT in renewable energy
- IoT challenges in renewable energy

21.1. Industry overview

Spurred by ongoing environmental sustainability initiatives and more recently, the Inflation Reduction Act of 2022,[1308] the renewable energy industry is one of the fastest growing industries in the United States.

This section presents some key facts about the renewable energy industry, as well as the most significant industry challenges.

21.1.1. Key facts

In 2021, the United States consumed 97 quadrillion British Thermal Units (BTU)[1309] of energy from primary energy sources. These sources include fossil fuels such as coal, petroleum, natural gas along with nuclear and renewables such as wind, solar, geothermal, hydroelectric and biomass. Of this total, one-eighth or 12.5%, comes from renewable energy sources.[1310]

The electricity that Americans consume is produced by converting primary energy sources into electrical power. In 2021, about 4.116 trillion kWh of electricity were generated at utility-scale electricity generation facilities in the United States. Of this, about 20% was from renewable energy sources.[1311] [1312]

Not included in these statistics are the additional 49 billion kWh of electricity generated from small scale photovoltaic systems.[1313] These are facilities that have less than one MW of electricity generating capacity. These small-scale PV systems are located near where the electricity is consumed. Some smaller systems are installed on building rooftops.

[1308] "H.R. 5376 – Inflation Reduction Act of 2022", Congress.gov. Link

[1309] Defined as the amount of heat required to raise the temperature of one pound of water by one degree Fahrenheit. The SI unit for energy is the Joule (J) and one BTU equals about 1,055 J

[1310] "July 2022 Monthly Energy Review", U.S. Energy Information Administration. Link

[1311] "What is U.S. Electricity Generation by Energy Source?", Frequently Asked Questions, U.S. Energy Information Administration. Link

[1312] Utility-scale electricity generation facilities are those power plants with at least one megawatt (MW) of electricity generating capacity.

[1313] ibid

© Strategy of Things, 2025. All rights reserved.

The percentage of power consumed from primary renewable sources has risen steadily from 6.2% in 2000 to 12.5% in 2021.[1314] In April 2022, renewable energy sources were 28% of total energy consumed.[1315] For the first five months of 2022, renewable energy sources accounted for 24.7% of total energy consumed. Most of the growth is attributed to solar and wind sources. By 2030, an analysis by the Sun Day Campaign forecasted the percentage will reach 30% by 2030.[1316]

Investments in clean energy transition infrastructure have been increasing annually, from $53 billion in 2014 to $105 billion in 2021. Most of this investment continues to be in renewable energy. For example, investments in renewable energy assets rose from just over $30 billion in 2014 to $47 billion in 2021.[1317] These investments have resulted in an increase in the U.S. renewable energy capacity, growing from 185 gigawatts (GW) to 353 GW over this period. Electric power generation grew from 550 terawatt hours (TWh) to 858 TWh over the same period.[1318]

The U.S. renewable industry directly and indirectly employed 620,000 people in 2020.[1319] The renewable electric power generation sector employed 517,000 people. Of that, 317,000 people were in solar, 51,900 were in hydropower and 116,800 were in wind power generation. The renewable fuels sector employed 103,000 people. Of this, 33,500 worked in corn ethanol, 32,400 with woody biomass and 19,500 with other ethanol products.

These job figures include those that indirectly support renewable energy generation such as growing the crops required for renewable fuels. For example, of the 317,000 jobs in solar, 165,000 were in construction of facilities, 49,700 were in professional services and 41,900 were in manufacturing of the solar equipment.[1320] Similarly, the corn ethanol sector created 33,500 jobs. Of that, 15,600 or 46.6% were in agriculture, 9,000 were in manufacturing and 6,200 were in wholesale trade.

Statistics from the U.S. Census Bureau indicated that there are 1,673 establishments that generate electricity from renewable sources. Hydroelectric, wind and solar generation establishments represent 85% of all establishments. In total, these establishments employ 18,777 people and generate $2.15 billion in annual payroll.[1321]

21.1.2. Industry challenges

[1314] "July 2022 Monthly Energy Review", U.S. Energy Information Administration. Link

[1315] Table 1.1. Net Generation by Energy Source: Total (All Sectors), 2012-May 2022, Electric Power Monthly. Link

[1316] "Renewables on Track to Provide 33-50% of U.S. 2030 Electricity, Biden's 80% Goal Still Possible", K. Bossong, July 22, 2021. Link

[1317] "Sustainable Energy in America: 2022 Factbook", p. 35, Bloomberg NEF, 2022. Link

[1318] "Sustainable Energy in America: 2022 Factbook", p. 22, Bloomberg NEF, 2022. Link

[1319] United States Energy & Employment Report 2021, U.S. Department of Energy. Link

[1320] Ibid.

[1321] U.S. Census Bureau, 2000, CBP Tables 2020. Link

© Strategy of Things, 2025. All rights reserved.

The U.S. renewable energy industry faces several challenges that constrain the growth of the industry. Four key challenges, which are relevant to the Internet of Things in renewable energy are:

- Integration of renewable sources into grid infrastructure
- Aging and outdated electric grid infrastructure
- Permitting and planning obstacles
- Workforce labor shortage

Each of these is discussed below.

21.1.2.1. Integration of renewable sources into grid infrastructure

While electricity consumed in the United States from renewable sources is predicted to reach one-third by 2030,[1322] managing and integrating this electricity into the existing grid is a complex task.

One of the major issues with electricity provided by solar sources into the electrical grid is the "duck curve" effect. Over the course of a day, solar energy is unable to meet all the electricity demands on its own and grid operators must spin up electricity produced by traditional power plants. In the early mornings and evenings when demand spikes, electricity from solar sources is low or zero and electricity is supplied exclusively from power plants.

From mid-morning to mid-afternoon, more electricity is supplied from solar sources and power plants are ramped down to align with demand. As the afternoon progresses and the sun sets, power plants must ramp back up to produce more electricity just as demand begins to rise. Over a twenty-four-hour period, the load or electricity demand, follows a profile resembling a duck.[1323] Wind sources, experiencing similar behaviors, follow a slightly different pattern called the "alligator curve."[1324]

Balancing electricity supply with demand in an agile way for operators is challenging. Power plants must operate at certain minimum levels to remain economically feasible. As more solar sources become operational and supply power to communities, these power plants ramp down power levels until they reach a level corresponding to the minimum level needed to maintain economic feasibility. When this happens, excess electricity from the solar sources must be

[1322] "Renewable energy could provide 33-50% of U.S. electricity by 2030, but unlikely to hit Biden 80% target," S. Rai-Roche, PV Tech, July 22, 2021. Link

[1323] Some imagination is required to see a duck. "Confronting the Duck Curve: How to Address Over-Generation of Solar Energy," B. Jones-Albertus, U.S. Department of Energy, October 12, 2017. Link

[1324] "Forget the Duck Curve. Renewables Integration in the Midwest is a Whole Other Animal," A. Twite, GreenTech Media, June 21, 2018. Link

© Strategy of Things, 2025. All rights reserved.

"curtailed" or taken off the grid.[1325] In other cases, the grid may not be able to deliver all the electricity supplied by renewable sources and production must be curtailed.[1326]

Another challenge of integrating renewable sources into the grid is the variability of the electricity supplied. Solar power generation relies on sunlight, which is subject to daily and seasonal variations. Factors such as cloud cover, time of day and geographical location can affect the amount of solar radiation reaching solar panels, leading to fluctuations in power output. Nighttime and cloudy weather result in a complete or partial cessation of solar energy production.

Similarly, wind power generation is dependent on wind speed and direction. Wind turbines require a minimum wind speed to start generating electricity and excessively high or low wind speeds may require shutting down the turbines for safety reasons. Wind patterns can fluctuate over short and long-time scales, resulting in unpredictable power generation.

Because of this variability, renewable energy sources pose challenges to grid stability. Sudden drops or spikes in power output can strain the balance between electricity supply and demand, potentially causing voltage fluctuations and frequency deviations.

This variability makes it challenging to accurately predict and plan for renewable energy generation. Utilities and grid operators must carefully manage power dispatch and system reserves to ensure a reliable electricity supply. The uncertainty associated with renewable energy can affect long-term energy planning and necessitate the integration of additional dispatchable power sources to maintain a stable grid.

Energy storage technologies, such as batteries, will alleviate some of these challenges. As the price of battery technologies continues to fall, the integration of batteries into solar power systems becomes more feasible. For example, lithium battery prices have fallen by 80% over the past five years. Research firm Mackenzie Power & Renewables has projected the amount of energy storage deployed to reach 5.4 GW by 2024. The National Renewable Energy Laboratory estimated that 120 GW of storage will be needed across the continental United States by 2050.[1327]

21.1.2.2. Aging and outdated electric grid infrastructure

The United States is in a transition to clean and renewable energy generation to address climate and sustainability goals. This transition is accelerated by President Biden's commitment to meet a 1.5°C-aligned goal of reducing emissions by 50-52 percent in 2030, a carbon-free power sector by 2035 and a net zero emissions economy by no later than 2050.[1328] In support of this,

---

[1325] "This "Duck Curve" is Solar Energy's Greatest Challenge," C. Waters, Vox Video, May 9, 2018. Link

[1326] "Reframing Curtailment: Why Too Much of a Good Thing is Still a Good Thing," D. Oleson, NREL, July 18, 2022. Link

[1327] "Declining Renewable Costs Drive Focus on Energy Storage," W. Hicks, National Renewable Energy Laboratory. January 2, 2020. Link

[1328] "President Biden to Catalyze Global Climate Action through the Major Economies Forum on Energy and Climate," The White House, April 20, 2023. Link

© Strategy of Things, 2025. All rights reserved.

thousands of wind and solar farms, as well as Distributed Energy Resources (DER) will need to be built and integrated into the electric grid.

This transition is difficult, however, due to an aging electric grid infrastructure. This infrastructure was designed to take power generated from large fossil fuel burning plants and carry it over miles of transmission lines to electricity consumers downstream.[1329] This infrastructure, with its 600,000 miles of backbone and 5.5 million miles of local distribution transmission lines,[1330] substations, transformers and other hardware, is decaying with age and underinvestment. In its 2021 report card for America's infrastructure, the American Society of Civil Engineers assigned a grade of "C -" to the overall energy infrastructure, including its electrical infrastructure.[1331]

According to reinsurance provider Swiss Re, transformers begin to malfunction after around 40 years.[1332] The average age of large power transformers, which manage 90% of U.S. electricity flow, is more than 40 years.

Transmission lines typically have a 50-year lifespan. The U.S. Department of Energy, in its 2015 Quadrennial Technology Review, reported that 70% of U.S. power transformers and transmission lines are more than 25 years old, while 60% of circuit breakers are 30 years or older.[1333] Consultancy Marsh & McLennan estimates 140,000 miles of transmission lines will need to be replaced by 2050, at a cost of $700 billion. An overhaul and update to an infrastructure capable of supporting future needs is estimated to cost from $1 to $2.4 trillion.[1334]

Another challenge is the lack of inter-region transmission lines that allow power to be shared across the country. The U.S. electric infrastructure is not one continuous grid, but three different grids that connect at a few points with little sharing of power.

These three grids are further divided into seven regional operators with competing interests.[1335] Due to the lack of inter-region transmission lines, energy generated from renewable sources in one region is generally "trapped" and stays in the region where it is generated, even if it has a surplus of energy to share with other regions.[1336]

[1329] "Why America's Outdated Energy Grid is a Climate Problem," C. Clifford, CNBC, February 17, 2023. Link

[1330] "2021 Report for America's Infrastructure," American Society of Civil Engineers, 2021. Page. 45. Link

[1331] ibid.

[1332] "Creaky U.S. Power Grid Threatens Progress on Renewables, EVs," T. McLaughlin, Reuters, May 12, 2022. Link

[1333] "Quadrennial Technology Review 2015, Chapter 3 Technology Assessments, Transmission and Distribution Components", U.S. Department of Energy, 2015.

[1334] "Creaky U.S. Power Grid Threatens Progress on Renewables, EVs," T. McLaughlin, Reuters, May 12, 2022. Link

[1335] "Why the U.S. Electric Grid Isn't Ready for the Energy Transition," N. Popovich and B. Plumer, New York Times, June 12, 2023. Link

[1336] "Creaky U.S. Power Grid Threatens Progress on Renewables, EVs," T. McLaughlin, Reuters, May 12, 2022. Link

© Strategy of Things, 2025. All rights reserved.

For example, while wind power in the regional grid operator Southwest Power Pool regularly meets 75% of its electricity demands in its 14-state region, the energy produced is not able to be shared with consumers in other regions. Solar farms in California produce excess electricity at midday but are unable to share it with regions in the east where solar production is decreasing as the sun sets.

In a February 2023 draft of the National Transmission Needs Study, the U.S. Department of Energy identified the need for interregional transmission as a key finding.

> *Expanding interregional transmission capacity enables the system to take advantage of the geographic and temporal diversity of energy resources, so that abundant production in one region can help compensate for low production in other areas, which improves the electric system's ability to produce affordable, reliable energy while increasing the operational flexibility of the grid. Utilizing increased geographic diversity of resources also reduces curtailment, thereby more efficiently integrating renewables to reach clean energy and decarbonization goals, realizing the full benefits of renewable generation investments and achieving further pollution reduction.*[1337]

A third challenge is the lack of interconnection transmission lines integrating power from the thousands of new wind and solar farms to the grid. Many of these solar and wind farms will be far from cities and the existing grid. Thousands of miles of new high-voltage transmission lines spanning multiple grid regions are needed to connect these renewable energy plants.

In a February 2023 draft of the National Transmission Needs Study, the U.S. Department of Energy stated that there is "a pressing need to expand electric transmission, driven by the need to improve grid reliability, resilience and resource adequacy, enhance renewable resource integration and access to clean energy, decrease energy burden, support electrification efforts and reduce congestion and curtailment."[1338]

A study conducted by the National Renewable Energy Laboratory (NREL), identified that "the total transmission capacity in 2035 is one to almost three times today's capacity, which would require between 1,400 and 10,100 miles of new high-capacity lines per year assuming new construction starts in 2026."[1339] With widespread adoption of electrical vehicles, Americans are estimated to use 40% more electricity by 2050.[1340]

The challenges faced by the current electric grid infrastructure to accommodate more renewable energy sources have led to several adverse impacts. One impact is the curtailment of energy from renewable sources. In some regions, the existing grid infrastructure may not have the capacity to carry all the electricity generated from renewable energy sources. This creates grid congestion and leads to power producers curtailing or reducing the output of renewable energy sources. This

---

[1337] "National Transmission Needs Study, Draft", U.S. Department of Energy, February 2023. Page 79. Link

[1338] ibid. p. 78

[1339] "Examining Supply-Side Options to Achieve 100% Clean Electricity by 2035", NREL, P. Denholm et al. Link

[1340] "Creaky U.S. Power Grid Threatens Progress on Renewables, EVs," T. McLaughlin, Reuters, May 12, 2022. Link

© Strategy of Things, 2025. All rights reserved.

results in revenue losses for project developers and inefficiencies in utilizing renewable energy potential. Grid congestion costs consumers $13.3 billion in 2021, double that of $6.7 billion in 2020.[1341]

Another major impact is the cancellation of planned projects. According to an analysis by the Natural Resources Defense Council's Sustainable FERC Project, 245 clean energy projects that had reached advanced stages of development withdrew their applications between January 2016 and July 2020.[1342] Experts and developers cited grid congestion and related grid upgrade costs as the main factors for withdrawing projects.[1343]

These factors make the projects financially less attractive or unfeasible. For example, while power producers typically pay for the interconnection lines needed to get their power to the grid, developers also incur additional costs to upgrade congested interstate transmission lines to get their electricity to market.[1344]

21.1.2.3. Permitting and planning obstacles

Renewable energy is a strategic contributor to addressing climate change and meet sustainability goals. Permitting and planning obstacles, however, slow the development, construction and connection of these renewable energy sources to the grid.

Developers are required to obtain a series of land-use and environmental permits from local, state and federal agencies. In addition, developers are required to undergo a series of reviews by utilities and grid operators to determine what grid infrastructure upgrades may be needed to support commercial operation. The review and permitting process is complex, onerous to navigate and may take years to complete. This results in unanticipated costs, lengthy delays and the cancellation of many proposed projects at various points in the development cycle. These obstacles are so significant that "[President] Biden's stated goal of purging polluting fossil fuels from the electrical grid by 2035 looks out of reach."[1345]

As an example, solar and wind farm projects occupy thousands of acres of land. This land use may violate current zoning and planning ordinances and require rezoning of the land before a "land-use" permit is issued. The project may also face opposition from local communities concerned about appearance, noise, pollution, traffic, hazards and other considerations. In addition, energy transmission lines that connect the electricity from the project site to the grid may run through federal, state, tribal and private property and other "right of ways." In addition, the construction process is disruptive to the land, the environment and the community. Access roads may need to be built or improved to accommodate the movement of materials, equipment

---

[1341] "US Grid Congestion Costs Soared to $13.3B in 2021, Will Likely Grow Until Transmission Capacity is Built: Report," E. Howland, Utility Dive, April 14, 2023. Link

[1342] "Grid Congestion a Growing Barrier for Wind, Solar Developers in MISO Territory," K. Lydersen, Energy News Network, September 29, 2020. Link

[1343] ibid.

[1344] ibid.

[1345] "Permits for U.S. Energy Projects Are So Bad Unlikely Allies Emerge," J. Saul et al, Bloomberg, June 7, 2023. Link

© Strategy of Things, 2025. All rights reserved.

and workers to the site. Finally, construction may result in the release of emissions into the air and discharges into streams and rivers.

Some states, such as California, have regulations such as the California Environmental Quality Act that requires the project planners to study and mitigate any environmental impacts. At the federal level, compliance with the Clean Air Act, the Clean Water Act, the National Environmental Policy Act and the Endangered Species Act requires developers to secure a variety of federal permits addressing wildlife protection, air and water protection and federal and protected land usage.

The process of obtaining the various permits is challenging. Between the period 2010 to 2017, the average time from formal start to final decision averaged 2.7 years for renewable energy generation projects.[1346] The required environmental impact studies averaging 661 pages, could take anywhere from three to six years and a median cost of $1.4 million to complete.[1347]

Before an energy source is connected to the grid, it is placed in an "interconnection queue" by the electric utilities and grid operators to undergo a series of impact studies. These studies assess the capability of the grid infrastructure to support the energy source and determine what transmission equipment and upgrades are needed and their cost. Successful completion of these studies results in an interconnection agreement between the utility and the project owner specifying operational terms and cost responsibilities. Upon execution of the agreement, projects are built and go into commercial operation.

At the end of 2022, there were over 10,000 proposed projects, representing 1,350 GW of generation capacity and 680 GW of storage, in the queue seeking interconnection. A majority of these, representing 1,260 GW of capacity are zero-carbon projects.[1348] The number of solar projects in the interconnection queue increased from 428 in 2018 to 1,934 in 2022. Similarly, installed power for wind projects continued to grow increasing to 135.9 GW in 2021 from 122.5GW in 2020. [1349]

Most of these proposed projects in the queue, however, will never be built. For example, only 21% of those projects in the queues, representing 14% of generation capacity, which requested interconnection between 2000 to 2017 reached commercial operations at the end of 2022. Wind and solar projects reaching completion rates are 20% and 14%, respectively.[1350] Nearly three-quarters, 72%, never completed and withdrew from the interconnection queues.[1351]

[1346] "America's Clean Energy Transition Requires Permitting Reform: Policy Recommendations for Success," P. Bledsoe and E. Sykes, Progressive Policy Institute, September 21, 2022. Link

[1347] "How Does Permitting for Clean Energy Infrastructure Work?", R. Sud and S. Patnaik, Brookings Institute, September 28, 2022. Link

[1348] "Queued Up: Characteristics of Power Plants Seeking Transmission Interconnection as of the end of 2022", J. Rand et al, Lawrence Berkeley National Laboratory, April 2023. Page. 3. Link

[1349] "Wind Market Reports: 2022 Edition", Office of Energy Efficiency and Renewable Energy. Link

[1350] "Queued Up: Characteristics of Power Plants Seeking Transmission Interconnection as of the end of 2022", J. Rand et al, Lawrence Berkeley National Laboratory, April 2023. p. 3. Link

[1351] ibid. p. 18.

© Strategy of Things, 2025. All rights reserved.

One of the contributors to the low completion rates is the long review cycles in the interconnection queues. As the number of proposed projects has grown, so have the review times. In 2022, the average time from entry into the interconnection queue to commercial operations is five years, up from under two years in 2008 and three years in 2015.[1352] These long review cycles put proposed projects at risk as changing costs affect economic viability, options to buy land expire and customers lose interest.[1353]

Another contributing factor is the cost required to connect to the grid. Project developers need to not only pay for the transmission line connecting to the grid, but also for upgrades to a sometimes remote grid to increase its overall capacity. These additional costs are unpredictable and may be higher than initially estimated.

For example, one developer cancelled a project after the studies determined the upgrade cost would be an additional $70 million beyond the original estimate of $10 million.[1354] One developer cancelling a project can create problems for others in the queue. When a proposed energy project drops out of the queue, the grid operator must redo studies for other pending projects and shift those upgrade costs to other developers which can lead to more cancellations and delays.

21.1.2.4. Labor shortage

The renewable energy industry in the United States is facing a significant labor shortage that will slow the country's transition to clean energy and its ability to meet climate and sustainability goals. This shortage is exacerbated by the passage of the Inflation Reduction Act of 2022, which will invest $370 billion in a variety of programs, tax credits and subsidies and initiatives that "will lower energy costs for families and small businesses, accelerate private investment in clean energy solutions in every sector of the economy and every corner of the country, strengthen supply chains for everything from critical minerals to efficient electric appliances and create good-paying jobs and new economic opportunities for workers."[1355]

Investments from the Inflation Reduction Act are estimated to create 537,000 jobs annually for the next ten years. Over a quarter, 152,500 or 28%, of the new jobs will be in "renewable and carbon-free power and transmission." Another 11%, or 61,447 will be jobs involved in "manufacturing clean energy components" and 18% or 95,394 will be jobs that create "energy efficient and electrified buildings."[1356] These jobs span a variety of disciplines, from manufacturing, installers, electricians, project managers to maintenance technicians and operators and other support and administrative roles.

[1352] ibid. p. 3.

[1353] "The U.S. Has Billions for Wind and Solar Projects. Good Luck Plugging Them In." B. Plumer. New York Times. February 23, 2023. Link

[1354] ibid.

[1355] "Building a Clean Energy Economy: A Guidebook to the Inflation Reduction Act's Investments in Clean Energy and Climate Action", The White House, January 2023. Page 5. Link

[1356] "Biden's Climate Agenda Has a Problem: Not Enough Workers", N. Groom and V. Volcovici, Reuters. January 11, 2023. Link

© Strategy of Things, 2025. All rights reserved.

A report issued by the American Clean Power Association identified manufacturing (38.1%), project development and operations (25.3%) and construction (20.7%) industries as the top 3 industries that would "experience the most significant job growth under a decarbonization policy."[1357]

As an example, 877 workers were employed in the offshore wind sector, out of a total of 120,164 workers in the U.S. wind industry in 2021. To meet the target of 30 GW of installed offshore wind capacity by 2030, the industry needs to add an annual average of 15,000 workers with 25% domestic content[1358] to 58,000 workers with 100% domestic content.

Analysis conducted by the National Renewable Energy Laboratory (NREL), estimates a majority (81.5%) of those manufacturing and supply chain jobs are concerned with the fabrication and assembly of the components, subassemblies, parts and materials from multiple tiers of the manufacturing process, assuming 100% domestic content. This includes jobs ranging from engineering and component design to factory level workers on the production lines. Around a tenth, or 7.2%, of the new jobs are in development activities, mostly professional roles that occur prior to installation of the offshore wind power.[1359]

The Interstate Renewable Energy Council (IREC) National Solar Jobs Census 2021 reported solar workers nationwide numbered 255,037 in 2021, an increase of just under 9 percent from the previous year. Two-thirds (14,350) of the new jobs were at installation and project development firms.[1360] The U.S. Bureau of Labor Statistics projects 2,500 job openings annually for solar photovoltaic installers until 2031.[1361]

Similarly, the ongoing shift to electrification is projected to result in 79,900 job openings for electricians every year until 2031.[1362] Many of these openings, however, are expected to replace workers who transfer to different jobs or retire. The American Clean Power Association identified construction (23.5%), production (17.9%), architecture and engineering (13.6%) and installation, maintenance and repair (10%) as the top four in-demand occupations that will be "impacted when increasing nationwide solar, wind and battery storage capacity."[1363]

[1357] "2021 Clean Energy Labor Supply", BW Research, American Clean Power Association report, 2021. Figure 7. Link

[1358] Domestic content is defined as the "percentage of domestic workers, vessels, suppliers or businesses supporting industry segments."

[1359] "U.S. Offshore Wind Workforce Assessment," J. Stefek, et al. National Renewable Energy Laboratory, October 2022. Page. 3. Link

[1360] "Solar Jobs Up in 47 States, Increase 9% Nationwide in 2021," A. Palmer, IREC Press Release, July 26, 2022. Link

[1361] "Job Outlook: Solar Photovoltaic Installers," U.S. Bureau of Labor Statistics, Occupational Outlook Handbook. Link

[1362] "Job Outlook: Electricians," U.S. Bureau of Labor Statistics, Occupational Outlook Handbook. Link

[1363] "2021 Clean Energy Labor Supply", BW Research, American Clean Power Association report, 2021. Figure 13. Link

© Strategy of Things, 2025. All rights reserved.

Most affected by the labor shortage will be electric vehicle and battery producers and solar panel and home efficiency installation companies.[1364] As an example, a majority (89%) of the solar firms surveyed reported difficulty finding qualified applicants, with nearly one-third (35%) reporting "very difficult." in their recruiting efforts.[1365]

There are several reasons that contribute to the labor shortage. These include:

- **Low overall U.S. unemployment rate.** As of February 2024, the unemployment rate is at a near historical low of 3.9%.[1366]
- **Low supply of trained and skilled labor**. Rapid industrial growth has created demand that outpaced the supply of skilled workers. The clean and renewable energy industry is competing with other industries for the same labor pool. In March 2023, there were 732,000 and 315,000 job openings in the U.S. manufacturing and construction industries, respectively.[1367]
- **Limited availability of training programs.** The development of comprehensive clean and renewable energy specific training programs has lagged the sector's growth. This reduces the supply of skilled workers and creates a mismatch between available job opportunities and the workforce's qualifications. While training and apprenticeship programs are emerging, these will take time to make a measurable impact.
- **Lower wages than comparable jobs in the fossil fuel industry.** The median annual 2021 salary for solar panel installers and wind turbine technicians was $47,670 and $56,260 respectively. In contrast, petroleum pump system and refinery operators were paid $79,340 over the same period.[1368]
- **Workforce retirements**. While many workers have reached or will reach retirement age, younger workers who typically replace them are increasingly choosing college over trade school. For example, a Pew Research study has found that 39 percent of millennials earned a bachelor's degree or higher, compared with 29 percent of Gen Xers and 24 to 25 percent of boomers.[1369] As a result, more people are leaving the energy industry faster than new hires are replacing them.[1370]

[1364] "Biden's Climate Agenda Has a Problem: Not Enough Workers", N. Groom and V. Volcovici, Reuters. January 11, 2023. Link

[1365] "Solar Jobs Up in 47 States, Increase 9% Nationwide in 2021," A. Palmer, IREC Press Release, July 26, 2022. Link

[1366] "The Employment Situation - May 2023", U.S. Bureau of Labor Statistics. News Release. June 2, 2023. Link

[1367] "US Unemployment Rate (I:USUR)" Link

[1368] "The Next Labor Secretary Will Face A Big Shortage of Clean-Energy Workers," M. Joselow, Washington Post, March 3, 2023. Link

[1369] "Millennial life: How Young Adulthood Today Compares with Prior Generations," Pew Research Center, February 14, 2019. Link

[1370] "Technical Skills Gaps Holding Renewable Energy Back," J. Marsh, Renewable Energy Magazine, June 23, 2023. Link

© Strategy of Things, 2025. All rights reserved.

21.2. IoT in the renewable energy industry

The U.S. renewable energy industry has been growing for the past decade, driven by a combination of state and federal climate action policies, consumer demand and economics.[1371] By 2030, it is estimated that one-third of the electricity generated in the United States will originate from renewable sources.[1372]

States play a key role in driving the transition to clean and renewable energy. Thirty U.S. states, as of 2020, have enacted policies or renewable portfolio standards requiring that a percentage of the electricity sold come from renewable sources by a specific date.[1373] For example, California has a renewable portfolio standard of 60% clean energy by 2030 and 100% by 2045. Similarly, Hawaii and Washington have renewable and clean energy goals of 100% by 2045.[1374]

The electrification of transportation, industrial applications and buildings is driving increased demand for electricity. This demand is met through increased electricity generation from both non-renewable and renewable sources. One study, co-authored by researchers at the National Renewable Energy Laboratory, Northern Arizona University and Evolved Energy Research, reported that electricity generation capacity must be doubled by 2050 to meet the increased demand.[1375] Electricity generated from renewable energy sources is likely to grow in proportion.[1376]

IoT is integral to the operation and maintenance of renewable energy systems. As the number of renewable energy systems increases, so will the demand for IoT solutions. Market analysts have projected the global IoT market in renewable energy is expected to grow from $62.4 billion in 2022 to $105.5 billion by 2029. North America represents over 50% of this market in 2022.[1377]

One of the biggest challenges that IoT addresses is the integration of renewable energy sources into the grid. IoT helps to optimize electricity generation from these sources. Sensors inform solar panel tracking motors to position the panels to maximize electricity generation throughout the day. Similarly, sensors inform positioning motors to orient the turbine blades to maximize power generation. This optimization of electricity generation helps to partially meet demand and

---

[1371] "Market Drivers", U.S. Environmental Protection Agency. Link

[1372] "Renewables on Track to Provide 33-50% of U.S. 2030 Electricity, Biden's 80% Goal Still Possible", K. Bossong, July 22, 2021. Link

[1373] "Contributions of Policies and Consumer Choice Drivers," U.S. Environmental Protection Agency. Link

[1374] "Renewable & Clean Energy Standards," DSIRE Insight, NC Clean Energy Technology Center, September 2020. Link

[1375] "Electrification Futures Study: Scenarios of Power System Evolution and Infrastructure Development for the United States," Murphy, Caitlin, Trieu Mai, Yinong Sun, Paige Jadun, Matteo Muratori, Brent Nelson and Ryan Jones. National Renewable Energy Laboratory. NREL/TP-6A20-72330. 2021. Figure ES-1. Link

[1376] ibid. Figure ES-2.

[1377] "IoT in Renewable Energy Market - Global Analysis and Forecast (2023-2029)", MMR, April 2023. Link

© Strategy of Things, 2025. All rights reserved.

reduces the use of fossil-fuel based "peaker plants"[1378] which run during periods of high electricity demand.

Another grid integration challenge is the management and distribution of electricity generated by solar and battery DER systems. Before batteries, the electricity generated by solar systems was immediately discharged to the grid, with only a small amount used by the home. The addition of batteries allows the DER owners and operators to store power and to manage how and when that power is discharged.

During the day there is an excess supply of electricity generated from solar sources and demand is met and the price the utilities pay is low. In the late afternoon, however, the solar generated electricity begins to decrease as demand starts. The batteries discharge the stored electricity to the local grid or microgrid as the price utilities pay is higher to reflect higher demand and limited supply.[1379] The discharge of this electricity helps to partially meet demand and reduces the use of "peaker plants" and upstream fossil fuel power plants.

A third challenge addressed by IoT is grid stability and resilience. The use of smart inverters facilitates the integration of solar and other DER into the local and larger electric grid. In addition to converting the generated electricity from Direct Current (DC) to Alternating Current (AC), smart inverters employ voltage and frequency sensors to detect grid conditions,[1380] communicate with grid operators and autonomously perform a range of functions to maintain grid stability and reliability.[1381] As more renewable systems and DERs are integrated into the grid, these functions are required to minimize grid disruptions.

Renewable energy systems will need to be maintained as they are deployed. IoT is well suited to facilitate and support some of these activities. For example, sensors mounted on wind turbines and other mechanical parts monitor the equipment's state of health indicating when a part will need service. Other sensors monitor battery state-of-charge, temperature and voltage to optimize the battery lifespan and performance through efficient charging and discharging.

IoT connectivity allows these systems to be monitored and controlled remotely, allowing many activities to be conducted from a central location instead of in the field. This proactive approach reduces unplanned downtime, the financial costs of lost power generation and extends equipment lifetime. Given the current labor shortage in the renewable energy industry, IoT facilitates operational efficiency and allows the workforce to be more productive.

21.2.1. IoT use cases

[1378] A peaker plant is a specialized type of power plant designed to generate electricity during periods of high electricity demand. These plants are typically activated during peak load times, such as hot summer days or cold winter evenings when energy consumption is at its highest.

[1379] "A Complete Guide to Distributed Energy Resources (Ders) and Their Role in a Sustainable Future," T. Thorsnes, Enode blog, May 3, 2022. Link

[1380] "Recent Trends In Smart Solar Inverter Technology," Delta, March 4, 2020. Link

[1381] "Smart Grid, Smart Inverters for a Smart Energy Future," B. Mow, National Renewable Energy Laboratory, December 14, 2017. Link

© Strategy of Things, 2025. All rights reserved.

Figure 21-1 shows a representative set of renewable energy use cases organized into four categories. These categories are:

- **Generation.** For example:
    - IoT sensors and data analytics are employed to monitor the performance of solar panels. This includes tracking panel efficiency, temperature and weather conditions to optimize energy production and identify maintenance needs.
    - Wind turbines are equipped with IoT sensors to monitor wind speed, direction and turbine performance. These data help operators adjust the orientation of wind turbines and maintain them more effectively

- **Storage.** The United States is expected to reach 49.5 GW of installed and operational energy storage capacity with over 10 GW expected to be added in 2023. Key energy storage technologies include Pumped Hydroelectric Storage (PHS), Compressed Air Energy Storage (CAES), Advanced Battery Energy Storage (ABES), Flywheel Energy Storage (FES), Thermal Energy Storage (TES) and Hydrogen Energy Storage (HES).

  IoT technology is used to monitor and manage these Energy Storage Systems (ESS). It helps maintain optimal charging and discharging rates, manages State of Charge (SoC) and State of Health (SoH) and ensures the safety of the storage system.

- **Distribution and Transmission.** IoT sensors and devices are used to create smart grids that optimize the distribution and consumption of renewable energy. These systems monitor real-time energy demand, supply and grid conditions, allowing for better load balancing and grid management

- **Consumption and Demand.** IoT platforms are used to create intelligent energy management systems that control energy sources, storage and consumption in real-time, ensuring efficient utilization of renewable energy.

© Strategy of Things, 2025. All rights reserved.

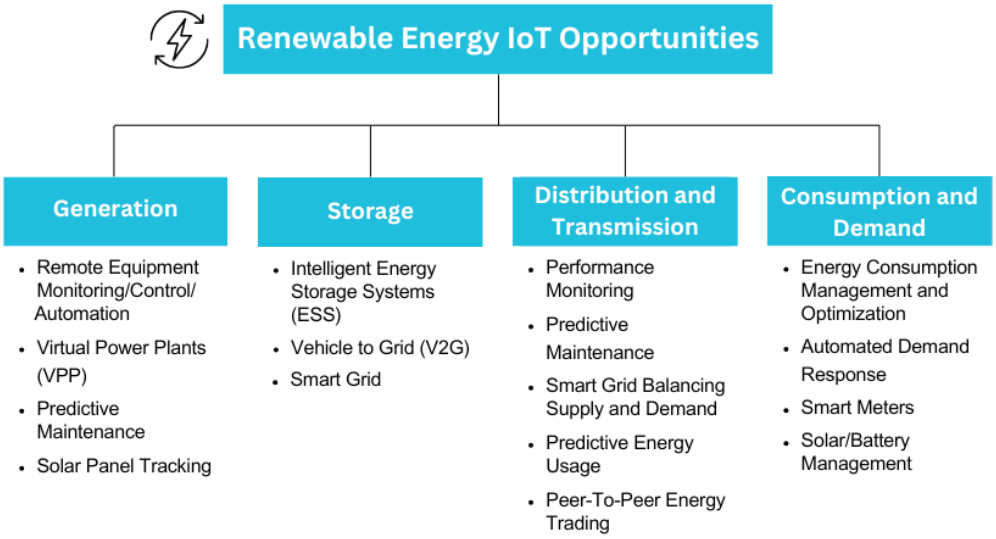


Figure 21-1: Renewable Energy: Use Case Categories and Selected Use Cases

21.2.1.1. Use case and industry challenges alignment

The renewable energy industry faces several challenges, some of which are described in Section 21.1.2 Figure 21-2 below shows the fit between the proposed use case subcategories and the documented industry challenges.

.

© Strategy of Things, 2025. All rights reserved.

Challenge	Role of IoT	Use case examples
Integration of renewable sources into grid infrastructure	Facilitate the integration of renewable energy sources into the grid by providing real-time data on energy production and consumption. Balances supply and demand and ensures the stability of the grid.	• Intelligent Energy Storage Systems (ESS) • Performance monitoring • Vehicle to grid (V2G) • Automated demand response
Aging and outdated electric grid infrastructure	Monitor the condition of the grid infrastructure, enabling predictive maintenance and timely upgrades. Helps extend the lifespan of the infrastructure and improves its ability to manage the variable nature of renewable energy.	• Virtual Power Plants (VPP) • Predictive maintenance • Solar panel tracking • Predictive energy usage • Smart grid balancing
Workforce labor shortage	Address labor shortages by automating routine tasks, such as monitoring and maintenance.	• Predictive maintenance • Smart Grid • Energy consumption management and optimization • Smart Meters
Permitting and planning obstacles	Support the permitting and planning process by providing accurate data, improving efficiency, and enhancing decision-making on potential renewable energy sites. Supports site analysis, feasibility studies and environmental compliance monitoring.	• Predictive analysis • Environmental monitoring • Operations monitoring • Construction monitoring

© Strategy of Things, 2025. All rights reserved.

Figure 21-2: Renewable Energy: Use Case and Industry Challenges Alignment

21.2.1.2. IoT use case details

Additional details on the use case subcategories shown in Figure 21-1 are provided below in Figure 21-3.

Category	Use Case	Definition
Generation	Remote equipment monitoring/ control/ automation	IoT sensors monitor and control renewable energy equipment, such as wind turbines and solar panels, from remote locations, allowing for real-time monitoring of energy production and performance and enables remote troubleshooting and maintenance.
	Virtual Power Plants (VPP)	Virtual Power Plants use IoT devices to aggregate the energy produced by decentralized sources such as rooftop solar and energy storage systems to meet the energy demands of a grid more efficiently and reliably.
	Predictive maintenance	Condition data from sensors are analyzed to predict when equipment, infrastructure and assets will need maintenance, before they fail, preventing breakdowns and reducing downtime by proactively scheduling maintenance based on actual conditions.
	Solar panel tracking	IoT devices monitor and control solar panel trackers to adjust panel orientation to receive the maximum exposure to the sun. The devices also collect data on operations performance for further optimization.
Storage	Intelligent Energy Storage Systems (ESS)	IoT-enabled batteries communicate with the grid to optimize energy usage and reduce costs. IoT sensors also monitor the status of batteries used for energy storage and predict when battery replacement is needed, allowing for better maintenance and energy management.
	Vehicle to grid (V2G)	IoT enabled smart charging systems and energy management software can monitor and control the flow of energy between electric vehicles and the power grid.

© Strategy of Things, 2025. All rights reserved.

Category	Use Case	Definition
Distribution & Transmission	Performance monitoring	Use of IoT devices to monitor and optimize the performance of energy distribution systems to help provide power efficiently and effectively.
	Predictive maintenance	IoT sensors are used to monitor the performance of renewable energy equipment, such as wind turbines and solar panels to predict when maintenance is needed.
	Smart grid balancing supply and demand	IoT devices monitor and control the distribution of renewable energy from sources such as wind turbines and solar panels allowing for more efficient use of energy and helping to balance supply and demand.
	Predictive energy usage	IoT devices collect data on energy consumption patterns and make predictions on future energy usage to facilitate more accurate decision making for energy production and distribution.
	Peer-to-peer energy trading	IoT enabled peer-to-peer energy trading platforms allow individuals to buy and sell energy from their own renewable energy systems. IoT enabled community microgrids allow communities to generate and manage their own energy distribution.

© Strategy of Things, 2025. All rights reserved.

Category	Use Case	Definition
Consumption and Demand	Energy consumption management and optimization	IoT devices and sensors monitor and optimize energy consumption with the goal of reducing waste and improving energy efficiency.
	Automated demand response	A system using IoT devices that automatically adjusts the energy usage of a building in response to changes in the electric grid's demand for power, reducing peak demand and increasing grid stability.
	Smart Meters	IoT enabled energy meters monitor and manage energy consumption in real-time eliminating the need for manual readings.
	Solar/battery management	IoT devices are used to help ensure energy stored in batteries is used efficiently and effectively such as using solar energy during peak hours maximizing the benefits of a solar energy system.

Figure 21-3: Renewable Energy: Use Case Details

© Strategy of Things, 2025. All rights reserved.

21.2.2. Market views of IoT in renewable energy

To understand market views on IoT and to inform on our gaps discovery and analysis, our research team conducted a survey of over 450 people, from adopters to solution providers, across the nine industries studied. Survey respondents were asked their opinion on the importance of IoT for the renewable energy industry over the next 5 to 10 years. Figure 21-4 below shows respondents expected IoT to have a relatively low impact (55%) as compared to other industries.

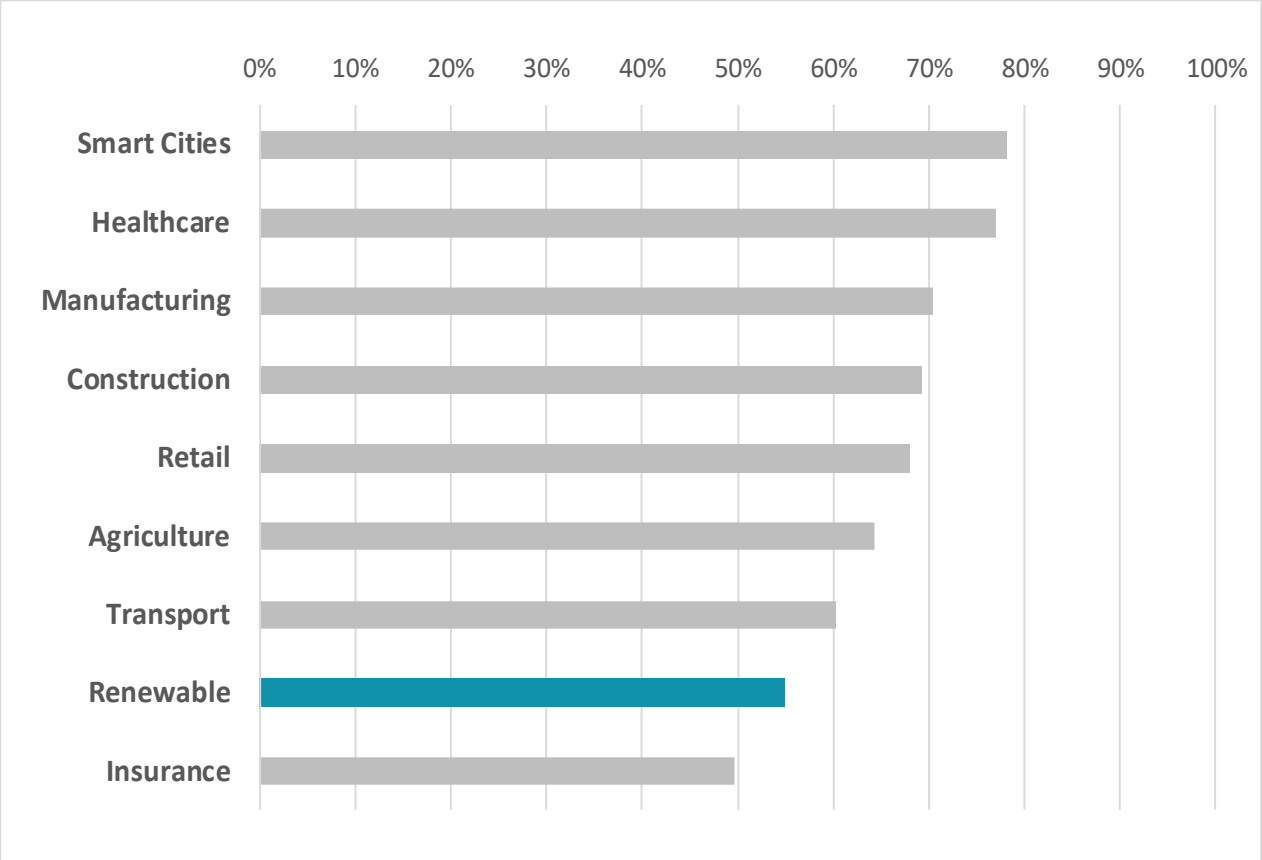


Figure 21-4: Renewable Energy: Importance of IoT

21.3. IoT gaps and findings in renewable energy

A combination of interviews, secondary research and surveys was conducted to identify and understand the opportunities and challenges to the development and adoption of IoT. Each research method approached the challenges from a different perspective.

For example, the survey targeted a large audience but asked specific questions that supported the economic analysis. The interviews targeted a small number of people who provided deeper insight and context to supplement the information already collected. Finally, the desk research, consisting of a review of online news articles, published research reports, vendor and government white papers, blogs, webinars, videos and other content provided a broad overview of the application of IoT in the industry.

© Strategy of Things, 2025. All rights reserved.

In our survey, respondents were asked to choose the most important technology areas to operationalize IoT in their industry. Figure 21-5 below shows respondent's selections of the top 10 IoT technologies and the percentage of respondents who chose that technology.[1382] The survey results are not seen as a technology gaps list, but rather an indication of what is important to the respondents. This information partially informs the gap selection process.

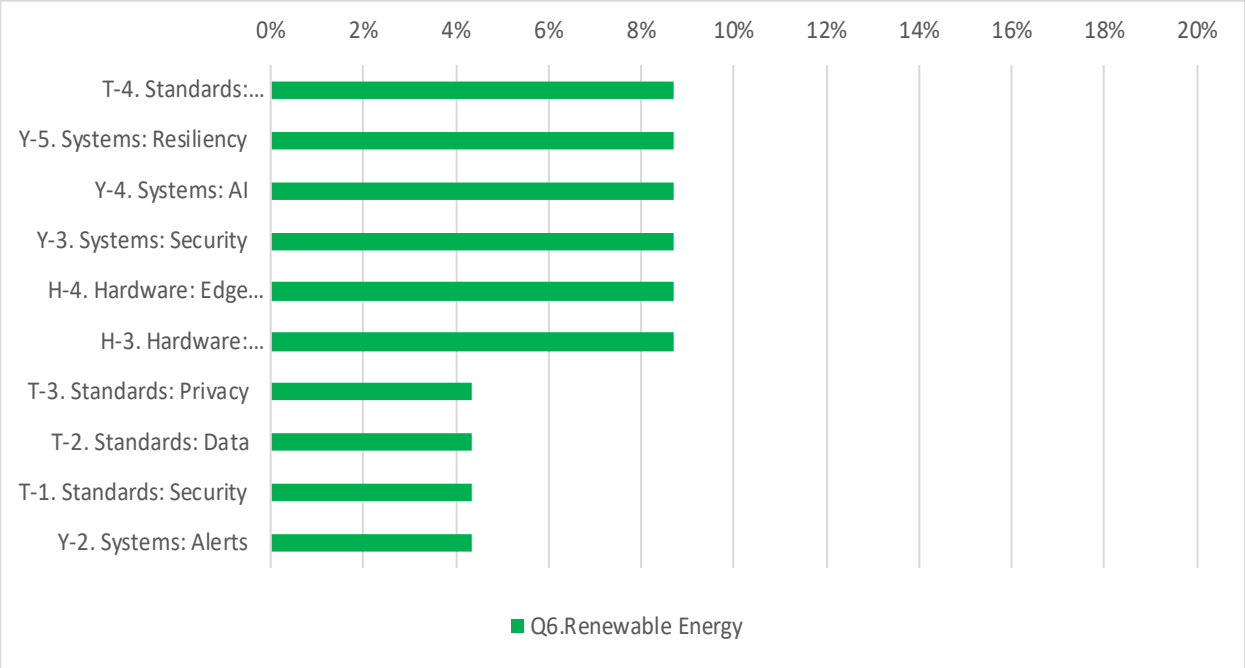


Figure 21-5: Renewable Energy: Top 10 Most Important Single Technologies

21.3.1. Top technology challenges

Based on the approach discussed above, the following three challenges were selected for further consideration. These are:

- DER cybersecurity
- Interoperability
- Data Management

21.3.1.1. Challenge # 1: DER cybersecurity

The energy infrastructure is an attractive target for hackers and cybercriminals. The U.S. Cybersecurity and Infrastructure Security Agency has identified electricity generation as one of 55 national critical functions that are "so vital to the United States that their disruption,

[1382] Respondents were asked to choose up to 5 out of the 25 technologies listed.

For renewable energy there were insufficient responses to undertake a more detailed breakdown of the importance of different use case categories or confidence in suppliers.

© Strategy of Things, 2025. All rights reserved.

corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety or any combination thereof."[1383]

The introduction of IoT and "smart technologies" into the energy infrastructure creates potential cybersecurity vulnerabilities that may allow cyber-attackers to disrupt grid operations and electricity delivery.

For example, distributed energy resources (DER)[1384] such as photovoltaic and energy storage systems, use "smart inverters" to integrate electricity into the grid. Smart inverters combine power electronics, software and two-way communications to monitor and manage when and how much electricity is released into the grid based on real time conditions. To support and automate the bi-directional electricity flows enabled by DERs, operators and utility companies add smart transformers and distribution management systems to the grid. The communications capabilities of the installed IoT devices introduces potential cybersecurity vulnerabilities that can be exploited by cyber-attackers. The impact of these disruptions becomes more significant as more renewable sourced utility scale generation plants and DERs are added to the grid.

In 2019, a renewable energy generator company, the largest private owner of operating solar assets in the United States, was subjected to a Denial of Service (DoS) attack. While no loss of energy generation was reported in the attack, the company lost visibility to around 500 MW of wind and solar generation in California, Utah and Wyoming.[1385]

This incident is one example of an increasingly frequent pattern. An IBM report found that the energy sector was the third and fourth most targeted sector in 2020 and 2021 respectively.[1386] According to a report by Check Point One, the utility industry averaged 736 cyberattacks per week and experienced a 46 per cent year on year increase in cyber-attacks in 2021.[1387]

> *Renewable energy penetration to the grid across the globe is on the rise and with their critical role of supporting sustainability, energy independence as well as quicker demand response, they are being incorporated not only by utilities but also residentially. This adoption makes them a lucrative target for cyber-attacks due to their interconnectedness with the power grid and their potential catastrophic consequences.*[1388]

[1383] National Critical Functions Set, Cybersecurity and Infrastructure Security Agency. Link

[1384] "Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid", U.S. Department of Energy's Office of Cybersecurity, Energy Security and Emergency Response and the Office of Energy Efficiency and Renewable Energy, October 2022, Page 3. Link

[1385] "First Cyberattack on Solar, Wind Assets Revealed Widespread Grid Weaknesses, Analysts Say," R. Walton, Utility Dive, November 4, 2019. Link

[1386] "As Solar Cybersecurity Becomes Critical, Industry Collaboration and Education Become Vital", Wood Mackenzie white paper. Link

[1387] "Renewable Energy Remains a Lucrative Target for Cyber Criminals", B. Maundrill, Cyber Security Hub, January 21, 2022. Link

[1388] ibid.

© Strategy of Things, 2025. All rights reserved.

The shift to integrate renewable energy sources is transforming the electric grid. One change is the generation of power from photovoltaic and battery systems in the local grid for cities and towns. The addition of these distributed energy sources to the grid poses unique IoT cybersecurity challenges. These include:

- **Large numbers of potential vulnerability points.** In traditional centralized power generation, a few large plants produce electricity and transmit it downstream for distribution and consumption. In distributed power generation, electricity is generated at the edge of the grid by many small power producers. These producers use IoT enabled devices and solutions from many different vendors with varying levels of cybersecurity measures, hardware configurations, software updates and configurations.

  In addition, the hardware and software supply chain for IoT and other smart devices could be vulnerable in the future. For example, compromised software or firmware updates could be installed during system updates.
- **New parties responsible for cybersecurity.**[1389] In the traditional centralized model, a small network of power producers, utility companies and grid operators was responsible for supplying electricity and managing the infrastructure and systems. The rapid growth of DERs, however, means that the DER owners, integrators, operators and aggregators are responsible not only for electricity generation, but also for addressing cybersecurity vulnerabilities of their systems. This may require skills and knowledge, tools, resources and coordination with each other in the DER supply chain as well as with the traditional utility companies.
- **Varying states of cybersecurity protections and updates.** In a distributed environment with hundreds of thousands of individual parties involved, the ability to effectively manage cybersecurity integrity is challenging.

  For example, implementing simple software or firmware updates can be challenging. Over-the-air firmware and software updates may not be completed due to poor connectivity at the time of update. The smart inverters may be built on older hardware which may not support the updated software. In addition, the inverter may be running an older version of the software and may require a two or three step process to complete the update. Finally, DERs may use inverters from different vendors making the version tracking process difficult.
- **Model of implied trust not suitable for modern grids.** In an automated environment with hundreds of thousands of DERs communicating in response to real time loads on the grid, IoT vulnerabilities may allow attackers to insert themselves in the middle and disrupt operations. The implied trust model which allows different systems and devices in the grid to communicate with each other "unchallenged" increases risk to the integrity of the grid and its ability to monitor, manage and deliver electricity to its users.

[1389] "Cybersecurity Considerations for Distributed Energy Resources on the U.S. Electric Grid", U.S. Department of Energy's Office of Cybersecurity, Energy Security and Emergency Response and the Office of Energy Efficiency and Renewable Energy, October 2022, Page 8. Link

© Strategy of Things, 2025. All rights reserved.

> *Addressing cybersecurity challenges over the next decade must be a key priority for the DER industry, which includes both utilities and DER owners, operators, developers, software and hardware vendors and aggregators. The goal is to mitigate current risks to the energy grid and to be prepared for the threats and vulnerabilities of the future. These mitigations form the base of a new framework for defining the defensive posture of the future grid.*[1390]

IoT technologies play a critical role in facilitating and accelerating the integration of electricity from renewable energy sources. Continued research and development is necessary in DER cybersecurity standards, trust models and cybersecurity operations.

21.3.1.2. Challenge # 2: Interoperability

Interoperability is a major challenge in the renewable energy industry. As the grid increasingly incorporates communications capabilities, the lack of interoperability slows the integration and exchange of data between different energy devices and systems. This communication is vital for the operation of renewable energy systems in supplying electricity into the smart electrical grid.

A survey of 250 American utility companies, conducted in January 2023 and commissioned by the Wi-Sun Alliance, reported that more than two-thirds of respondents (69%) cited open standards and multi-vendor interoperability as important drivers of smart utility development.[1391]

> *There are no standards today… we work with a lot of battery companies to integrate with their systems... I feel like they're in some weird competition of who uses the most odd communication standard. In general, it's kind of the wild west in that there's just so many different APIs and different communication protocols and different rules and every company is using their own.*
>
> *Alex Bazhinov, CEO, Lumin*[1392]

Grid operators continuously balance the dynamic demand for electricity with supply. To meet daily demand, grid operators bring in electricity generated by a combination of upstream fossil fuel power plants, clean energy such as solar, wind, hydro, geothermal and nuclear generation plants along with local DERs.

During periods where demand exceeds supply, demand is artificially reduced through partial service shutdowns and the use of utility provided Automated Demand Response (ADR) systems that limit the use of devices and equipment in participating homes and businesses.

Electricity supplied by DERs is increasingly common in homes and commercial buildings in the United States. These solar systems generate electricity, some of which is stored in batteries, some used by the home or business and some discharged into the local grid to meet local

---

[1390] See note 1384 p. 3

[1391] "Utilities call for more government funding and pilot projects to drive smart utility development - Wi-SUN Alliance survey," Energy Central News, February 21, 2023. Link

[1392] Research interview with Alex Bazhinov. October 12, 2022

© Strategy of Things, 2025. All rights reserved.

electricity demand. In addition, the increasing number of electric vehicles presents a future opportunity where EV batteries supply electricity into the local grid.

The ability of the various energy management devices and systems to communicate and interoperate with each other is essential to matching electricity supply and demand. For example, DERs employ smart inverters that communicate between the solar system, the battery and the local grid to distribute electricity appropriately. Smart meters provide the utility and grid operators with information to optimize the distribution of energy resources, predict demand, prevent outages and integrate renewable energy sources more effectively.

Utility companies communicate with ADR systems to limit electricity use in homes and businesses during summer peak demand times. A 2023 report by UK based sustainability advisory firm, Carbon Trust, identified five nodes in a DER system where interoperability is essential.[1393] These are inverters, smart meters, electric vehicle supply equipment, smart building applications and energy aggregators.

Some examples of this lack of interoperability include:[1394]

- Equipment such as batteries and inverters may not work together or with legacy devices.
- Inverters and/or batteries lack a standardized set of capabilities such as black start or back-up power
- Legacy devices lack the capability to connect to the internet or communicate with energy aggregators
- Building Energy Management Systems cannot communicate with DER system components and the grid

A lack of "standards" and competing standards reduces interoperability. For example, California's need for more advanced inverter functionality to support its grid infrastructure resulted in the state enacting Rule 21. This regulation mandated that smart inverters deployed after 2017 have certain grid support and communications capabilities.[1395]

The global standard for smart inverters, IEEE 2547-2018 was published a year later in 2018. To adhere with this global standard and eliminate interoperability issues, California is harmonizing its Rule 21 interconnection requirements with IEEE 1547-2018. As of April 2023, approximately twenty states are in various stages of adoption of this standard for smart inverters.[1396]

[1393] "Interoperability of distributed energy resources: Benefits, challenges and solutions," R. Harris, Carbon Trust, June 2023. Link

[1394] See note 1393

[1395] "California's New Smart Inverter Requirements: What "Rule 21" Means for Solar Design," Blog Post, Aurora. Link

[1396] "IEEE 1547™-2018 Adoption Tracker," IREC, April 3, 2023. Link

© Strategy of Things, 2025. All rights reserved.

> *.Contractors are not able to specify batteries and inverters and have it work together. This is unlike the solar panel side where contractors can specify all the components themselves and be assured that everything works together.*
>
> *What you want is to have an automated script that runs when you plug it in and IoT takes over. It identifies what component parts you are connected to, what the configuration is and boom, it makes it happen.*
>
> *But in reality, what happens is that the technician runs into issues in the field. The Modbus map may have been updated from previous installs, now this doesn't work with that. Now you have to get to technical support with three different vendors to find out what is going on. This is the state of industry. It can take days to do final commissioning on a battery system because you have to jump through all sorts of hoops..*
>
> *Adam Boucher, CEO, Molecule Systems*[1397]

Even when standards have been developed, driving adoption of those standards is challenging. While there are ongoing industry efforts to standardize communications, there are three barriers to adoption of these standards. These include:[1398]

- Reluctance to move away from proprietary protocols without regulatory or utility mandates.
- Focus on development of narrow standards to solve specific needs instead of broader standards that can accommodate new applications.
- Lack of knowledge in specifying and deploying standards to innovative applications especially those applications that impact reliability and rate structure.

There are several reasons cited for a lack of interoperability, including:[1399]

- DERs that are not designed 'from the ground up' to be interoperable.
- Manufacturer's competitive use of proprietary approaches such as faster go-to-market and limited development costs.
- Provincial or piecemeal approach to DER integration into the grid.[1400]
- Government regulations and policies that are inconsistent across states or regions

---

[1397] Research interview with Adam Boucher, April 4, 2022.

[1398] "Standardizing the Battery Storage Communications Infrastructure," J. Mater, Bulletin. IEEE Smart Grid. February 2017. Link

[1399] See note 1393

[1400] "The Transition to a High-DER Electricity System: Creating a National Initiative on DER Integration for the United States," Distributed Energy Resources Task Force, Energy Systems Integration Group, August 2022. Link

© Strategy of Things, 2025. All rights reserved.

- Lack of open standards.[1401]

The lack of interoperability impacts both DERs and the smart grid, including:[1402] [1403] [1404]

- A fragmented marketplace of "walled garden" DER solutions that work with a small set of "compatible" equipment limits choice and creates vendor "lock-in".
- The inability to access current and future functionality, such as V2G charging for electric vehicles[1405] and back-up power for batteries to meet demand.
- Reduced effective integration of energy efficiency and renewable energy technologies at scale and limited ability to effectively monitor, manage and distribute electricity to meet demand. This leads to higher carbon emissions, higher energy investment and fuel costs per delivered unit of electricity and less energy security and independence.
- Limited new product and service innovation opportunities for utilities and device manufacturers.
- Reduced adoption by increased deployment costs, making energy efficiency and renewable energy solutions less affordable for consumers and utilities.
- Reduced entry to new markets with innovative offerings to support energy efficiency, cost reduction, customer-specific service needs and enhanced reliability of the electricity infrastructure.

Interoperability has financial and economic impacts. A 2009 study by the Gridwise Architecture Council, an industry group of professionals from across the electricity supply chain, estimated interoperability can lead up to $10 billion in annual savings, a 1 to 3% savings based on value of electricity produced in the United States.[1406] These savings result from lower transaction costs, increased operating efficiency, lower operations and maintenance needs, lower design and installation costs, lower support and upgrades costs, high quality service with fewer mistakes and new products and services through competitive innovation.

A 2016 report from the U.S. Department of Energy, examined the economic benefits enabled by interoperability on "the end-use devices in homes and buildings. [1407] [1408] This would enable

---

[1401] "The National Opportunity for Interoperability and its Benefits for a Reliable, Robust and Future Grid Realized Through Buildings," U.S. Department of Energy: Energy Efficiency and Renewable Energy, February 2016. P. ii. Link

[1402] See note 1393

[1403] See note 1401

[1404] "Financial Benefits of Interoperability," Harbor Research, Gridwise Architecture Council, 2009. Link

[1405] In a V2G application, electric vehicle batteries can be used to supply electricity to the grid as needed.

[1406] See note 1404

[1407] See note 1401

[1408] Buildings are the physical location for millions of new innovative energy efficient, renewable and "smart" technologies—including smart meters, smart building controls, electric vehicles (EVs), operational diagnostics

© Strategy of Things, 2025. All rights reserved.

devices to simply "work" without complications, complexity or additional cost to the consumer if the consumer so desires to coordinate electric system operations more effectively and efficiently." The report cited economic data from two sources:

- McKinsey estimated that customer applications, deployed in residential and commercial buildings, could be worth $59 billion, in 2009 dollars, in smart grid benefits annually by 2019
- The Pacific Northwest National Laboratory (PNNL) estimated the potential value of continuously engaging real-time flexible loads in both residential and commercial buildings to provide grid services at the national scale to be $22 billion in 2014 dollars

While the Department of Energy report examined end-use devices in homes and buildings, it also provided an overall vision into the energy grid and the innovative products and services that are possible when full interoperability is achieved. The report provides an understanding of the possible roles of government in enabling interoperability, including internal procurement of interoperable systems, promoting open standards, convening and building consensus with industry and developing the foundational approaches, technologies and workforce.[1409]

21.3.1.3. Challenge # 3: Data management

Information is essential to the operation of the modern electric grid. The IoT data produced from measuring the real time performance and energy production of wind turbines and solar panels supports actions that optimize grid performance and better meets demand. Furthermore, the health and condition data produced from monitoring wind turbines, solar panels and batteries can be used to optimize real time performance, detect potential problems and predict maintenance needs.

The management of these data, however, is a challenge for both the renewable energy industry and the electric power generation industry. The energy industry produces a large amount of data, on the order of 100 to 200 exabytes[1410] per year.[1411] There are 135 million smart utility meters in the United States producing a total of 54 petabytes[1412] of data or 400 MB of data per meter per year.[1413] The data are used for a variety of purposes including system planning, regulatory compliance, grid operations, commercial transactions and market efficiency.[1414]

---

and smart appliances. These devices represent an untapped opportunity and underused resource that, if appropriately configured and realized in open standards, can provide significant energy efficiency and commensurate savings on utility bills, enhanced and lower cost reliability to utilities. In addition, there may be national economic benefits in the creation of new markets, sectors and businesses being fueled by the seamless coordination of energy and information through device and technology interoperability

[1409] See note 1401 p. ii.

[1410] One exabyte is equivalent to 250 million DVDs. "What is an exabyte?" xtract.io Glossary. Link

[1411] "Analyzing Energy Consumption: Unleashing the Power of Data in the Energy Industry," Data Dynamics. Link

[1412] One petabyte is equivalent to 11,000 4K movies. "What is a petabyte?", xtract.io Glossary. Link

[1413] "Smart Meter Data Analysis," Heavy.AI. Link

[1414] "Data and the Electricity Grid," A. Shumavon, P. De Martini and L. Wang, More than Smart. Link

© Strategy of Things, 2025. All rights reserved.

The continuous real-time stream of information produced poses challenges in aggregating, securing, storing and distribution. This challenge is exacerbated by the growing deployment of DERs in local communities and as renewable energy utilities scale power generation plants which will generate additional data.

This inability to manage the growing amounts of data threatens the operation and automation of the grid, lessens the use of analytics and AI to plan and optimize grid operations, reduces regulatory compliance and limits innovation and the evolution of a potentially autonomous grid.

A 2022 survey conducted by consultancy EY across a segment of the electricity industry found that only 29% of respondents have a data strategy and 57% reported their data governance is "at a developing or initial level or maturity."[1415]

In addition to the growing amount of data produced and managed, other factors add to the complexity of the challenge. These include:

- Data comes from diverse and siloed sources, including Advanced Distribution Management Systems, Supervisory Control and Data Acquisition (SCADA), Geographic Information Systems (GIS), Advanced Metering Infrastructure (AMI) and Distributed Energy Resource Management Systems (DERMS).[1416]
- Large continuous streams of IoT data must be stored, processed and analyzed in real time.
- Varying levels of syntactic and semantic interoperability from data sourced from inverters, batteries, meters and other devices.
- Varying levels of data quality and accuracy from the disparate sources.
- Cybersecurity protection of the data in accordance with regulations.
- Privacy protection of the data such as demand response information in accordance with any applicable regulations.
- Existing and evolving regulatory and compliance requirements.
- Integration of data from various sources and types to support grid operations, planning and analytics, market trading, reporting and compliance.

Effective data management also provides usable information that AI and data analytics algorithms can process and act on to optimize operational decisions.

The growth in data volumes, however, requires that data management technologies evolve. For example, legacy data warehouses store data on servers using traditional Relational Database Management Systems (RDBMS). Whereas to store, process and analyze massive amounts of data from multiple sources in various formats, modern data warehouses store data in the cloud.

[1415] "Why the future of power and utilities depends on data," T. Thornton, EY, December 2, 2022. Link

[1416] "The Big Data Problem For Utilities," Camus, December 27, 2023. Link

© Strategy of Things, 2025. All rights reserved.

> Data fabrics, an emerging approach uses a network-based architecture to connect various disparate cloud databases and provides virtualized access to massive volumes of data not possible with legacy data warehouses.
>
> The growing volumes of IoT data are not unique to the renewable energy industry. Continued research and development of data management technologies and operations is important to meeting the evolving data needs across multiple industries. Extracted from Section 18.3.1

Data observability software company Monte Carlo has identified eight trends that impact the future of data management.[1417] These are:

- Data management supports and complies with increasing regulatory requirements.
- Data governance plays a more prominent and integrated role in data management.
- Data meshes require that data management support the decentralization of data, with "distributed data products, owned by independent cross-functional teams oriented around data domains."
- Decentralization of data requires data access governance that enables "restricting access only to those who need it as well as applying the right security measures and preventing breaches."
- Automation of data transformation with no-code tools enabling less technical data professionals to perform these activities.
- Increasing need to perform real-time processing of data streams.
- AI-based applications to simplify data management.
- Observability supports data management systems in understanding the health and state of data.

Potential areas for research include:

- Scalable and efficient data storage to manage the increasing volume of data generated by IoT devices in renewable energy systems, including distributed storage architectures, compression techniques and data deduplication methods to optimize storage efficiency.
- Real-time data processing and analytics to enhance real-time processing and analytics of IoT-generated data, including advanced algorithms, edge computing and in-memory processing techniques.
- Security and privacy in renewable energy IoT data, including encryption techniques, access control mechanisms and privacy-preserving analytics.
- Data quality assurance methodologies for ensuring the accuracy and reliability of IoT-generated data, such as developing calibration techniques for sensors, anomaly detection algorithms and data validation processes.

[1417] "The Future of Data Management: 8 Fast Growing Trends," J. So, Monte Carlo, July 15, 2022. Link

© Strategy of Things, 2025. All rights reserved.

- Data governance and compliance including compliance mechanisms for data protection regulations, standards for cybersecurity and ethical considerations in handling sensitive energy data.
- Lifecycle management of IoT data, including data collection, storage, processing, analysis and archiving in the context of renewable energy systems.

21.3.2. Other challenges

In addition to the technology challenges for further consideration, our research has identified other challenges that impact IoT adoption. These challenges did not meet the criteria for research consideration because they were either not a technology challenge or a technology related challenge that can be addressed by current marketplace offerings or capabilities.

21.3.2.1. Utility company alignment

The utility company business model is not fully aligned to support the rapid expansion of the renewable energy industry. In the United States, Investor Owned Utilities (IOU) represent 6% of the 2,938 electric utilities but serve 71% of the electricity customers in 2017.[1418] These IOU companies are incentivized to maximize revenues and profits for shareholders by selling as much electricity as possible. Electricity generated by the rapidly growing number of residential and commercial rooftop solar producers reduces the amount of electricity the IOUs sell. These conflicting goals lead to slower adoption and perceived utility resistance to the renewable industry.

> *There is a tug of war between solar developers, the marketplace and utility companies. The resistance by the utilities is slowing down solar adoption. Utilities have to hold on or control certain things. This drives up utility rates and results in a less reliable grid.*
>
> *Adam Boucher, CEO, Molecule Systems*[1419]

On a periodic basis, regulated utility companies undergo a formal regulatory process, called the rate case, to determine what they can charge customers for electricity over a specific period. Regulators determine the utility's revenue requirement, which is the total amount of money a utility must make, to pay for all expenses during the period.

The revenue requirements consider the utility's estimated expenses, such as capital spending to upgrade infrastructure, operating and maintenance expenses, return on investor capital, taxes and other costs to meet electricity demand over the specified period.

The revenue requirement is used to set the electricity rates that customers pay over the specified time. The rate case process drives IOUs to maximize electricity revenues, but in doing so, creates a conflict. While energy produced from DERs supports sustainability goals and helps meet local

[1418] "Investor-owned utilities served 72% of U.S. electricity customers in 2017," U.S. Energy Information Administration, August 15, 2019. Link

[1419] Research interview with Adam Boucher, April 4, 2022.

© Strategy of Things, 2025. All rights reserved.

electricity demand, DERs threaten the utility's ability to sell enough electricity to meet or exceed their revenue requirement.[1420]

> *... distributed solar is in direct conflict with the current utility business model. The current utility business model is to sell you more electrons all the time and when you're putting in solar on your roof, now they're selling you fewer electrons, even though they have to maintain exactly the same distribution infrastructure, in order to provide you with some electrons when the sun is not shining. So now they still have to pay for that infrastructure. But their top line is lower now, because they don't sell us much. And in the past, we've definitely seen utilities not acting fast enough on and quite often, actually acting in opposition to solar adoption and battery adoption. One of the most famous cases is early this year, net metering 3.0. It was a policy that was suggested for adoption in California that would be extremely harmful for solar by introducing the asymmetric metering concept. And it was fully sponsored by utility companies.*
>
> *Alex Bazhinov, CEO, Lumin*[1421]

One recent example of this is the implementation of Net Metering 3.0 (NEM 3.0) in California. Approved by regulators in December 2022 and taking effect on April 15, 2023, NEM 3.0 incentivizes the use of battery systems by reducing the rates that three IOUs will pay for excess electricity exported to the grid by 75%. This reduces the overall lifetime savings enjoyed by DER owners and increases the payback period of home solar.[1422] As a result, the California Solar and Storage Association (CALSSA) has reported that the industry lost 17,000 jobs as rooftop solar sales declined between 66% to 83% in 2023.

A 2023 industry survey reported that 70% of residential solar contractors are concerned about their business outlook with 43% of 300 companies believing it will be hard to remain in business over the winter[1423] At the same time, the state's goals of reaching 90% clean energy by 2035 and 100% by 2045[1424] are at risk.

[1420] "Policy Explainer: How Utility Reform Can Align Profits with Climate Goals," Climate Xchange, November 10, 2022. Link

[1421] Research interview with Alex Bazhinov. October 12, 2022.

[1422] "What is NEM 3.0 and How Will it Impact California Solar Owners in 2024?" S. Wigness, solar.com, December 28, 2023. Link

[1423] "Massive Layoffs, Business Closures and Loss of Clean Energy Progress Since CPUC Slashed Rooftop Solar Incentives, New Analysis Shows," Press Release, California Solar and Storage Association, November 30, 2023. Link

[1424] "Is California Still on Track to Meet Its Goal of 100% Clean Power by 2045?" L. Klivans, KQED, December 6, 2023. Link

© Strategy of Things, 2025. All rights reserved.

21.3.2.2. Lack of digital skills

Digitization is transforming the renewable energy industry, creating opportunities to enhance efficiency, drive sustainability and increase overall performance. Digital technologies are increasingly integrated across the renewable energy value chain from energy generation and distribution to consumption.

One prominent contributor to this digital transformation is the deployment of IoT devices and sensors across the renewable energy infrastructure. The data they generate are then analyzed using advanced analytics such as AI and machine learning algorithms, allowing for predictive maintenance, optimal resource allocation and improved overall system reliability.

Digital technologies also support the growth of decentralized and distributed energy systems, empowering consumers to actively participate in energy generation and consumption through technologies like rooftop solar panels and home energy management systems.

Digital skills are essential for the effective design, operation and maintenance of renewable energy infrastructure. A study predicting the future skill requirements of the renewable energy sector required to support industry digitization identified thirty-six skills. These include IoT, big data, artificial intelligence, machine learning, cloud computing, collaborative/autonomous robotics, cybersecurity, augmented reality, digital twins, agile human-machine interfaces and advanced IT and programming.[1425] Others have reported that data-driven management, data science, analytics and modeling are some of the most important skills for energy teams.[1426]

In a survey of 12,000 energy professionals in 149 countries conducted in 2023, the 2024 Global Energy Talent Index reported that 32% of respondents in the renewable energy industry use AI in their roles.

Furthermore, survey respondents believe AI will increase the demand for technical skills such as programming/software engineering and IT (both 27%), machine learning (26%), cybersecurity (24%) and robotics (23%).[1427]

There is, however, a shortage of digital talent that the industry needs to address. A survey of 1,395 business and IT leaders from large organizations in the UK, France, Germany, Ireland and India reported that 83% of energy business leaders have "under-invested in the technical skills base of their employees" and 79% reported that a "scarcity of skills in emerging technologies is a growing problem for their organization." In addition, nearly half, 49%, reported that talent shortages are a growing concern.[1428]

The impact of digital talent shortages is far reaching and includes:[1429]

[1425] "Definition of the Future Skills Needs of Job Profiles in the Renewable Energy Sector," I. Arcelay, et al., Energies 2021, 14(9), 2609; Link

[1426] "What's Needed To Close The Skills Gap In The Power Industry," B. Karschnia, Forbes, April 8, 2022. Link

[1427] "The Global Energy Talent Index 2024", Airswift report. 2024. Link

[1428] "Skills gap & underinvestment disrupting industry – survey," Y. Latief, Smart Energy International, May 24, 2023. Link

[1429] "Skills Shortage for the Energy Industry," S. Smith, People with Energy, September 21, 2023. Link

© Strategy of Things, 2025. All rights reserved.

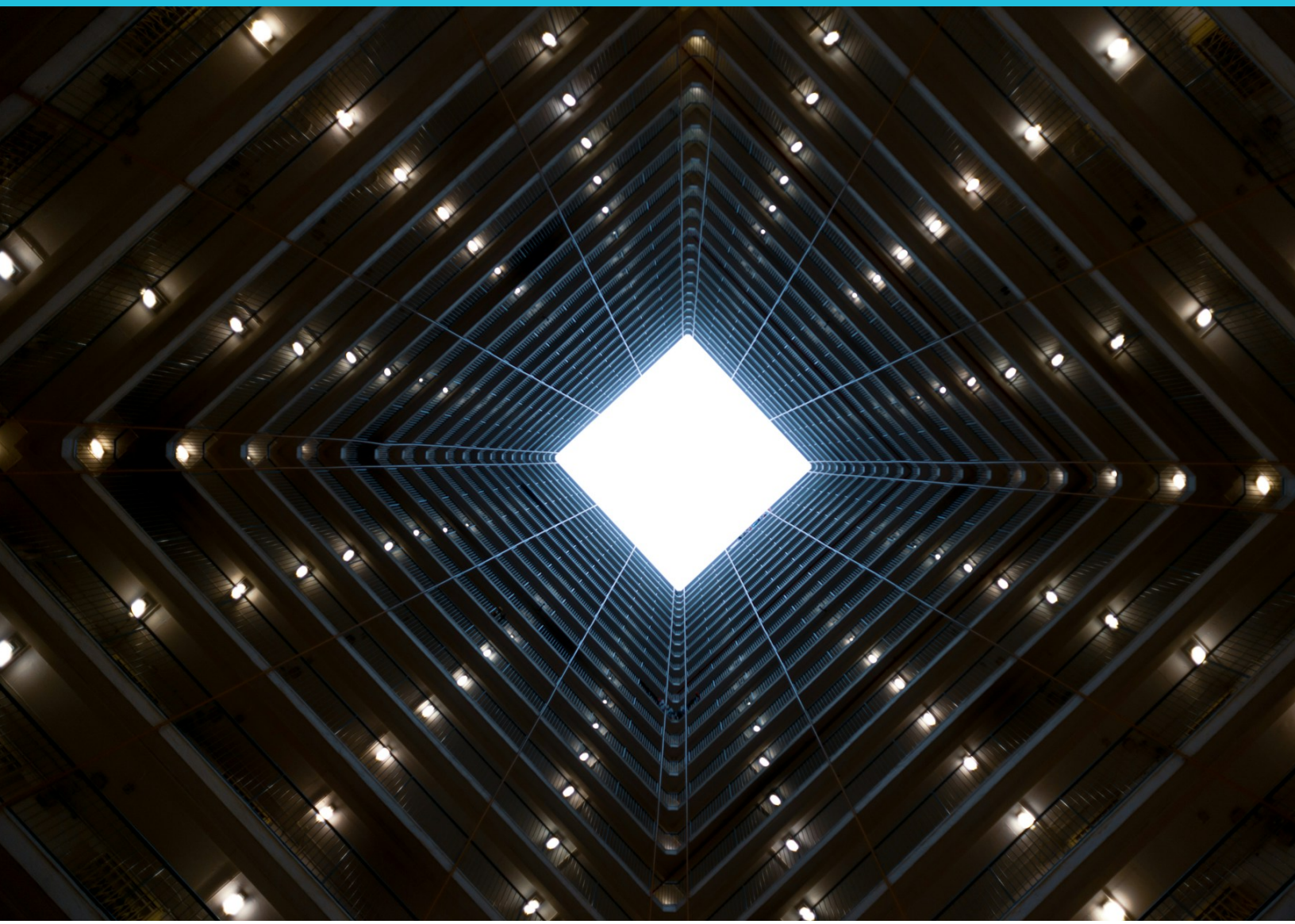
- Increased costs due to project delays and reduced efficiency leading to higher energy production costs.
- Limited innovation hampers development and deployment of new technologies that could improve sustainability and increases efficiencies.
- Adverse economic impact from reduced productivity and competitiveness
- Inability to meet sustainability goals.

Future of energy doesn't exist without software but the energy industry doesn't have in-house talent.

Adam Boucher, CEO, Molecule Systems[1430]

[1430] Research interview with Adam Boucher, April 4, 2022.

© Strategy of Things, 2025. All rights reserved.



Appendix: IoT Evolution

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

© Strategy of Things, 2025. All rights reserved.

22. Appendix: IoT evolution

This appendix proposes a possible IoT evolution model as well as examining the drivers and associated enabling technologies.

22.1. Four stages of IoT evolution

This section proposes four stages of IoT evolution. At each stage, IoT provides users and organizations with new capabilities and tools to deliver economic, social and strategic value. This value grows at each stage as organizations build on the capabilities and value developed in prior stages.

The remainder of this section discusses each of the stages shown below in Figure 22-1 in detail.

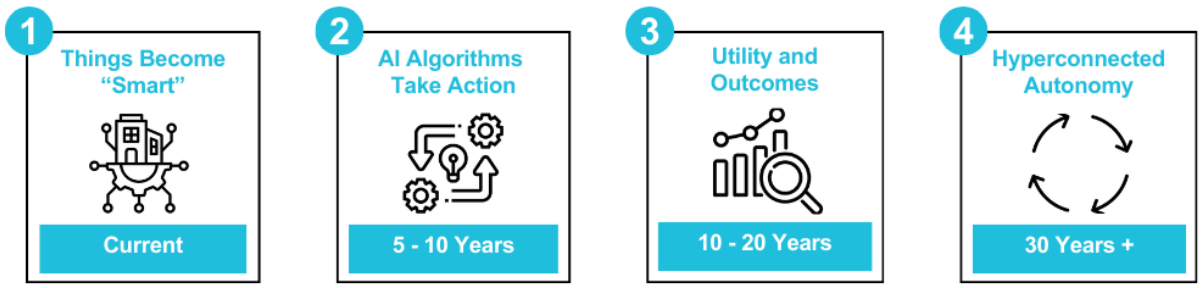


Figure 22-1: The IoT Journey: Operational Efficiency to Full Autonomy

22.1.1. Stage 1: "Things" become smart

The addition of sensors, actuators and embedded systems to devices and machinery allows both the device and the surrounding environment to be monitored, managed and controlled in ways not previously possible.

Facilitating the growth of "smart things" are:

- Connectivity technologies designed for low bandwidth applications.[1431]
- Standards and protocols allowing different devices from different suppliers to communicate with each other.
- Cloud technologies and business models.
- Low-cost embedded computing systems.

Examples of "smart things" include our "smart phones", "smart thermostats" for homes and buildings, "smart watches", soil moisture sensors for agriculture, asset tracking sensors for inventory and vibration sensors on manufacturing equipment. The "smart" enablement of devices

[1431] Not all IoT applications are low bandwidth. However, the introduction of connectivity technologies designed for low bandwidth applications created new market opportunities.

© Strategy of Things, 2025. All rights reserved.

creates new economic opportunities for existing product manufacturers as well as for new entrants in the marketplace.

IoT devices collect and use data to create new capabilities, value and outcomes. AI and machine learning algorithms act on the collected data to create new insights, enhance execution and optimize outcomes.

The recognition of the value of the data has led to the growth of a data economy. This economy is based on marketplaces offering a range of data products, development of advanced analytics and powerful AI algorithms, commercially available analytics tools and applications and an increasing pool of data scientists.

22.1.2. Stage 2: AI algorithms take action

AI is increasingly used to analyze large volumes of data to identify patterns, spot anomalies and propose insights. Initial applications of AI augment human and manual activities. As the amount of collected data and data quality increases, along with rapid improvements in AI algorithms and hardware processing power, confidence in the outcomes produced from AI grows. The use of AIs shifts from descriptive ("what happened?") and predictive ("what could happen?") activities to prescriptive ("what should be done?") and responsive ("act on it") activities.

The emergence of edge computing servers and AI capable processors on IoT devices will enable real-time processing. When integrated with sensors and actuators, systems employing prescriptive AI algorithms will be able to act autonomously in response to real time events. Some examples of an automated AI-IoT system currently in use are autonomous vehicles, robot vacuum cleaners and warehouse "pick and pack" robots.

22.1.3. Stage 3: Utilities and outcomes

As devices add sensors and actuators, the ability to monitor, measure and control previously unavailable parameters creates consumption or outcome based "IoT as a Service" products. For example, location sensors installed on cars allow users to car-share and pay by the mile. Heating, Ventilation and Air Conditioning (HVAC) systems equipped with high fidelity sensors and controllers will allow building owners to pay for the quality of the thermal comfort provided, instead of purchasing a heating and cooling system.

Smart factories could offer "production as a service" by making their excess manufacturing capacities and capabilities available and discoverable to third parties. For a product to become a utility and be economically and technically viable, the results produced by actions from IoT must be predictable, stable, reliable and consistent. AI algorithms play an important role in optimizing and enabling these outcomes. The transition to a utility-based economy from a product-based economy will likely bring significant disruptions and yield significant benefits.

22.1.4. Stage 4: Hyperconnected autonomy

As industries become integrated, automated and internally connected, they could begin to integrate externally with other industries. For example, the manufacturing ecosystem would begin to integrate with the transportation and logistics industry, as well as with the retail industry.

© Strategy of Things, 2025. All rights reserved.

As these processes begin to integrate and interoperate, so do industry IoT systems. For example, IoT sensors in a retail store detect inventory levels and pass that information to distributors and wholesalers. That information is processed by inventory forecasting systems. As autonomous AI algorithms merge with the utility economy, industries become increasingly autonomous, from raw material sourcing to manufacturing to demand fulfillment.

The automation of businesses that support multiple industries, such as transportation and logistics, links not only automation between value chains, but also accelerates automation across multiple industries. Supporting the operation and maintenance of the autonomous economy will require convergence of digital and physical infrastructure, skillsets and resources.

22.2. IoT evolution drivers and enablers

Industry analysts estimate that the number of connected IoT devices will grow from 11.3 billion in 2020 to 27 billion by 2025.[1432] As the physical environment is equipped with additional sensors, the way those sensors and devices are used will evolve. Many of the IoT devices currently deployed operate in isolation or "islands." Driven by cross industry standards, use cases and middleware, these systems of connected devices integrate with other systems to form broader and bigger "systems of IoT systems."

Several interdependent factors will play influential roles in driving the evolution of IoT. The relationships between these factors are shown below in Figure 22-2.

[1432] "State of IoT 2022: Number of Connected IoT Devices Growing 18% to 14.4 Billion Globally", M. Hasan, May 18, 2022. Link

© Strategy of Things, 2025. All rights reserved.

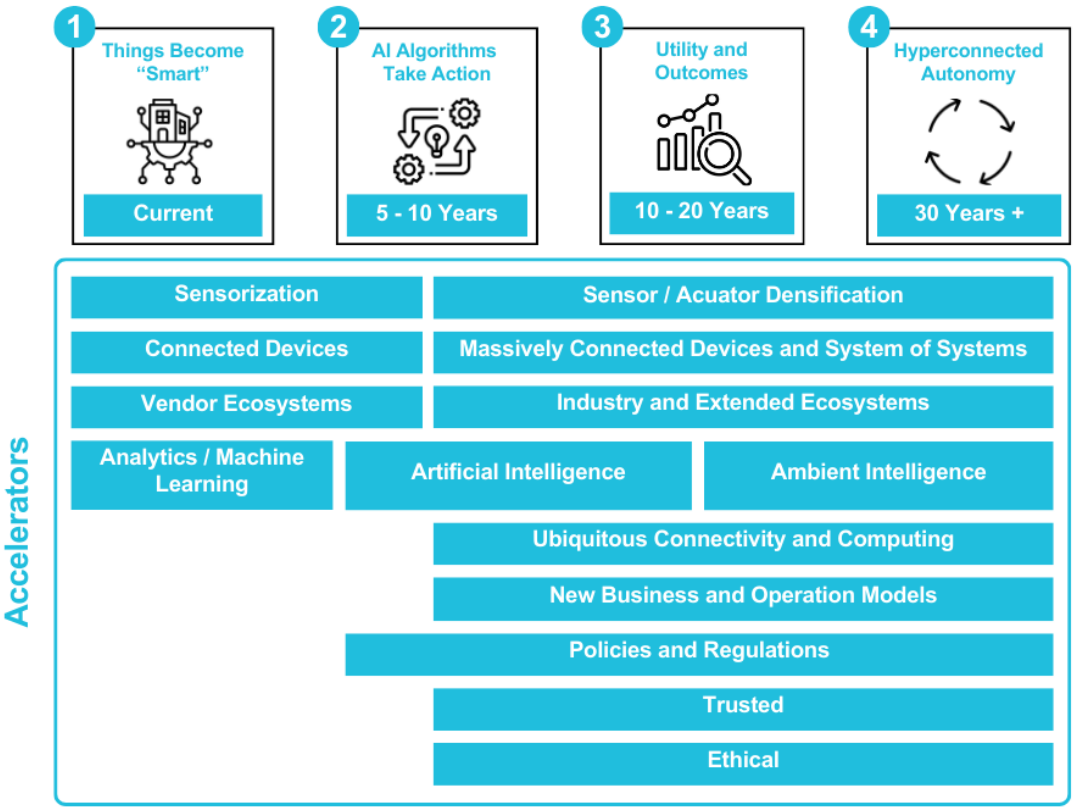


Figure 22-2: IoT Accelerators

The main factors that drive and enable IoT evolution are:

- Interoperability and standards.
- Ubiquitous computing.
- Trustworthy IoT.
- Convergence of IT, OT and enterprise systems.
- Policies and regulation.
- Innovative businesses and operating models.

Each of these is discussed below.

22.2.1. Interoperability and standards

Interoperability allows heterogeneous devices and systems to integrate, communicate and share information with each other. For example, information collected from one IoT device is used as input data by another device or devices from different brands may communicate and work together in a system.

While interoperability is enabled by standards, it is difficult to achieve for a variety of reasons. In some areas, IoT technology is still new and rapidly evolving. There are many areas of IoT

© Strategy of Things, 2025. All rights reserved.

technology to be standardized and attaining agreement on a standard takes time. While open standards provide the potential for seamless interoperability, the current market is filled with products with proprietary protocols, "walled gardens"[1433] device ecosystems and differing international standards and protocols. Some vendors believe their proprietary protocols are technically superior, some were first to market before standards developed, while others are concerned with commoditization of their offerings. For IoT to evolve, interoperability and open standards across devices and industries and countries are critical.

22.2.2. Ubiquitous connectivity

The availability of connectivity service coverage supports IoT adoption. While urban areas have the infrastructure to offer different connectivity service options, rural areas and remote regions do not. Limited infrastructure, low population and population densities, terrain challenges and poor economic returns limit connectivity investments in these areas. Several government and private sector initiatives offer the potential to make connectivity ubiquitous. For example:

- A portion of the $65 billion in the federal Bipartisan Infrastructure Law will build infrastructure in underserved areas.[1434]
- California is building a $6 billion middle mile fiber network to facilitate the creation of last mile services to underserved areas.[1435] Middle mile networks connect the last mile with the broader Internet.
- The FCC is considering the use of the frequencies in the TV white space for connecting IoT devices over wide expanses of rural areas.[1436]
- Several satellite operators are planning the launch of next generation Low Earth Orbit (LEO) broadband and IoT connectivity services to rural and underserved areas.[1437]

These initiatives are supplemented by private enterprises establishing LTE and 5G private networks to connect campuses, factories and other facilities and augment commercial telecommunications services.

22.2.3. Ubiquitous computing

Analyzing data from IoT sensors and devices yields insights that optimize operations, boost efficiencies and create new value. While some of the data processing and analysis is performed in cloud data centers, other data are better suited to be processed at or near the point of use. This includes data from low latency applications and those in areas with unreliable connectivity. The development of AI capable microprocessors and microcontrollers, along with the emergence of

---

[1433] A "walled garden" ecosystem is one in which a vendor or a group of vendors together form an ecosystem where their products are compatible with each other.

[1434] "Fact Sheet: The Bipartisan Infrastructure Deal", White House Statement and Releases, November 6, 2021. Link

[1435] State of California Middle-Mile Broadband Initiative. Link

[1436] "FCC Expands TV White Space Use for Wireless Operations," M. Balderston, TV Tech, October 27, 2020. Link

[1437] "Satellite IoT Connectivity: Three Key Developments to Drive the Market Size Beyond $1 Billion", E. Pasqua, IoT Analytics, August 25, 2022. Link

© Strategy of Things, 2025. All rights reserved.

efficient analytics (tinyML) algorithms optimized to run on resource constrained devices allow some data processing for certain types of applications to be processed on the device.

Telecommunications companies and other companies are building out mobile edge computing capabilities in cities. For example, one of the major telecommunications companies is building out a network of mobile edge computing centers across the country to support low latency, AI based applications. One U.S. startup company proposed placing servers in traffic cabinets in cities to support a variety of smart city applications. As IoT evolves, its myriad applications require the placement of computing infrastructure to support data processing to be located where it makes the most sense, whether that is in the cloud, at edge servers or on the device.

22.2.4. Trustworthy IoT

IoT raises several cybersecurity and data privacy concerns. Cybersecurity is a priority for developers, adopters and privacy advocates. IoT devices expose new attack surfaces that can be exploited by criminals to enter the network, steal information and disrupt operations. Such data collected from IoT devices can be stolen, improperly accessed or used for purposes outside its initial design. In addition, algorithms can be biased to produce incorrect or unintended outcomes.

While interoperability, connectivity and processing provide the technical infrastructure for IoT to scale, a trust infrastructure is necessary for IoT market adoption to scale. An example of a trust infrastructure is illustrated by the Strategy of Things' article on a trust model for a smart city.[1438] In this model, data privacy and cybersecurity are only two of the elements that make up trust. The other elements include people and organizations, change and transformation management, governance, processes, algorithms, technology, user experience and strategic vision.

The article cites the air transportation industry as an example of a "trust" ecosystem "that ensures that flying is safe and reliable. A combination of rigorous engineering, regulations, policy, operational processes, stringent oversight and maintenance have made air transport safe. An ecosystem of partners, from government agencies, aircraft and component manufacturers, airlines, engineers and others worked together to ensure these outcomes."[1439] For IoT to evolve and market adoption to scale, the focus on data privacy and cybersecurity must expand to build IoT trustworthiness.

22.2.5. Analytics and intelligence

Data collected from IoT devices are analyzed to create insights and drive positive outcomes. Some of these data are used to train Machine Learning (ML) and artificial intelligence algorithms to create those outcomes. As more sensors and devices are deployed, the quality of the data collected and used to train the algorithms improves, leading to more refined models, the extension of those models to more use cases and more accurate model outcomes. Continuing advances in algorithm development create new models that service more complex and computationally intensive applications, as well as enable more efficient processing on existing resource constrained microprocessors.

[1438] "Smart City Trust – Think Beyond Cybersecurity and Privacy", B. Chan, Strategy of Things blog, March 13, 2019. Link

[1439] ibid.

© Strategy of Things, 2025. All rights reserved.

As connectivity and processing infrastructure expand, IoT will scale with new use cases that are ML/AI enabled. Continuing advances in interoperability and development of low-cost devices will eventually lead to an environment with ubiquitous intelligence. This state, called ambient intelligence, is reached when intelligence is embedded and integrated transparently into the physical environment.

This leads to a positive feedback cycle where developments in low-cost devices lead to more IoT devices, which increases the need for more connectivity service and coverage. As the number of devices scales, the amount of data collected grows. The need to process these data drives advances in computing infrastructure and algorithms to produce improved outcomes. These better outcomes increase the need for more devices to be integrated into the physical environment and the day-to-day interactions with people.

22.2.6. Convergence of IT, OT and enterprise systems

The Internet of Things is not a standalone technology. For IoT to scale into the economy and daily use, there must be a convergence of IT, Operational Technology (OT), IoT and the cloud. While many uses of IoT today are in standalone applications or silos, for IoT value to be maximized, these different solutions across the spectrum must integrate and exchange information and data seamlessly.

There are millions of legacy and OT systems in use today, from manufacturing machinery to Programmable Logic Controllers (PLCs) and SCADA (Supervisory Control and Data Acquisition) systems. While some of these legacy and OT systems may offer data collection and control capabilities, they were not designed to connect to and communicate across the Internet.

It is neither feasible nor practical to replace all these legacy and OT systems with new connected "smart systems". Some of the legacy systems must be retrofitted with IoT technologies to enable them to connect, communicate and be interoperable with existing systems and modern smart systems. An ecosystem of solutions providers who build "bridging" solutions is required. In addition, as IoT evolves, the ability of users to maintain and sustain these legacy systems is critical. This integration is a journey that will occur over years, with progress mirroring advances in IoT capabilities.

22.2.7. Policies and regulations

These technological advances create new opportunities and challenges. For example:

- The integration of IoT into a manufacturing operation results in increased efficiencies which may reduce the size of the labor force and simultaneously require new skills.
- Facial recognition algorithms running on a city's network of video cameras help to deter and solve crimes but may lead to privacy violations when used outside of intended purposes or when inaccurate results are provided which may lead to false accusations, improper actions and other negative outcomes.
- Autonomous vehicles offer the potential of significant enhancements to traffic safety but may also incur significant and complex liabilities if an accident occurs.

© Strategy of Things, 2025. All rights reserved.

From a historical perspective, technical advances often create both intended and unintended outcomes. Government policies and regulations help inform, facilitate and reduce the impact of unintended consequences while retaining the benefits of the intended consequences.

While mature technologies are well suited for existing policies and regulations, new and emerging technologies often outpace the effectiveness of in place policies and result in unintended consequences.

For example, in San Francisco, the city enacted legislation that banned the use of facial recognition technology for cameras on city infrastructure and premises.[1440] This legislation, however, does not apply to merchants in a shopping district with cameras mounted on privately owned facilities.[1441] Currently, San Francisco is running a 15 month pilot that will allow law enforcement to view footage from video from private cameras.[1442]

In addition, policies and regulations can be enacted by various government jurisdictions, such as cities, states, federal and international institutions. These well intended policies may conflict with one another, resulting in barriers to adoption, use, compliance and the value realized from IoT.

22.2.8. Innovative businesses and operating models

The application of IoT creates opportunities to extend and create new operating models and innovative businesses. Having the requisite technology infrastructure in place enables the creation of innovative business models and leads to market adoption of new business offerings.

For example, cellular connectivity and GPS-enabled tracking devices combined to enable ridesharing services. The success of the ridesharing businesses extended to the creation and adoption of shared micro-mobility services such as bike and scooter sharing. Besides transporting people, new businesses leveraged the existing infrastructure to deliver other goods such as meals and consumer products.

In areas without the technology infrastructure, however, these services are not offered. For example, ridesharing services are not offered in areas with limited or no cellular connectivity. The availability of such supportive infrastructure enables businesses to create innovative applications for IoT, which then drives new businesses and economic models. In a positive feedback loop, the success of these businesses drives the evolution of IoT, which then leads to new businesses developments and emerging opportunities.

22.3. Emerging IoT trends

As IoT adoption grows, IoT technology continues to mature. The research identified ten current broad technology trends that are significant to the evolution and development of IoT. While

---

[1440] “San Francisco Bans Police, Municipal Use of Facial Recognition Technology”, M. O’Brien and J. Har, KQED, May 14, 2019. Link

[1441] “San Francisco's Facial Recognition Ban Still Lets Corporations Spy on You”, N. Karlis, May 21, 2019. Salon. Link

[1442] “Despite Privacy Concerns, San Francisco Supervisors Expand Police Access to Live Camera Feeds”, J. Har, KQED, September 21, 2022. Link

© Strategy of Things, 2025. All rights reserved.

these trends lead to the advancement of IoT, they also create new challenges and gaps to be addressed. These trends are:

1. Emergence of the edge.
2. Development of "low code" and "no code" software tools.
3. Increased open-source IoT ecosystem of users and developers.
4. Developing cybersecurity standards and regulations for IoT.
5. Next generation satellite IoT connectivity services.
6. Rollout of 5G will accelerate and enable IoT.
7. AI and machine learning capable IoT devices.
8. Energy harvesting technologies deployed.
9. Multi-sensor data fusion becomes commonplace.
10. Adoption of digital twin models.

Each of these is discussed below.

22.3.1. Emergence of the edge

In a traditional IoT architecture, shown previously in Figure 11-1, data are routed from the device to a remote cloud data center for processing and storage. Not all data collected, however, needs to be or should be sent to the cloud for processing.

> For example, sending data collected from sensors on autonomous vehicles to the cloud creates additional latency and processing must be done on the vehicle for the car to properly respond to sensor readings. In mission critical applications or in those where connectivity is intermittent or unreliable, processing is performed at the gateway or the device itself. Extracted from Section 17.3.1

In other cases, not all data need to be stored. Some data can be acted upon on the device and never sent to the cloud. In other cases, only a subset of the data collected is transmitted. For example, data that records an event is saved for further analysis and processing, while data collected that shows no change, or are not significant, are not saved.

A 2022 survey of 910 IoT developers, conducted by the Eclipse IoT Foundation, found that the top computing workloads performed at the edge were artificial intelligence (38% of respondents), control logic (34%), data exchange across multiple nodes (22%) and data analytics (20%).[1443]

Edge processing can occur in various locations. For example, solutions providers are deploying servers and storage in local data centers to process IoT data. In some cases, IoT devices are employing more capable microprocessors and microcontrollers to process the data directly as it

[1443] "IoT and Edge Developer Survey Report", Eclipse Foundation survey, September 2022, Page. 12. Link.

© Strategy of Things, 2025. All rights reserved.

comes in from the sensors. And finally, other cases require data from deployed IoT devices be routed to a local gateway, where it is aggregated and processed.

22.3.2. Development of "low code" and "no code" software tools

These tools democratize IoT application development. Many IoT users turn to outside resources to integrate, develop and update applications for devices in their network because they lack the skills and capabilities to do so on their own. This challenge slows the widespread IoT adoption, utilization and value creation across the U.S. economy.

In response, software tools which simplify coding for IoT adopters are emerging in the marketplace.[1444] These third-party tools, integrated into popular IoT platforms, allow users with limited coding skills to create or update IoT applications. "No code" tools provide users with a graphical interface to "drag and drop" predefined "functions" in a logical sequence to create an application. "Low code" tools require limited skills, but instead of coding, the user is writing "scripts" to perform certain routine and non-routine actions, similar to recording macros in Microsoft Excel.

This "democratization" of integration and application development allows business users and consumers to create their own applications as needed without relying on a specialized IT department. Today, these tools are still limited in what they can do and will evolve to address technical shortcomings, industry specific functions and best practices.

22.3.3. Increased open-source IoT ecosystem of users and developers

The use of open-source software is accelerating among business enterprises globally. Open-source software is "designed to be publicly accessible—anyone can see, modify and distribute the code as they see fit" and developed in a "decentralized and collaborative way, relying on peer review and community production." [1445] This approach leads to lower development and ownership costs, continuous innovation, improved code functionality, performance and resilience and mitigation of vendor lock-in concerns associated with proprietary software but has implications for long-term maintenance and cybersecurity updates.

A 2022 study of 1296 global enterprise IT leaders across several industries revealed that the percentage of enterprise and community based open-source software in the organization will grow from 50% today to 58% in two years. Respondents in the United States. reported their percentage of open source software will grow from 53% today to 59% in two years.[1446] The same report found that 73% of U.S. enterprise IT leaders are currently using edge computing and IoT and that 80% of them are planning to increase the use of open source software for these technologies in the next two years.[1447] The principal benefits of using open source software

---

[1444] "Using Low-Code and No-Code in IoT App Development", L. Rosencrance, IoT World Today, May 17, 2021. Link

[1445] "What is Open Source?", Red Hat, October 2019. Link

[1446] "The State of Enterprise Open Source: A Red Hat report", P. Cormier, Red Hat report, February 22, 2022. Link

[1447] See note 1446

© Strategy of Things, 2025. All rights reserved.

included better security (32% of respondents), better quality (32%), ability to safely leverage open source technology (28%) and ability to work in cloud/cloud native[1448] (26%).

There is a growing number of development initiatives and projects in the IoT community. One active community is Eclipse IoT, an open-source community within the Eclipse Foundation, a European based international non-profit association that provides the global community of individuals and organizations with a scalable environment for open-source software collaboration and innovation.

The Eclipse IoT community has 50 current open source IoT projects and has generated 8.2 million lines of code in development by 170+ committed developers and organizations.[1449] One of the Eclipse IoT community members is a major global industrial technology company that integrates open-source development as part of its product development strategy. The company relies on open source developed code for some parts of its commercial IoT software. This allows them to "outsource" the development of select IoT stack components to the community and reallocate internal resources to develop more strategic proprietary code for their commercial IoT software.[1450]

In addition to open-source software components, there are several open source IoT platforms and frameworks available to developers and users. Thingsboard, Kaa and MainFlux are three examples of open-source platforms that users can deploy to connect, manage and operate IoT devices. FiWare and IoTivity are two examples of IoT open-source frameworks, which provide a basic reference structure that can be adapted to build an IoT platform for a specific application or industry domain. FiWare is built around its context broker (software that enables the integration of gathered IoT data) and is a "curated framework of open-source software platform components which can be assembled together and with other third-party components to build platforms".[1451]

IoTivity is another example of an open source IoT framework built around the Open Connectivity Foundation's standards for connectivity and security. Many of these open source IoT platforms have been developed with significant sponsorship. For example, FiWare was developed as an initiative from the Future Internet Public Private Partnership (FI-PPP), a European Union innovation program.[1452] The IoTivity framework is sponsored by the Open Connectivity Foundation and its member companies, who develop specifications, interoperability guidelines and a certification program for IoT devices.[1453]

To facilitate adoption of open source IoT, some platforms are offered in an optional commercially supported version (e.g., Thingsboard Professional edition) while other platforms have community members who offer professional technical support services. There are examples of adoption and market success with open source IoT platforms. FiWare has over a thousand

---

[1448] Cloud native refers to the approach of building applications on cloud-based services and delivery models.

[1449] Link

[1450] Interview notes. Eclipse IoT personnel, Frederic Desbiens, May 7, 2020

[1451] "FIWARE Catalogue", FIWARE. Link

[1452] "FIWARE – a European Success Story", European Commission, Shaping Europe's Digital Future, March 2018. Link

[1453] "IOTIVITY", Open Connectivity Foundation. Link

© Strategy of Things, 2025. All rights reserved.

businesses and members, developing market ready products and applications from its framework. The businesses using FiWare were expected to generate revenue of more than 330 million euros in 2020 from serving at least 1.5 million business customers and reaching a market of more than 20 million consumers.[1454]

22.3.4. Developing cybersecurity standards and regulations for IoT

Cybersecurity is one of IoT's major concerns. Several high-profile events justify these concerns, including:

- In 2016, the Mirai IoT botnet, in one of the highest profile incidents, infected over 600,000 devices with a Distributed Denial of Service (DDOS) attack on a few services including the Dyn Domain Name Service and the French web service OVH.[1455] Since its initial release, variants of the original Mirai botnet continue to infect IoT devices today.[1456]
- In March 2021, hackers gained access to 150,000 security cameras from Verkanda, a Silicon Valley startup that provides cloud-based security camera services to factories, schools, gyms, police stations and other corporate customers.
- In December 2020, cybersecurity researchers announced the discovery of 33 vulnerabilities found in open-source TCP/IP communication stacks used by millions of devices from over 150 product vendors. Hackers can use these vulnerabilities to take full control of affected devices, penetrate the broader IT network and to maintain continued access to the network.[1457]

Industry has responded to these challenges through education, standards and certification programs. Representative examples include:

- The Industry IoT Consortium has developed the Industrial Internet Security Framework, a common security framework and an approach to assess cybersecurity in Industrial Internet of Things systems.[1458]
- The International Society of Automation (ISA) has developed a series of standards (ISA/IEC 62443) that addresses current and future security vulnerabilities in industrial automation and control systems (IACSs).[1459]

[1454] See note 1452.

[1455] "Inside the Infamous Mirai IoT Botnet: A retrospective analysis", E. Bursztein, Dec 14, 2017. Link

[1456] "Why Mirai is Still A Threat to the IoT Ecosystem", Intel471 blog, January 25, 2022. Link

[1457] "AMNESIA:33 Vulnerabilities in TCP/IP Stacks Expose Millions of Devices to Attacks", I. Arghire, December 9, 2020, Security Week. Link

[1458] "Industrial Internet Security Framework ", Industry IoT Consortium. Link

[1459] ":An Industry IoT Foundational Publication", Industry IoT Consortium, Industrial Internet Security Framework, K. Caindec et al. Link

© Strategy of Things, 2025. All rights reserved.

- The IoT Security Foundation has developed the IoT Security Assurance Framework to help IoT vendors provide fit-for-purpose security in their products and services.[1460]
- The CTIA had developed a cybersecurity certification program for IoT devices that establishes an industry baseline for device security on wireless networks. It certifies IoT devices at three levels - consumer-grade devices (level 1), business and enterprise managed devices (level 2) and infrastructure-managed devices (level 3).[1461]
- The Open Connectivity Foundation has developed a common security framework and certification testing that enables reliable interoperability among devices from different manufacturers.[1462]

In parallel with industry efforts to address cybersecurity concerns, governments have acted. Examples of these efforts include:

- Some states have enacted cybersecurity legislation, including California (SB-327: Information privacy: connected devices)[1463] and Oregon (HB 2395)[1464] for IoT devices to incorporate unique passwords and other reasonable security measures. Other states, including Illinois, Kentucky, Massachusetts, Maryland, New York, Rhode Island, Vermont and Virginia have considered similar legislation.[1465]
- Federal legislation such as the IoT Cybersecurity Improvement Act of 2020 (H.R. 1668),[1466] which directs NIST to develop, publish and update standards and guidelines on the appropriate use and management of IoT devices owned and used by the federal government. It also directs the OMB to review agency information security policies to ensure that they are consistent with the NIST standards and guidelines and to oversee the implementation of those policies. The legislation prohibits federal agencies from procuring and using IoT devices that do not comply with these standards and guidelines.
- The NIST Cybersecurity for IoT program[1467] "supports the development and application of standards, guidelines and related tools to improve the cybersecurity of connected devices, products and the environments in which they are deployed" in collaboration with stakeholders across government, industry, international bodies, academia and consumers." Select activities include guidance for manufacturers creating IoT devices (NISTIR 8259), recommendations for cybersecurity in consumer IoT products (NISTIR 8425) and guidance for federal agencies looking to deploy IoT (SP800-213).

[1460] "The Home of IoT Security Best Practice and Next Practice", IoT Security Foundation. Link

[1461] "Internet of Things (IoT) Cybersecurity Certification", CTIA Certification. Link

[1462] "An IoT Ecosystem Foundation to Build On", Open Connectivity Foundation. Link

[1463] California SB-327. Link

[1464] Oregon HB 2395. Link

[1465] "State Lawmakers Go After IoT Security Risks", J. Richter, K. Milne, V. Hiner, Government Technology. November 2019. Link

[1466] "H.R.1668 - IoT Cybersecurity Improvement Act of 2020." Link

[1467] NIST Cybersecurity for IoT Program. Link

© Strategy of Things, 2025. All rights reserved.

- The FCC has approved the launch of the U.S. Cyber Trust Mark, a voluntary label on consumer IoT devices that "confirms for consumers that a product meets cybersecurity standards developed by the National Institute of Standards and Technology."[1468]
- The European Union announced the Cyber Resilience Act that will impose mandatory cybersecurity requirements for products with digital elements throughout their whole lifecycle.[1469]
- The European Telecommunications Standard Institute (ETSI) has released the EN 303 645 standard for internet connected consumer products in June 2020.[1470]

22.3.5. Next generation satellite IoT connectivity services

Coverage is one of the most significant barriers to IoT adoption and operation. Many rural areas lack broadband service and cellular coverage. There are vast areas of the earth, such as oceans, forests, deserts and other areas that are remote, barren and unconnected. Despite this, these areas offer many opportunities for IoT. For example, rural areas are home to farms and grasslands for ranching. Electrical grid infrastructure and oil pipelines traverse long stretches of remote and forested areas. Mining operations occur in remote and barren areas. Oil rigs operate in remote areas and offshore locations and are as far as 400 kilometers from land.

While the Bipartisan Infrastructure Law provides funding for broadband initiatives, it will only partially address the connectivity gaps in unserved rural and urban areas and not at all in remote areas. Satellite based IoT connectivity services provide coverage to the areas of the country where terrestrial based connectivity options are not economically feasible or physically possible. These services complement terrestrial based connectivity services.

The projected growth of IoT devices and the need to connect those devices no matter where they are, led satellite operators to create space-based services that complement terrestrial services to provide global coverage. Innovative space start-up companies like Space-X and Rocket Labs, have reduced launch costs from $11,600/kg (Delta IV Heavy) in 2004 to $1,500/kg (Space-X Falcon Heavy) in 2018. [1471] At the same time, the miniaturization of electronic components and microprocessors have resulted in smaller, lighter and less expensive satellites and satellite constellations. Satellite operators no longer need to buy a dedicated rocket for themselves but can share a launch vehicle with other commercial payloads.

Since 2018, 13 startups and 7 incumbent satellite operators have announced plans to offer satellite IoT services. These privately owned and operated services come in two types – device to satellite connectivity and satellite backhaul (IoT gateway to satellite). Globally, there are around

[1468] "FCC approves cybersecurity label for consumer devices," C. Vasquez, CyberScoop, March 14, 2024. Link

[1469] "EU Wants Cyber Resilience Act to Set the Global Standard for Product Cybersecurity", S. Waterfield, TechMonitor, September 15, 2022. Link

[1470] ETSI EN 303 645 Cybersecurity for Consumer IoT: what is it and why it's important", TUV. Link

[1471] "Space Launch to Low Earth Orbit: How Much Does It Cost?", T. Roberts, Aerospace Security, September 1, 2022. Link

© Strategy of Things, 2025. All rights reserved.

5 million satellite IoT subscribers.[1472] The number of satellite IoT devices is expected to reach 30.3 million by 2025.[1473] Market revenues for connectivity services are expected to grow at CAGR of 14% from 2021 to 2026, reaching 1 billion USD by 2026.[1474] Global revenues for satellite IoT device and connectivity services are expected to reach $5.9 billion USD by 2025.[1475]

Key use cases of satellite IoT include wide area monitoring (farms, electrical grid infrastructure, oil pipelines), equipment monitoring of machinery in remote areas, real time tracking of inventory in cargo ships and monitoring and operation of assets after a natural disaster where the existing infrastructure has been destroyed.

One of the major developments in satellite IoT is the emergence of connectivity service delivered by Low Earth Orbit (LEO) satellites. Operating at an altitude of 200 km, LEO satellites services offer lower latency than services provided by Geosynchronous Earth Orbit (GEO) satellites operating at 35,785 km. In addition, because of the shorter distances, wireless transmissions from and to LEO satellites suffer lower signal propagation losses. This allows low power and power constrained IoT devices and gateways to utilize satellite IoT connectivity services. Satellite based 5G service is a possibility in the future with Release 17 of the 5G standard.[1476] For these reasons, there are 31 satellite operators planning or already operating in low earth orbit, as compared to 9 GEO operators and 4 LEO+GEO operators.[1477]

22.3.6. Rollout of 5G will accelerate and enable IoT

The fifth generation of cellular technology, also known as 5G, is in various stages of rollout across the United States. Compared to fourth generation technology (4G LTE, 4.5G), the performance improvements and capabilities offered by 5G are significant.[1478] For example, 5G offers these improvements:

- Up to 100 times faster with a theoretical peak data rate of 10 Gbps.
- Low latency (1 millisecond). [1479]
- High bandwidth capacity, around 1000 times more.
- Connects a minimum of 1 million devices in a square kilometer.[1480]
- Supports high availability of 99.999%.

[1472] "Satellite IoT Connectivity: Three Key Developments to Drive the Market Size Beyond $1 Billion", E. Pasqua, IoT Analytics, August 25, 2022. Link

[1473] "Satellite IoT: A Game Changer for the Industry?", H. Urlings, Satellite Markets and Research, September 3, 2019. Link

[1474] See note 1472.

[1475] See note 1473.

[1476] "How Satellite Became a Part of 5G", L. Bernstein, Constellations. Link

[1477] See note 1472

[1478] "5G Technology and Networks (Speed, use cases, rollout)", January 5, 2022. Link

[1479] "What is URLLC?", RCR Wireless, January 7, 2019. Link

[1480] "5G and IoT: A Failure to Fly", D. Jones, EETimes, April 27, 2022. Link

© Strategy of Things, 2025. All rights reserved.

- Supports IoT device energy efficiency and low power needs of IoT devices.

One key 5G capability is its ability to support a broad range of use cases, including massive Machine Type Communication (eMTC) low bandwidth IoT applications, enhanced mobile broadband (eMBB) applications and ultra-reliable, low latency communication (URLLC) applications. 5G's ability to slice the network to support these three use case categories, along with its high capacity and availability characteristics, will facilitate the development and deployment of IoT applications.

Today, a variety of different connectivity options are used to support various use cases. For example, battery powered low bandwidth applications use licensed (NB-IoT, Cat M1) and unlicensed (LoRaWAN, SigFox, etc.) LPWAN connectivity options. Low bandwidth IoT applications, with access to continuous power, have the additional option of using cellular 4G. Medium bandwidth applications, such as those involving video, use cellular 4G or WiFi connectivity options.

5G also supports a new category of IoT application that is not possible today. For example, mission critical applications that require high network availability and real time performance. These applications are often seen in industrial automation, intelligent transportation, critical infrastructure operations and remote healthcare. A 2020 white paper by the Next Generation Mobile Networks (NGMN) Alliance, an industry consortium of telecommunications companies, solutions providers and advisors, has identified several prioritized URLLC use cases, including:[1481]

- Augmented Worker. Using Augmented Reality (AR) and Virtual Reality (VR).
- Energy management. Differential protection, fault location identification, fault management in distributed power generation.
- Smart Factories. Industrial robotics, automated guided vehicles (AGV) control, production line robot tooling.
- Unmanned Aerial Vehicles (drones). UTM connectivity, command and control, payload management.
- Positioning services. Precise positioning, cellular positioning, 5G NR positioning.
- Intelligent transport. Autonomous vehicles.

Other URLLC applications include:[1482]

- Healthcare. Remote Diagnosis, Emergency Response, Remote Surgery.
- Transportation. Driver Assistance, Enhanced Safety, Autonomous Driving, Traffic Management.

[1481] "5G E2E Technology to Support Vertical URLLC Requirements", NGMN Alliance White Paper, Feb 10, 2020. Link

[1482] "What is URLLC?", everythingRF. Link

© Strategy of Things, 2025. All rights reserved.

22.3.7. AI and machine learning capable IoT devices

The first generation of IoT devices contained simple microprocessors with limited processing and storage capabilities. These resource constrained devices performed simple tasks and consumed little power. Heavy computational tasks, such as analyzing data streams and running AI/ML algorithms, were offloaded to servers in the edge or to cloud data centers.

Recent industry efforts have led to the development and introduction of more powerful and energy efficient AI capable processors for IoT devices.[1483] These "designed for AI" chips provide the acceleration and algorithm processing capabilities that AI operations require, while doing so in a manner that is more power efficient. The ability to process data on the device itself creates "smarter" IoT devices, yields faster device responses and allows the device to work without network connections.

In addition to hardware enablement, other industry efforts focused on the development of algorithms that operate on resource constrained devices. Tiny Machine Learning, or TinyML, is a subset field of machine learning that incorporates techniques and methods to run and operate algorithms specifically on resource constrained devices such as microcontrollers.[1484] This increases the functionalities and capabilities of IoT applications running on these devices. Some applications of TinyML include running machine learning algorithms for predictive maintenance, video object recognition and "wake word" detection in smart speakers.

22.3.8. Energy harvesting technologies deployed

Power is required for IoT devices to function. Today, devices are powered through electrical line power, solar power and both rechargeable and non-rechargeable batteries. There are, however, limitations to these power sources. Line power is only practical for a small subset of applications. Batteries have a limited lifetime and must be replaced or recharged. In some cases, changing batteries is not possible or practical, especially for IoT devices installed in rural areas or inaccessible locations, such as on a bridge structure or in high IoT device density installations. Solar panels work during the day and must be paired with rechargeable batteries for continuous operation, but these capabilities add significant cost to IoT devices.

Energy harvesting solutions are emerging in the marketplace to partially address these power gaps and to power IoT applications. These technologies harness energy from the ambient environment and convert it to electricity. These energy harvesters include photovoltaic cells (light), piezoelectric transducers (vibration), RF (electromagnetic radio frequency) and thermoelectric generators (heat).[1485] These harvesters currently produce small amounts of electricity and are only usable for select low power consumption applications. This includes powering low power IoT devices, as well as trickle charging batteries to extend their useful life. These energy harvesting solutions will augment rather than replace existing power systems. These systems, however, will allow many new IoT applications and devices to be created that would otherwise not be realizable with existing power systems.

[1483] "Processors Roll for IoT and AI", G. Roos, March 23, 2020, Electronic Products. Link

[1484] "What is Tiny ML and Why Does It Matter?", J. Riberio, December 22, 2020. Link

[1485] "What is Energy Harvesting?", Versa Technology, August 24, 2021. Link

© Strategy of Things, 2025. All rights reserved.

The importance of energy harvesting technologies to support IoT and other applications is significant. Researchers at EnABLES, a project studying the European infrastructure needed to power IoT, estimated that 78 million batteries that power IoT devices will be disposed every day by 2025 if battery life is not extended.[1486] According to a 2021 article in industry publication Tech Briefs, a significant majority of the "trillion sensors that could be deployed within the next several years" will be of the ultra-low power wireless type and are ideal for integration with energy harvesting technologies.[1487]

Multi-sensor data fusion becomes commonplace

Sensor fusion is the collection, joining, synthesizing and analysis of data from multiple and disparate sensors to create better insights for decision-making or acting than can be yielded by each sensor alone. For example, a car has a variety of different sensors, with each collecting information about its surroundings. When the separate data are integrated it provides a more complete context of the surroundings, so that the proper actions can be undertaken by the driver or the autonomous driving algorithms. In the future, the onboard car algorithms may supplement the car's on-board sensors with sensors from nearby cars and the roads to obtain additional context for decision-making and action. As the number and types of deployed sensors grows, the potential number of sensors that can potentially be fused will increase exponentially. An August 2021 Allied Market Research report projects that the global sensor fusion market will grow from $3.55 billion in 2020 to $19.8 billion by 2030, representing a CAGR of 19.7% from 2021 to 2030.[1488]

22.3.9. Adoption of digital twin models

A digital twin is a virtual or digital model of a physical object, a group of objects, or a system. A machine, a factory, a building and even a city can be modeled as a digital twin. It acts and operates like the physical system. What happens in the physical system is mirrored by the digital twin. What is simulated in the digital twin is portrayed by similar responses in the physical system.

The digital twin is enabled by instrumented sensors and IoT, simulation and physics models and analytics algorithms. The sensors and IoT devices feed real time data into the digital twin, where simulation models and analytics algorithms act on it to replicate responses, actions and outcomes. The accuracy and fidelity of the digital twin is enabled by IoT and sensors in key parts of the physical system that measure system response and incorporate that back into the model.

A digital twin allows operators to evaluate new designs in a safe and controlled environment and to see how the physical system may respond. Based on system responses, the physical design is updated and operational actions are undertaken. IoT and sensors on the updated physical system then measure the response and the information is used to update the underlying model and simulation.

[1486] "Up to 78 million batteries will be discarded daily by 2025, researchers warn," European Commission, July 23, 2021. Link.

[1487] "Energy Harvesting Can Enable 1 Trillion Battery-Free Sensors in the IoT," M. Hayes and B. Zahnstecher. Tech Briefs. October 1, 2021. Link.

[1488] "Sensor Fusion Market", S. Wankhede and V. Kumar, August 2021. Link

© Strategy of Things, 2025. All rights reserved.

Digital twins can be used throughout the physical system's life cycle, starting from the design and construction to the commissioning, operations, maintenance and decommissioning of that system. For example, a digital twin facilitates the design of an airport by modeling airport building design and site orientation of materials, energy usage, noise levels in adjacent communities and existing road traffic patterns. It can model the size of the airport and road design and its impact of traffic on the local highways during certain times of the day. During construction, that digital twin is used to help project managers measure progress and optimize use of resources to maintain schedules. The impact of inevitable construction delays is mitigated by modeling different work-around options to understand the impact on schedules, cost and resources. When the airport is open, the digital twin is used to help managers plan, test and optimize operations and resources to support day-to-day and holiday travel periods.

A representative sample of Digital Twin applications include:[1489] [1490] [1491]

- Manufacturing: A digital twin of a manufacturing line is created by using IoT sensors and operational process models. By continuously monitoring the sensors and reviewing the model outputs, operations managers can analyze and tune the performance and output of the manufacturing line. They use the digital twin to identify potential adjustments, simulate new operating scenarios and measure production outcomes, variances and resource requirements.
- Transportation and logistics: Distributers and shippers use digital twins to model package form factors in optimizing truck loading, model routes, vehicle fleets and traffic patterns to optimize schedules, fuel usage and route efficiencies.
- Healthcare: A digital twin of a human body helps doctors provide targeted and effective healthcare to their patients. By collecting patient data, such as blood pressure, oxygen levels, heart rates and feeding these into a digital twin, doctors can model and diagnose different scenarios, to prescribe personalized and effective healthcare treatments.
- Cities: A digital twin of a smart city helps city planners and administrators simulate various scenarios and understand the impact of proposed designs, zoning, policies, legislation, public works projects and programs on the community, traffic patterns, health and safety and economic vitality on a city level scale.

As the physical world is increasingly instrumented with IoT, more systems and operations can be modeled and the use of digital twin models use will grow. Beyond Market Insights, a market research and consultancy firm, projected the digital twin market will grow at a CAGR of 41.5%, from $6.3 billion in 2021, to $143.2 billion by 2030.[1492] Key benefits provided by digital twins include increased efficiencies, lower costs, faster time to action, lowered risks and enhanced

[1489] "7 Digital Twin Applications for Manufacturing", M. Crawford, ASME, March 17, 2021. Link

[1490] "3 Best Use Cases of Digital Twin in Healthcare & Their Benefits", H. Şimşek, AI Multiple, November 10, 2021. Link

[1491] "Smart City Digital Twins Are a New Tool for Scenario Planning", P. Hurtado and A. Gomez, American Planning Association magazine, April 1, 2021. Link

[1492] "Digital Twin Market", Beyond Market Insights report, September 2022. Link

© Strategy of Things, 2025. All rights reserved.

customer experiences. A 2022 Capgemini survey[1493] of over 1000 global organizations with or planning a digital twin reported that the top reasons for adoption of digital twins were:

- Saving costs (79% of respondents)
- Technological advancement (77%)
- Reducing time to market (73%)
- Improving operational efficiency (71%)
- Introducing new business models (67%)

In closing, the federal government is well-suited to address the gaps found. These gaps are too broad, complex and challenging for industry, academia or government to address solely. Each stakeholder plays a vital and complementary role. It is the hope of the authors that the findings from this research will also drive new collaboration models and partnerships between government, industry and academia to advance the research necessary to develop and build out the vision enabled by the Internet of Things.

[1493] "Digital Twins: Adding intelligence to the real world", Capgemini Research Institute, 2022. Link

© Strategy of Things, 2025. All rights reserved.

Appendix: Cross Industry Gap Analysis

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

© Strategy of Things, 2025. All rights reserved.

23. Appendix: Cross industry Gaps Analysis

One of the objectives of this study is to identify technology infrastructure gaps that are hindering the adoption of IoT into the U.S. economy and civil society. Several factors are considered in identifying the gaps, including:

- The Internet of Things is not one technology, but a variety of disparate technologies at various stages of maturity. Gaps may exist for one or more of these technologies.
- Industries adopt IoT at different rates and levels due to a variety of technology and non-technology gaps specific to that segment. Different industries have different gaps.
- IoT is evolving. Each stage of evolution has a different set of gaps.
- A majority of the gaps are unlikely to be addressed fully by private sector investment.

Based on these considerations, these gaps are identified using the process shown in Figure 23-1 and are described below:

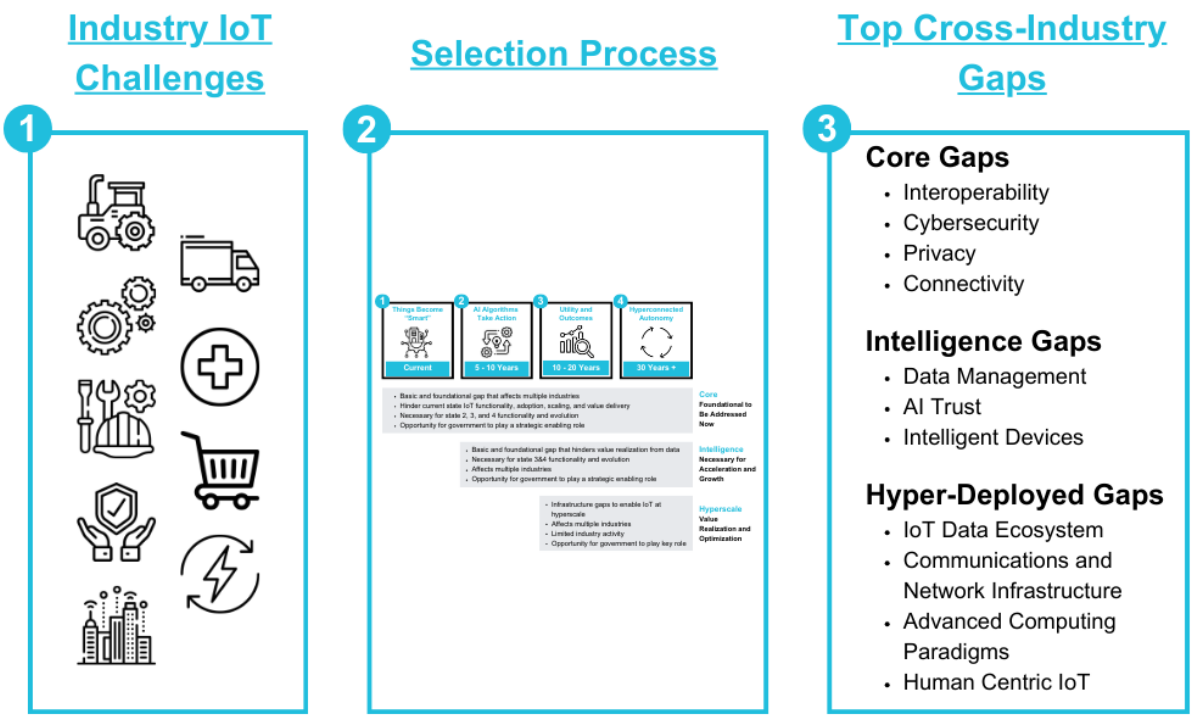


Figure 23-1: Overview of Process Used to Identify Key Gaps

- **Identify industry level IoT technology infrastructure challenges**. For each industry studied, an initial set of IoT technology challenges was identified through secondary research, surveys and interviews. The specific challenges by industry are discussed in detail in Sections 0 to 21.
- **Aggregate and analyze industry challenges**. Individual technology challenges from each industry are reviewed and aggregated into a broader industry challenge. For

© Strategy of Things, 2025. All rights reserved.

example, a number of industries cited specific privacy-related challenges. These specific challenges are aggregated to create a broader privacy challenge. The IoT technology challenges are aggregated and summarized in Section 5.1.

- **Identify the cross industry IoT technology infrastructure gaps**. The cross industry IoT technology infrastructure gaps were identified by mapping them to one of three gap categories. Figure 23-2 shows how these categories are aligned to the IoT stages of evolution and provides a context on prioritization.

The identification of the top cross industry IoT technology infrastructure gaps considers the maturity and evolution of IoT over the next 10 to 30 years by mapping them to one of three categories. These categories are:

- **Core**. The core gaps are gaps in foundational IoT technology infrastructure. Foundational infrastructure and capabilities are essential for the function and operation of IoT. They are needed in all industries and span all four stages of the IoT evolution (Figure 23-2). Examples of foundational capabilities include connectivity and interoperability. The inability to overcome core gaps hinders IoT adoption and operation today and limits the further evolution of IoT. Core IoT technology gaps meet the criteria shown in Figure 23-2.
- **Intelligence**. The Intelligence gaps are gaps in technology infrastructure that support and enable the intelligent and autonomous operation of IoT. They are needed in all industries and span three stages (2, 3 and 4) of the IoT evolution. Examples of intelligent IoT capabilities include data management and edge computing. The inability to overcome intelligence gaps hinders the integration of intelligence into IoT today and limits the further evolution of an intelligent and autonomous future state for IoT.
- **Hyper-Deployed**. The future IoT-enabled economy and society may contain billions of interconnected devices working autonomously in a secure and trusted manner. Hyper-Deployed gaps are gaps in technology infrastructure that if addressed, support and enable the intelligent and autonomous operation of a hyperconnected IoT at scale. They need to be addressed in all industries and span the last two stages (3 and 4) of the IoT evolution. An example of hyper-deployed IoT capabilities include a hyperconnected communications infrastructure and human centric artificial intelligence. The inability to overcome hyper-deployed gaps hinders the emergence of autonomous operation of billions of IoT devices and systems.

© Strategy of Things, 2025. All rights reserved.

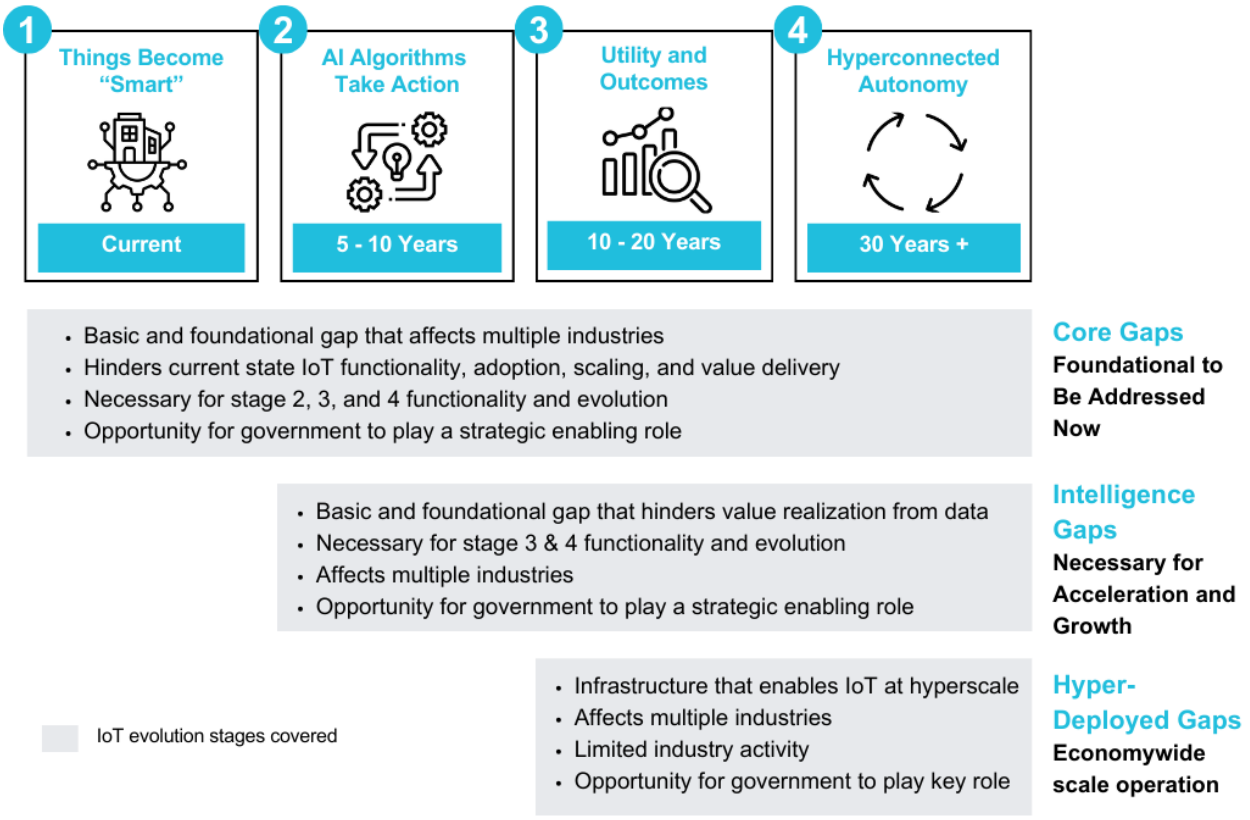


Figure 23-2: IoT Technology Infrastructure Gap Categories and Criteria

Figure 23-3 below shows the cross industry IoT technology infrastructure gaps that were identified for each category.

© Strategy of Things, 2025. All rights reserved.

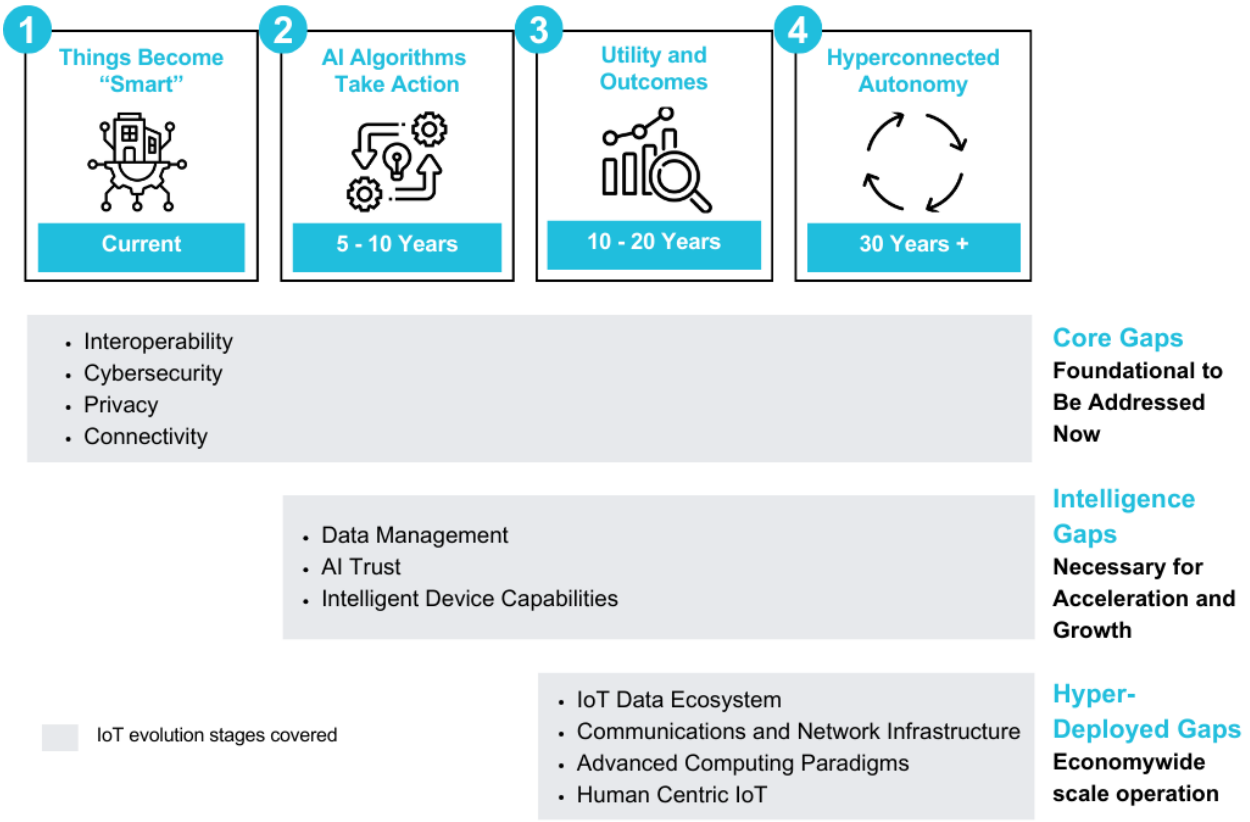


Figure 23-3: Key Gaps by Category

The remainder of this section discusses each of these gaps as they fall in their respective categories.

23.1. Core

The identified gaps in core include:

- Interoperability
- Cybersecurity
- Privacy
- Connectivity

23.1.1. Core: Interoperability

Interoperability was identified as a top challenge in seven of the nine industries studied. These industries include agriculture, manufacturing, construction, cities, transportation and logistics, healthcare and renewable energy.

The lack of interoperability slows the full realization of benefits offered by IoT by preventing IoT devices from connecting, communicating and collaborating with each other and with other

© Strategy of Things, 2025. All rights reserved.

systems. It also hinders IoT's evolution where intelligence and hyperconnectivity combine at scale and bring national economic and society-wide transformational benefits.

The lack of interoperability slows IoT functionality, adoption, scaling, value realization and delivery and evolution in a number of ways described below:

- **Difficult to integrate devices and systems.** Interoperability challenges lead to situations where devices and systems from one vendor may not work with a similar system from a competing vendor due to incompatible communication protocols. Data may be in different formats and have different meanings.

  In some instances, older systems may not work with newer systems from the same vendor. These challenges result in "siloed" data that are trapped within the device or a specific vendor's "walled garden" ecosystem. Integrating devices and systems together to facilitate communication and data exchange is complex and adds additional costs in middleware and to custom integration.
- **Inability to innovate and realize the full benefits of interconnected and automated IoT systems.** Factories have substantial existing investments in legacy and modern industrial OT systems. The inability of IoT technologies to integrate with these systems to share information and services creates operational inefficiencies and increases cost in production lines. Examples are provided below:
  - Cities employ a variety of IoT enabled systems that are independently procured and operated by different municipal agencies. The lack of interoperability prevents these disparate devices and systems from achieving broader and integrated municipal-wide functions that lead to community benefits.
  - In healthcare, interoperability challenges can prevent timely detection and response to patient conditions, leading to errors and misdiagnoses.
  - In transportation and logistics, the inability to exchange data across the supply chain hinders the development and operation of an agile and resilient supply chain. Real-time end-to-end visibility is needed for industry participants to be responsive to supply chain disruptions and able to plan and optimize corrective actions.
- **Unable to realize cost savings and revenue opportunities.**
  - In healthcare, the lack of medical device interoperability has the potential to lead to $35 billion in missed annual cost savings across the U.S. healthcare system.[1494]
  - In renewable energy, attaining interoperability can lead up to $10 billion annually in savings from lower transaction costs, increased operating efficiency, lower operations and maintenance needs and lower design and installation costs.[1495] The lack of interoperability may cost customers $59 billion in forgone opportunities

[1494] See note 1131

[1495] See note 1404

© Strategy of Things, 2025. All rights reserved.

from having innovative customer energy applications deployed in residential and commercial buildings.[1496]

- **Create adverse environmental impacts due to inefficient operations.**
  - In renewable energy, interoperability challenges, some attributed to a lack of standards, hinder integration of energy efficiency and renewable energy technologies, resulting in decreased adoption of these technologies.
  - In contrast in transportation and logistics, interoperability enables data sharing of logistics data in near real-time and can reduce global freight emissions by 22%.[1497]
- **Create vendor lock-in and switching barriers.** The lack of interoperability creates a fragmented market of "walled garden" IoT solutions that work with a small set of "compatible" equipment, leading to reduced choices and vendor "lock-in."

> IoT technologies based on proprietary protocols do not work with systems having different standards and protocols. This "locks in" the buyer to procure and use systems from the vendor and its ecosystem partners. These systems may be more expensive, have fewer innovative features or have capability limitations.
>
> Migrating from these systems to other lower cost or more innovative alternatives is difficult and may require significant switching costs. Extracted from Section 17.3.1.

The federal government supports and facilitates interoperability through the development of standards. Except in matters related to safety, environmental and health concerns, the U.S. government's approach to standards development is "industry leads, government supports." In this capacity, the federal government provides the foundational pre-standards research and development necessary for industry to establish technical standards. This role and representative actions are discussed in Section 24.

Federal agencies may participate in standard-setting organizations, both domestically and internationally, to advocate for U.S. interests and ensure that U.S. standards are harmonized with global practices.

In addition, the government promotes consensus standards by adopting technologies with those standards and incorporating their requirements into federal regulations and procurement processes to facilitate broader adoption and adherence.

Interoperability issues are broad, complex and differ between industries. At an aggregate level, our research identified some representative opportunities for the federal government to facilitate IoT interoperability. These include:[1498]

[1496] See note 1401

[1497] See note 911

[1498] "Interoperability in Internet of Things: Taxonomies and Open Challenges," Link

© Strategy of Things, 2025. All rights reserved.

- **Semantic and syntactic interoperability.** The heterogeneity of IoT devices in standards, datasets and formats reduces interoperability. While interoperability challenges vary by industry, new methods and approaches to facilitate interoperability that are developed or investigated have the potential to address these concerns.
- **Cross-platform interoperability.** IoT applications may cut across industry domains, such as in transportation and smart cities. Many standards focus on the device and network levels and less on the platform levels and their interactions.
- **Interoperability testing of solutions and standards**. IoT solutions follow certain standards and testing is performed to verify that those standards have been implemented correctly. Support for the development of testbeds facilitates the verification of interoperability and that standards have been implemented correctly.
- **AI-facilitated interoperability.** The use of AI technology to translate between formats and meanings can facilitate interoperability. Examples include mapping and aligning data schemas to translating protocols and adapting to changes in devices. AI offers the potential to facilitate interoperability as systems evolve.
- **Interoperability of future IoT technologies.** IoT continues to evolve with technologies at varying stages of maturity. Pre-standardization initiatives, such as developing frameworks and the science to develop standards, are needed to facilitate the development of standards for these evolving technologies.

23.1.2. Core: Cybersecurity

Cybersecurity was identified as a top challenge in manufacturing, insurance, healthcare and renewable energy and was frequently mentioned as an area of concern in the remaining industries.

Cybersecurity concerns slow the realization of benefits offered by IoT by reducing user trust and confidence, preventing its adoption and use and hindering its integration and interconnection with other information technology and industrial operations technology systems. It also slows IoT's evolution where intelligence and hyperconnectivity combine at scale to bring economic and society-wide transformational benefits.

Cybersecurity concerns slow IoT adoption, scaling, value realization and delivery and evolution in many ways including:

- **Increasing intrusion risks.** Cybersecurity risks were identified as one of the top three project risks that hinder IoT adoption.[1499] IoT presents a new and massive attack surface for cybercriminals to exploit. Some IoT devices and systems may have weak authentication and authorization controls, inadequate encryption and vulnerabilities in hardware, firmware and software that cybercriminals can exploit. Furthermore, some IoT devices are placed in locations with limited or no physical security, providing easy access to cybercriminals.

[1499] "Three Main Risks That Prevent Companies From Adopting Iiot Solutions", IIoT World, November 24, 2021. Link

© Strategy of Things, 2025. All rights reserved.

Successful cyberattacks result in unauthorized access to devices and the systems to which they are connected, operational disruptions, loss of sensitive data and compromised control IoT devices and systems. These impacts are amplified as IoT systems are increasingly interconnected and integrated across the economy and society.

- **Raising cybersecurity risks across entire industries.** IoT technology provides cybercriminals with new ways to access certain industries. Manufacturing is the most targeted industry by cybercriminals in North America.[1500] In factories and industrial environments, the introduction of IoT into formerly "air gapped" environments[1501] containing OT systems provides cybercriminals with potential entry points.[1502] Similarly, the Personally Identifiable Information (PII) collected by insurance carriers makes them attractive targets for cybercriminals. The use of IoT-enabled insurance products may expose vulnerabilities that allow access to this data.

> A study of the top 99 insurance companies found that these carriers are vulnerable to cyber-attacks. Extracted from Section 16.3.1
>
> In healthcare, many medical devices, especially legacy and early generation models, were not designed with cybersecurity protections. The average medical device has 6.2 vulnerabilities. This challenge is exacerbated by the fact that more than 40% of medical devices are near end-of-life and poorly or unsupported by the device manufacturers. Extracted from Section 19.3.1

- **Disrupting operations and services.** One consequence of cyberattacks is the potential to disrupt operations and services, especially in critical applications. For example, IoT devices in the smart grid have the potential to be compromised, resulting in a disruption of electricity supply and delivery to downstream users. In healthcare, ransomware and malware are able to spread to medical devices, resulting in risks to patient outcomes.[1503]

[1500] "X-Force Threat Intelligence Index 2022", IBM Security Report, February 2022. Link

[1501] An air-gapped system is isolated from other systems and cannot connect wirelessly or physically with other systems and the Internet.

[1502] "2022 State of Operational Technology and Cybersecurity Report", Fortinet report, 2022. Link

[1503] "Total Cost of Ownership Analysis on Connected Device Cybersecurity Risk," Asimily Report, 2023. Link

© Strategy of Things, 2025. All rights reserved.

> Nearly two-thirds, 64%, of 641 health delivery organizations suffered operational delays and 59% had longer patient stays.
>
> A woman sued an Alabama hospital for providing "severely diminished" care during childbirth, citing the impact of a ransomware attack that locked down hospital systems, preventing crucial tests, leading to brain damage and the subsequent death of her baby nine months later due to an undetected umbilical cord entanglement. Extracted from Section 19.3.1.1.

Vulnerable IoT devices may be compromised and be enlisted into botnets and used to launch Distributed Denial-of-Service (DDoS) attacks, disrupting services and causing financial losses for individuals and organizations.

> In 2016, the Mirai IoT botnet, in one of the highest profile incidents, infected over 600,000 devices with a Distributed Denial of Service (DDOS) attack on a few services including the Dyn Domain Name Service and the French web service OVH.[1504] Since its initial release, variants of the original Mirai botnet continue to infect IoT devices today. Extracted from Section 22.3.4

- **Losing personal and proprietary information.** Device intrusions may allow cybercriminals lateral access to the backend systems, where confidential data and proprietary data are stored. This data and information are attractive to cybercriminals. For example, insurance and healthcare companies collect vast amounts of Personally Identifiable Information (PII) that is prized by cybercriminals. On the other hand, nation-state attackers target proprietary and sensitive information held by corporate and government organizations.
- **Incurring financial damages.** Cybersecurity incidents involving IoT devices can result in significant economic losses due to downtime, recovery costs, legal fees and damage to business operations.

> For example, a 2022 IBM report estimates that the average total cost of a data breach was $4.82 million for critical infrastructure organizations, including those in the public sector. In healthcare, cyberattacks are responsible for a 20% increase in patient mortality and cost Health Delivery Organizations (HDO) an average of $10.1 million per incident. Fixing and recovering from a cyberattack could put smaller HDOs and hospitals out of business. Hospitals are most susceptible to closure with their median operating margin 0.4% in March 2023. Extracted from Section 17.3.2

A 2023 Cybersecurity Risk analysis, studying the average loss exposure (probable likelihood and probable financial impact) of various attack scenarios across several industries, reported financial impacts of $5.5 million, $2.1 million and $1.1 million per scenario for the healthcare, financial and insurance and manufacturing industries respectively.

[1504] "Inside the Infamous Mirai IoT Botnet: A retrospective analysis", E. Bursztein, Dec 14, 2017. Link

© Strategy of Things, 2025. All rights reserved.

These scenarios include insider misuse, web application attack, system intrusion, insider error, ransomware, social engineering and denial of service attacks. Extracted from Section 14.3.1

- **Creating regulatory compliance issues.** Some industries are subject to regulations and compliance standards governing data protection and cybersecurity. A lack of IoT cybersecurity could lead to non-compliance with these regulations, resulting in fines, legal penalties and other regulatory consequences.

  For example, the healthcare industry is subject to HIPAA regulations. Breaches of unsecured Personal Health Information must be disclosed to the affected individuals, the Secretary and the media if appropriate.[1505] Firms that violate HIPAA regulations are subject to fines.
- **Incurring reputational, safety and national security risks.** Cybersecurity breaches may lead to a variety of risks. Companies and organizations that fail to secure IoT devices risk damaging their reputation and losing the trust of customers, partners and stakeholders. High-profile security breaches can result in financial losses and long-term harm to brand reputation.

  IoT devices are increasingly being integrated into critical infrastructure systems such as smart cities, healthcare facilities and industrial control systems. A lack of cybersecurity could lead to physical safety risks, such as manipulating traffic signals, tampering with medical devices or disrupting industrial processes.

  Inadequately secured IoT devices pose national security risks, as they can be exploited by state-sponsored actors or cybercriminal organizations to conduct cyber warfare, espionage or sabotage against critical infrastructure and government systems.

IoT cybersecurity is a complex and wide-ranging challenge. Each industry has different operating environments that create unique cybersecurity challenges. For example:

- Factories employ industrial automation and control systems and devices in a "cybersecurity by air gap" environment that is now exposed to the outside world through IoT.
- Hospitals are filled with 10 to 30 years old medical devices with infrequent to no firmware updates. Many of these devices collect and access patient data without requiring user authentication or credentials.
- The distribution of millions of solar panel and battery systems into homes and communities decentralizes cybersecurity responsibility to the individual system owner.

[1505] "Breach Notification Rule," U.S. Department of Health and Human Services. Link

© Strategy of Things, 2025. All rights reserved.

This section focuses on the industry-agnostic aspects of cybersecurity. Our research identified the following IoT technology infrastructure opportunities that will partially address the cybersecurity challenges. These include:

- Artificial intelligence based IoT cybersecurity
- Post-Quantum Cryptography (PQC)
- Other areas of research

Each of these is discussed in the following sections.

23.1.2.1. Artificial intelligence based IoT cybersecurity

Many studies have identified the use of artificial intelligence as an important capability in addressing IoT cybersecurity threats.[1506,1507] AI is well suited for analyzing vast amounts of data from IoT devices, detecting and recognizing patterns and responding to potential attacks in a proactive and timely manner.

The integration of AI into the broader "cybersecurity fabric" of capabilities and tools enables organizations to have comprehensive visibility of all their IoT devices, perform unified threat analysis and automate threat containment.[1508] Management consultancy Deloitte calls AI a "force multiplier that enables organizations not only to respond faster than attackers can move, but also to anticipate these moves and react to them in advance."[1509]

Cybercriminals do not always need to penetrate an IoT device or network to compromise or disrupt its operation.[1510] Instead, they use a variety of methods to modify the IoT AI algorithms to change the response to sensor inputs. For example, covering up a stop sign to hide the word STOP can confuse autonomous vehicles in a smart city. A similar type of attack with a different goal is data poisoning. This type of attack alters inputs over a period of time to compromise the integrity and the behavior of the IoT AI algorithm. For example, the AI algorithm can be altered to not respond to certain incidents.

To be effective, the "right" AI models must be developed. Building effective machine learning and AI models and maintaining them is, however, challenging. Different devices have different operating characteristics, constraints and types of data collected for security training. Furthermore, a variety of different techniques is used to train the models according to the type of threats. A model's efficacy, precision and outcomes may be reduced if the incorrect training

---

[1506] "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review," U. Tariq, I. Ahmed, et al. Sensors 2023, 23(8), 4117, April 19, 2023. Link

[1507] "Cybersecurity Risk Analysis in the IoT: A Systematic Review," T. AlSalem, M. Almaiah and A. Lutfi. Electronics 2023, 12(18), 3958; September 20, 2023. Link

[1508] "The Role of Artificial Intelligence in IoT and OT Security," BrandPost, CSO, October 30, 2018. Link

[1509] "Cyber AI: Real defense," E. Bowen, W.Frank and D. Golden, Deloitte Insights, Deloitte Consulting. December 7, 2021. Link

[1510] "Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity," M. Kuzlu, C. Fair and O. Guler, Discov Internet Things 1, 7 (2021). February 24, 2021. Link

© Strategy of Things, 2025. All rights reserved.

method is used. Collecting the right IoT security data to train the models once the right method is selected is critical. The data must be representative, relevant and recent.[1511]

Many cyberattacks can be mitigated or prevented by early detection and recognition of unusual activities and traffic patterns. Some attacks are subtle and less obvious, escaping the notice of people, algorithms and AI. Threats are evolving, with the most recent ones being the least detectable. These attacks and how to defend against them effectively are critical topics for research. Representative areas of related research include:

- Research, development and enhancement of AI cybersecurity algorithms, exploring ensemble learning approaches and implementing real-time adaptive cybersecurity systems.[1512]
- Research and development of lightweight and efficient ML and AI models for IoT devices with limited resources while ensuring their security and privacy.[1513]
- Approaches to detect and protect AI algorithms against input and data poisoning attacks[1514]

One research publication that conducted a literature survey of the use of AI in cybersecurity noted research gaps for further study. These gaps were identified and organized into specific topic categories.[1515] These are:

- **Emerging areas of AI cybersecurity applications.** Research gaps to be addressed include real time automated retrieval of key risk indicators to create an early-warning system, detection of new attacks, and improving predictive intelligence and analytics to support automated decision-making. Other topics of research include studying AI-powered cyber defense and resilience, data breach prevention and discovery and context driven alert processing triage and AI powered incident response.
- **Data representation.** Research gaps include refined data representation, context aware adaptive cybersecurity, incremental learning and recency mining.
- **Advanced AI methods.** Research gaps include multiple data source analysis, explainable AI and augmented human-AI intelligence.
- **Infrastructure to support AI.** Research gaps include the development of information sharing hubs at national and international levels to enable threat intelligence platforms at the economy wide level and the evaluation and development of AI models using new, real-time and broader datasets.

[1511] "Analysis of IoT Security Challenges and Its Solutions Using Artificial Intelligence," T. Mazhar, D. Talpur, et al. Brain Sci. 2023, 13(4), 683; April 19, 2023. Link

[1512] See note 1507, 1506

[1513] See note 1506

[1514] See note 1510

[1515] "Artificial intelligence for cybersecurity: Literature review and future research directions," R. Kaur, D. Gabrijelčičand and T. Klobučar. Information Fusion, Volume 97, 2023, 101804, ISSN 1566-2535. Link

© Strategy of Things, 2025. All rights reserved.

23.1.2.2. Post Quantum Cryptography (PQC)

Quantum computing is a rapidly emerging technology that uses the principles of fundamental physics to solve complex problems in a short amount of time. While traditional computer systems use digital processors to perform calculations, quantum computing uses "specialized hardware and algorithms that take advantage of the principles of quantum mechanics."[1516] In a 2019 experiment, Google performed and completed a target computation in 200 seconds and suggested that it would take the world's fastest supercomputer 10,000 years to complete.[1517]

This technological advancement, however, poses significant challenges to cybersecurity. One of the primary concerns is that "quantum computers have the potential to bypass the encryption locks that currently protect the world's communications and data."[1518] According to the White House National Security Memorandum/NSM-10 on Quantum Computing, "a quantum computer of sufficient size and sophistication, also known as a Cryptanalytically Relevant Quantum Computer (CRQC), will be capable of breaking much of the public-key cryptography used on digital systems across the United States and around the world. When it becomes available, a CRQC could jeopardize civilian and military communications, undermine supervisory and control systems for critical infrastructure and defeat security protocols for most Internet-based financial transactions."[1519]

Traditional encryption methods, such as RSA and ECC, rely on the difficulty of certain mathematical problems, like factoring large numbers or solving discrete algorithms. These are susceptible to being efficiently solved by quantum computers using algorithms like Shor's algorithm.[1520] As quantum computing matures, these cryptographic schemes could be rendered obsolete, leaving IoT devices and their data vulnerable to interception and manipulation.

IoT devices are particularly vulnerable to the risks posed by quantum computing. Professionals often operate IoT devices in environments with limited computational and energy resources, making them ill-equipped to handle the sophisticated encryption algorithms required to resist quantum attacks. Additionally, the scale and diversity of IoT deployments make it challenging for users to implement security updates and patches uniformly across all devices. As a result, cybercriminals could exploit vulnerabilities in IoT devices to gain unauthorized access to sensitive data or launch large-scale attacks, potentially causing widespread disruption and damage.

[1516] "Quantum computing could threaten cybersecurity measures. Here's why – and how tech firms are responding," S. Torkington, World Economic Forum, April 23, 2024. Link

[1517] "Quantum Supremacy Using a Programmable Superconducting Processor," J. Martinis and S. Boixo. Google AI Quantum, October 23, 2019. Link

[1518] See note 1516

[1519] "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," NSM-10, The White House, May 4, 2022. Link

[1520] Shor's Algorithm is an algorithm for finding the prime factors of large numbers in polynomial time. In cybersecurity, a common encryption technique is RSA (Rivest–Shamir–Adleman). RSA is based on a public key that is the product of two large prime numbers that are kept secret. RSA assumes that a computer will not be able to factor a very large number into its prime components, as factoring is a very different kind of problem-solving compared to addition or multiplication. Link

© Strategy of Things, 2025. All rights reserved.

While the concerns about the ability of quantum computers to break today's encryption algorithms are valid for professionals, CRQ computers powerful enough to do so will not be available until at least the 2030s.[1521] To prepare for the post-quantum computing era, NIST is soliciting, evaluating and standardizing a number of quantum-resistant public-key cryptographic algorithms.[1522] As of July 2022, four encryption algorithms have been selected for inclusion into NIST's post-quantum cryptographic standard. Four other algorithms are still under consideration.[1523]

Integrating Post Quantum Cryptography (PQC) into IoT devices is a balance between security, performance and resource limitations. The PQC algorithms are computationally intensive but IoT devices are compute, memory and energy constrained. Latency is introduced during encryption and decryption, which requires limiting the size of public keys for low latency applications but makes the PQC less resistant.[1524] The PQCs must be backward compatible and work with existing IoT communication protocols. Opportunities exist for continued research to identify, understand, evaluate and optimize lightweight quantum safe algorithms that are suitable for use on resource constrained IoT devices for various domains and applications.

23.1.2.3. Other areas of research

A scan of the research literature has identified other areas of research opportunities. Some of these opportunities include:[1525]

- **Context-aware adaptive cybersecurity frameworks.** Evolving cybersecurity threats render static cybersecurity measures and responses inadequate and irrelevant. The ability to continuously assess and adjust security measures based on real-time threat intelligence increases cybersecurity protection.
- **Secure firmware and hardware design.** The security of IoT devices depends on the integrity of their firmware and hardware components. Studies have emphasized the importance of implementing secure development practices and utilizing hardware security modules to safeguard against physical attacks and firmware tampering. Future research should address the challenges of secure firmware updates, hardware-based attestation and supply chain security.

[1521] "When a Quantum Computer Is Able to Break Our Encryption, It Won't Be a Secret," E. Parker, RAND, September 13, 2023. Link

[1522] "NIST Asks Public to Help Future-Proof Electronic Information," U.S. National Institute of Standards and Technology, December 20, 2016. Link.

[1523] "NIST Announces First Four Quantum-Resistant Cryptographic Algorithms," News, NIST, July 5, 2022. Link

[1524] "Post-Quantum Cryptosystems for Internet-of-Things: A Survey on Lattice-Based Algorithms," R. Asif. IoT 2021, 2(1), 71-91; February 5, 2021. Link

[1525] Link

© Strategy of Things, 2025. All rights reserved.

- **Lightweight encryption algorithms.** IoT devices are resource constrained and cannot process computationally intense algorithms. Encryption algorithms designed to work with resource constrained IoT devices are needed to provide strong cybersecurity.[1526]
- **Alternative approaches to cryptography.** Approaches such as "friendly jamming" that can be used with existing resource constrained devices and do not require extra computing power should be studied.[1527]
- **Hardware-based security solutions.** Adoption of pervasive hardware-based security solutions such as trusted execution environments, secure boot and secure storage would strengthen the security of IoT devices and prevent physical tampering and attacks.[1528]
- **Blockchain.** Integration of adaptive and scalable blockchain technology would enable secure and transparent data sharing and management among IoT devices and stakeholders.[1529]

While there are considerable industry efforts to address cybersecurity, the problem cannot be solved by industry alone. Achieving robust cybersecurity requires a long-term multi-stakeholder effort with active participation from buyers, manufacturers, consultants, academia and government. The federal government plays a key role in helping to minimize cybersecurity risks through a variety of actions. This role and representative actions are discussed in Section 24.

23.1.3. Core: Privacy

The need to address privacy requirements appeared as a gap in five of the nine industries. These industries include agriculture, insurance, retail, cities and healthcare.

[1526] "LSEA-IOMT: On the Implementation of Lightweight Symmetric Encryption Algorithm for Internet of Medical Things (IoMT)," S. Saif, P. Das and S. Biswas. Lecture Notes in Networks and Systems, vol 519. Springer, Singapore. Link

[1527] "Securing Internet of Medical Things with Friendly-jamming schemes," X Li, H. Ning Dai, et al. Computer Communications, Vol 160, pp 431-442. July 1, 2020. Link

[1528] See note 1506

[1529] See note 1506

© Strategy of Things, 2025. All rights reserved.

Privacy challenges include the unauthorized collection, storage and use of data, unauthorized disclosure of private information through theft and data sharing, as well as the misuse of private and proprietary information. These challenges are exacerbated as IoT systems are increasingly integrated into the economy, leading to a loss of trust and resistance to IoT adoption and scaling. Extracted from Section 8.3.1.3

Privacy concerns are a top-of-mind concern. In a KPMG survey of 2,000 U.S. adults in 2021, 86% reported that data privacy was a concern, 68% were concerned with the level of data collected by businesses, 40% did not trust companies to use their data ethically, while 30% were not willing to share any personal information. Extracted from Section 16.3.1

A 2016 American Farm Bureau Federation survey of 400 farmers and ranchers reported they wanted to control the information collected from their equipment. Specifically, 77% were concerned with who accesses their data and whether it could be used for regulatory purposes. Two-thirds, or 67%, stated they will consider how outside parties use and treat their data when deciding which technology or service provider to use. Extracted from Section 13.3.2

A 2021 survey of 1,001 U.S. adults indicated that 45% of drivers between the ages of 18 and 24 are not comfortable with sharing their driving data. Extracted from Section 16.3.1

Privacy concerns slow the realization of benefits offered by IoT by reducing user trust and willingness to participate. This hinders IoT adoption, limiting its use and slows integration and interconnection with other information technology and industrial operations technology systems. It also delays IoT's evolution where intelligence and hyperconnectivity combine at scale to bring economy and society-wide transformational benefits.

In response to these concerns, IoT adopters and users may forgo purchase, purchase a smaller quantity, limit how the devices are used and limit the sharing of personal and proprietary data. Key privacy concerns hindering adoption revolve around the following:

- **Surveillance and monitoring.** IoT devices and systems may collect data without people's knowledge or consent. For example, Amazon's Alexa smart speakers recorded a private family conversation and sent that recording to someone.[1530] Residential doorbell cameras capture video footage that, under certain conditions, may also be accessed by police to support law enforcement activities.[1531] These concerns have led the American Civil Liberties Union (ACLU) to call smart cities "surveillance cities."[1532] Some technology buyers have forgone purchases, disabled features or restricted how and when the systems can be used.

[1530] "Woman says her Amazon device recorded private conversation, sent it out to random contact." G. Horcher, KIRO 7 News, May 25, 2018. Link

[1531] "The privacy loophole in your doorbell," A. Ng, Politico, March 7, 2023. Link

[1532] "How to Stop 'Smart Cities' From Becoming 'Surveillance Cities'," C. Marlow and M. Saifuddin, ACLU, September 17, 2018. Link

© Strategy of Things, 2025. All rights reserved.

For example, during the 2022 time period, seventeen cities across the United States banned the government use of facial recognition systems. These cities include Boston, New Orleans, Portland (Oregon) and San Francisco.[1533] San Diego temporarily shut down its network of 3,000 streetlight mounted cameras until the city developed an ordinance addressing surveillance technology. While this may achieve the privacy result, it also keeps the users from realizing the full range of benefits available. Extracted from Section 17.3.2

- **Discriminatory and unfair outcomes.** Data collected from IoT systems may be applied incorrectly or without controls and yield improper or incorrect outcomes. Facial recognition systems are a common IoT application used in a number of industries. A national drugstore chain, in a settlement with the Federal Trade Commission (FTC), was barred from using these systems for five years because "the system generated thousands of false-positive matches" and its "reckless use of facial surveillance systems left its customers facing humiliation and other harms and its (FTC) order violations put consumers' sensitive information at risk."[1534]

In a separate incident in 2022, a company used its facial recognition technology to identify and deny a ticket holder entry to an entertainment event. The ticket holder was barred because she worked for a law firm that engaged in litigation with the company, even though she was not involved in the specific case. Extracted from Section 20.3.1

In insurance, the data collected from IoT devices helps insurers better identify, assess and price risks better, reduce fraud and losses and create new personalized insurance products. At the same time, the collection of vast amounts of data from IoT devices allows insurers to continually understand, differentiate and price risk pools to ever smaller segments. This may lead to "uninsurables", or individuals and businesses who are not able to obtain or afford insurance because of their risk rating. Extracted from Section 16.3.2

- **Theft and disclosure of private and proprietary data.** IoT devices and systems collect, store and transmit sensitive personal or proprietary data, such as Personally Identifiable Information (PII), Personal Health Information (PHI), asset and people location tracking data and behavioral patterns. These data may potentially be disclosed inadvertently such as the example of a well-known fitness app that published a map showing all the sports activity locations and routes of its users, including sensitive locations of military bases and spy outposts.[1535] More commonly, IoT data are stolen due to security vulnerabilities and unauthorized access, resulting in identity theft, as well as theft of proprietary business and government data.

[1533] "The movement to ban government use of face recognition," N. Sheard and A. Schwartz, Electronic Frontier Foundation, May 5, 2022. Link

[1534] "Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards," Press Release, Federal Trade Commission, December 19, 2023. Link

[1535] "Fitness tracking app Strava gives away location of secret U.S. army bases," A. Hern, The Guardian, January 28, 2018. Link

© Strategy of Things, 2025. All rights reserved.

- **Secondary use of data without user consent.** Private and proprietary IoT data may be collected with user approval for a specific purpose. Concerns arise, however, when that IoT data are repurposed by the IoT solution owner or shared with third parties for unrelated purposes without the user's knowledge or consent. Data may be used for something else. Examples include:
    - Video from city traffic monitoring cameras may be accessed by the police to monitor people in the local community.
    - Health information collected by wearable devices may be shared with insurance companies that may consider it in underwriting policies.
    - Precision agriculture data collected by smart farming machines may be resold to fertilizer manufacturers who recreate the grower's "secret recipe" for success and make it available to competitors.
- **Ownership of data collected from IoT devices and systems.** While the value of IoT is clear, the ownership of the data collected is less so. For example, a factory uses IoT to predict maintenance, optimize production and improve product quality. The sensors collect data on how the machines are used and their usage patterns. The factory uses the IoT data to optimize operations, the equipment manufacturers use it to improve machine design and the IoT solution providers uses the data to improve its analytic capabilities. These data patterns may, however, contain information about the factory's "secret recipe" for maximizing productivity. Ownership issues arise if the equipment manufacturer wants to sell the data to third parties or the solution vendor wants to create an offering based on the data to the factory's competitors. The ambiguity surrounding data ownership in this context raises critical questions about who has the right to control, access and monetize this valuable resource. Without clear frameworks and regulations, potential adopters may be reluctant to consider or use IoT and those that do may limit the amount of data they are willing to share.

Our research identified the following IoT technology infrastructure opportunities that will partially address the privacy challenges. While some of these were mentioned as opportunities in specific industries, they are aggregated here as part of a broader industry-agnostic discussion. The three technology areas of opportunity are listed below:

- Privacy by Design (PbD)
- Privacy enhancing technologies
- Context aware privacy

Each of these is discussed in the following sections.

23.1.3.1. Privacy by Design (PbD)

This system engineering approach to building privacy-compliant products and services embeds privacy considerations throughout the product development process instead of "bolting" it on afterwards. A detailed description of PbD is found in Section 16.3.1.2

© Strategy of Things, 2025. All rights reserved.

Despite the value offered by PbD, there is no agreed-upon methodology to support the systematic engineering of privacy into systems.[1536]

> *A challenge, however, is that system development life cycles and organizational engineering processes do not consider such practices. So far, privacy is simply not a primary consideration for engineers when designing systems. This gap raises many questions: When should privacy requirements first enter the system development life cycle? Who should be responsible? Given that privacy controls impact business goals, who can actually decide on appropriate measures? Must there be ongoing privacy management and practices monitoring? If organizations purchase standard software solutions or outsource operations, pass data to third parties or franchise their brands, who is responsible for customer privacy?*[1537]

IoT devices integrate into complex environments with IoT, OT and IT systems. For example, future smart cities, farms and factories may contain thousands of IoT devices of various types and capabilities that communicate with each other. Designing privacy for the systems that IoT operate in is much more complex than designing privacy by design for individual products. Further research and development is required in understanding how privacy can be embedded into the underlying infrastructure and systems to create "Privacy by Design" infrastructures, platforms and systems at scale.

23.1.3.2. Privacy enhancing technologies.

Privacy Enhancing Technologies (PETs) are a "broad set of technologies that protect privacy by removing personal information, by minimizing or reducing personal data or by preventing undesirable processing of data while maintaining the functionality of a system."[1538] Privacy enhancing technologies include cryptographic algorithms, data masking, artificial intelligence algorithms and other technologies. [1539] Detailed discussion of privacy enhancing technologies is found in Section 17.3.1.2.

While PETs partially mitigate some of the privacy concerns, its use in IoT is not widespread. PETs suffer from "the need for more research and development, limited technical expertise, perceived and possible risks, financial cost and the lack of generalizable solutions."[1540]

Continuing research and development is necessary to advance the state of privacy enhancing technologies. According to the 2023 National Strategy to Advance Privacy-Preserving Data Sharing and Analytics 2023 report, while cryptographic technologies have demonstrated initial

---

[1536] "The challenges of privacy by design," S. Spiekermann, Communications of the ACM, July 1, 2012. Link

[1537] See note 1536

[1538] "National Strategy to Advance Privacy-Preserving Data Sharing and Analytics," Fast-track action committee on advancing privacy-preservation data sharing and analytics, Networking and information technology research and development subcommittee, National Science and Technology Council Report, March 2023. Link

[1539] "Top 10 Privacy Enhancing Technologies & Use Cases in 2023," C. Dilmegani, AI Multiple, July 21, 2020. Link

[1540] "Advancing a Vision for Privacy-Enhancing Technologies," A.Macgillivray and T. deBlanc-Knowles, White House Office of Science and Technology Policy blog, June 28, 2022. Link

© Strategy of Things, 2025. All rights reserved.

success for real world adoption in simple applications, scalability and efficiency challenges must still be addressed in the context of a broader set of threat models."[1541]

Furthermore, PET technologies lack consensus industry standards. The National Strategy to Advance Privacy-Preserving Data Sharing and Analytics report found that "there are no widely adopted standards for data formats, application programming interfaces or system architectures that are necessary to facilitate the interoperability and deployment of PPDSA technologies."

While some standards development is underway for homomorphic encryption and zero knowledge proofs, there is a need for "more standards that specify foundational cryptographic primitives and other Privacy Preserving Data Sharing and Analytics (PPDSA) technologies which would facilitate adoption and trust in solutions."

23.1.3.3. Context aware privacy.

Context-aware privacy is an advanced systems approach to privacy that recognizes that different situations and conditions warrant various levels of data collection.

> Context-aware privacy considers the location, the environment and the specific situation and seamlessly adjusts how and what data are collected, processed and shared. Extracted from Section 23.3.2
>
> For example, smart parking systems that employ cameras analyze video images in real time to detect open parking spaces and relay that information to a mobile app. In normal situations, the cameras do not scan for license plate information, nor store any video images. When an Amber Alert is issued for the local region, however, the system is automatically enabled to scan license plates and relay the location of the vehicle matching the description to law enforcement. Upon cancellation of the Amber Alert, the parking system returns to its normal privacy mode.
>
> Several broad research areas need to be addressed for the implementation of context-aware computing and privacy for smart cities and other domains. These include context definition, context-aware architectures, context sensing, context prediction based on limited to no data, context representation, context interpretation and adaptation, evaluation of context aware systems and privacy control. Other areas requiring additional research include notification and consent, context-aware privacy protection methods, algorithmic explainability, risk assessment of potential harms and user-centric tools, processes and interfaces. Extracted from Section 17.3.1.2.

While there are various industry efforts to address privacy, the problem cannot be solved by industry alone. Achieving robust privacy requires a long-term multi-stakeholder effort with active participation from buyers, manufacturers, consultants, academia and government. The federal government plays a key role in achieving privacy through a variety of actions. This role and representative actions are discussed in Section 24.

23.1.4. Core: Connectivity

IoT devices and other smart equipment requires connectivity to send data to edge servers and remote data centers in the cloud for processing and storage. While connectivity challenges were

[1541] See note 1274

© Strategy of Things, 2025. All rights reserved.

directly identified in two of the nine industries studied, agriculture and manufacturing, the lack of connectivity availability in rural and underserved communities affects other industries operating in those areas. For example, a variety of healthcare, smart city, community and transportation and logistics IoT applications would not be available or would be significantly limited without connectivity. For this reason, connectivity challenges have been included as a core gap.

Connectivity challenges that affect IoT operation come in a variety of forms, including a lack of supporting broadband infrastructure, poor signal coverage, interference from built and natural sources and lack of affordable service. These challenges vary for urban, rural and remote communities.

Many rural and remote communities lack connectivity service due to an absence of broadband infrastructure and while urban communities have the infrastructure, they may experience signal coverage issues such as interference. Furthermore, when underserved urban communities have infrastructure, the affordability of connectivity services issues may hinder access to those connectivity services.

Connectivity challenges slow the realization of benefits offered by IoT use limiting those who can connect, where they can connect and what applications can be supported. These factors hinder IoT adoption by limiting its use and outcomes and slowing integration and interconnection with other information technology and industrial systems. They also delay IoT's evolution where intelligence and hyperconnectivity combine at scale to bring economic and society-wide benefits.

In response to these challenges, IoT adopters and users may forgo purchases, purchase in smaller quantities or limit their purchases and applications to those applications that are supported by the available connectivity. Key connectivity concerns slowing adoption include:

- No connectivity service to access.
- Inability to support a full range of IoT applications.
- Inability to realize IoT application benefits.
- Inability to fully connect and automate.
- Reduced trust in IoT.
- Inability to scale.
- Increased security risks.

Each of these concerns are discussed below.

- **No connectivity service to access.** Without connectivity IoT cannot operate. The U.S. Federal Communications Commission (FCC) reported that as of December 2022, 45 million Americans lack access to both 100/20[1542] Mbps fixed download and upload service and 35/3 Mbps mobile 5G-NR service. Of this, 24 million Americans, including 28% in rural communities and 23% in Tribal Lands, are in areas where fixed terrestrial

[1542] On March 14, 2024, the FCC has updated its definition of broadband service from 25/3 to 100/20 Mbps. Source: "FCC increases broadband speed benchmark," FCC News Press Release, Federal Communications Commission, March 14, 2024. Link

© Strategy of Things, 2025. All rights reserved.

broadband service has not yet been physically deployed. Mobile 5G-NR service of 35/3 has not been deployed for 36% of Americans in rural areas and 20% in Tribal Lands.[1543]

- **Inability to support a full range of IoT applications.** IoT devices rely on the type and quality of the available connectivity. For a rural community lacking high speed broadband service, IoT applications are limited to those that are non-latency sensitive and require low bandwidth, such as air quality, soil moisture and equipment condition monitoring. In contrast, an area with high-speed broadband infrastructure can support video based IoT applications such as drone imagery and video monitoring.
- **Inability to realize IoT application benefits.** Connectivity challenges reduce the reliability, functionality and outcomes of IoT applications. For example, an IoT application may work intermittently in an area with high interference, reduced coverage or unreliable service. This intermittency results in missed data collection and transmission, reducing the application's ability to perform in a consistent and intended manner. Similarly, low latency IoT applications operating in high interference urban environments may have difficulty transmitting and receiving information.
- **Inability to fully connect and automate.** Many IoT devices are integrated into operations systems and designed to improve efficiency by automating processes and systems. The inability to connect compromises the operations of these systems and prevents benefit realization. For example, smart energy management systems may not be able to adjust usage based on real-time data if they cannot communicate with utility providers or other devices in the network.
- **Reduced trust in IoT.** Timeliness of data and the reliability and quality of the connectivity service are crucial in many IoT applications, especially in sectors such as healthcare, industrial automation and public safety where quick decisions are needed. Without reliable and consistent connectivity, the reduced availability of data can lead to the use of outdated information in the decision-making processes. This creates situations where the user does not trust the outcomes produced by the IoT system and limits its use in critical situations or applications.
- **Inability to scale.** Connectivity challenges slow the scaling of IoT deployments. Insufficient infrastructure and coverage limit what types of IoT applications can be supported as well as limiting the number of supported IoT applications that can be deployed, connected and operated. For example, limited spectrum may lead to interference and degraded performance of IoT devices in a smart city with hundreds of thousands of devices. Similarly, a rural community with reduced coverage may only be able to connect a small number of IoT devices.
- **Increased security risks.** Connectivity issues can exacerbate security risks in IoT networks. Weak or intermittent connections may create vulnerabilities that malicious actors could exploit. Additionally, without a reliable connection it becomes difficult to implement over-the-air security updates and patches, leaving devices and networks more susceptible to cyber-attacks.

[1543] "FCC increases broadband speed benchmark," FCC News Press Release, Federal Communications Commission, March 14, 2024. Link

© Strategy of Things, 2025. All rights reserved.

Our research identified the following IoT technology infrastructure gaps. While some of these were mentioned as gaps in specific industries such as agriculture or manufacturing, they are aggregated here and discussed in an industry-agnostic context. The three areas of gaps are:

- Broadband ubiquity
- "Last Acre" coverage
- Evolving connectivity capabilities with future needs

Each of these is discussed in the following sections.

23.1.4.1. Broadband ubiquity

The availability of broadband infrastructure is a prerequisite for enabling connectivity services. Without this infrastructure, the data collected by IoT devices and networks cannot be transmitted to cloud data centers for storage and processing. There are still parts of the United States, particularly rural and tribal communities, where broadband infrastructure is not available. Furthermore, there are large areas of the country, including forests, deserts and the sea and ocean areas adjacent to land, which are remote, barren and unconnected. These unconnected areas of land and sea offer many opportunities for the implementation of IoT.

For example, rural areas are home to farms, factories and people that would benefit from precision agriculture, remote healthcare monitoring and smart manufacturing. Energy infrastructure, such as solar and wind generation plants, electrical grid infrastructure and oil pipelines and oil rigs operate in remote areas and are frequent users of IoT technologies. Mining operations, conducted in remote areas, benefit from using IoT applications to manage operations, equipment maintenance and worker safety.

Multiple approaches are needed to enable ubiquitous broadband as there is no "one size fits all" approach. Existing approaches have strengths but also challenges. They include:

- Fiber infrastructure provides high capacity, but is expensive, takes decades to deploy and may not reach all areas.
- Service from wireless carriers and operators is best for high density areas but the lack of sufficient financial returns stops wireless operators from entering rural and tribal communities with low population densities.
- Geosynchronous satellite broadband service offers coverage over wide areas but suffer from latency and interference challenges.
- Low Earth Orbit (LEO) broadband satellites offer low latency service but require high investments to build. Satellite operators face complexities in managing multi-satellite fleets.

In addition to these there are alternative or niche approaches, such as TV White Spaces (TVWS) which utilize the unused UHF/VHF frequencies to carry Internet traffic and Power Line Communications (PLC) which carry broadband over power lines. These niche approaches may be appropriate in some cases for specific situations. Some challenges and limitations of these alternative approaches are discussed below.

© Strategy of Things, 2025. All rights reserved.

23.1.4.2. "Last Acre" coverage

In addition to the availability of broadband, wireless coverage in the locations where the IoT devices and systems are operating is critical. For example, IoT in agriculture requires that the sensors in the field, or the "last acre" be connected.[1544] This is a major challenge as farms occupy vast stretches of land, with the largest farm in the United States spanning 190,000 acres.[1545]

Bringing broadband to the farmhouse doesn't address the need to connect the sensors in the field. Besides agriculture, other applications where "last acre" coverage is needed include environmental monitoring, forest monitoring and management, rural emergency services, remote infrastructure monitoring such as electrical, oil pipelines, water infrastructure, and wildlife conservation. Another area, although not land-based, is ocean transport and offshore oil rig operations.

Enabling "last acre" wireless service availability is challenging. Not all areas can be covered due to geographic and topographic constraints. For example, signal attenuation and interference from hills and tree foliage is a common challenge.[1546] According to one technology solution provider, soil moisture sensors placed underneath leafy vegetables in a farm had experienced difficulties communicating with a nearby gateway.

Finally, many wireless operators face unfavorable economics, construction challenges and inability to secure suitable "right of ways."[1547] Privately owned wireless networks are financially infeasible to all but the largest farms who have the capital and resources to operate this type of network.

Special "gap-filler" approaches, such as satellite-based services, TVWS and PLC may partially address some of these "last acre" challenges for specific applications. Specifically, these challenges include the following:

- **TV White Spaces.** TVWS utilizes the unused frequencies in the 470 and 790 MHz range in the United States to provide wireless internet service.[1548] The advantages of TVWS include a range up to 30 km, no requirement for line-of-sight and the ability to penetrate buildings, trees and other obstructions.[1549] TVWS throughput can reach up to 186 Mbps.[1550] TVWS, however, suffers from a variety of challenges, including an absence of

[1544] "Examining Current and Future Connectivity Demand for Precision Agriculture", Interim Report FCC, Precision Agriculture Connectivity Task Force, December 2022, Page 2. Link

[1545] "Top 5 Farms with the Largest Acreage in the U.S.", E. O'Keefe, Successful Farming, September 28, 2019. Link

[1546] "Factors That Affect Lora Propagation in Foliage Medium", R. Anzum, The 18th Learning and Technology Conference, Procedia Computer Science, Volume 194 (2021), Page 149-155

[1547] "Rural Broadband Access in the United States", Center Forward, February 2021. Link

[1548] "What is TV White Space?" Everything RF. Link

[1549] "SAS technology for TV White Spaces", Red Technologies. Link

[1550] "Tuning into the future," M. Suarez, ISE, November 1, 2020. Link

© Strategy of Things, 2025. All rights reserved.

standards-based products and limited or uneven performance based on terrain and susceptibility to interference from other unlicensed sources.[1551]

- **Power line communications.** This approach uses power lines to convey Internet traffic and is increasingly used for smart grid communications. This approach suffers from radio frequency interference and performance is compromised by electrical noise and the overall quality of the power line infrastructure.[1552]
- **Satellite IoT.** Coverage to the "last acre" is provided by satellites. A number of technological challenges remain to be addressed that would "fully unleash the potential of satellite IoT." These areas include physical layer design, antenna design, medium access, network and higher layer protocols and edge computing.[1553]

To address these issues for agriculture, the "Last Acre" bill was introduced in July 2023. This proposed legislation would "establish a new USDA Rural Development competitive grant and loan program to advance connectivity across acreage."[1554] This bill, however, does not address the needs of the other non-agriculture "last acre" applications.

23.1.4.3. Evolving connectivity capabilities to support future needs

As IoT evolves, as described in Section 22.1, the capabilities of the connectivity services must evolve to accommodate future applications. For example:

> Today's communication networks and architectures are not designed to manage the diverse needs of IoT at scale. The network must support heterogeneous devices of all types, brands and models and variations of those models. The traffic from these IoT devices ranges from small bits of data on a periodic basis to continuous streams of high bandwidth video traffic.
>
> Some IoT data are time sensitive and must be acted upon immediately, while other data are stored for future analysis. Some data support critical applications, such as public safety and require a reliable communication network. To support time-sensitive and critical applications, some data are processed in servers integrated into the network near the point of use (edge) and in vehicles (mobile edge), while other data are sent to remote data centers (cloud). The network infrastructure must be resilient against cyberattacks, introduced through known and undiscovered vulnerabilities from the IoT devices. Extracted from Section 23.3.2.

Another example highlights a use case of an autonomous agriculture application.

[1551] "TV White Space: a work in progress," Broadband Center of Excellence, University of New Hampshire. Link

[1552] "Broadband over Power Line," DevX, October 11, 2023. Link

[1553] "A survey on technologies, standards and open challenges in satellite IoT," M. Centenaro, C. Costa, et al., IEEE Communications Surveys & Tutorials PP(99):1-1, May 2021. Link

[1554] "Last Acre Act", Fact Sheet, Senators Deb Fischer (R-Nebraska) and Ben Ray (D-New Mexico). Link

© Strategy of Things, 2025. All rights reserved.

> For example, in row crop farming, machines equipped with GPS, computer vision, sensors and connectivity, operate autonomously to perform a variety of farming tasks, from soil preparation, seed planting, weeding and harvesting.
>
> These smart machines communicate and coordinate with other nearby machines for offloading, refueling and tracking. In addition, the machines collect information, which is sent to the farm operations center in real time for monitoring, processing and action.
> Extracted from Section 13.3.1.1

To support future IoT needs, researchers need to address a number of connectivity considerations. These include service bandwidth, spectrum allocation, connectivity technologies, energy efficiency, interference and sixth generation (6G). Each of these is discussed below.

Service bandwith. While many use cases, including condition monitoring and asset tracking, will continue to be supported by low bandwidth connectivity services, future IoT applications will increasingly involve autonomy, robotics, computer vision and large amounts of sensor data. These applications require a stable and continuous connection, higher bandwidth, low latency and symmetric upload and download speeds. While the FCC's definition of broadband has changed from 25 upload/3 download Mbps to 100/20 Mbps,[1555] the FCC Precision Agriculture Task Force expects a 1 Gbps upload to support future precision agriculture applications.[1556] The availability of this level of service bandwidth will accelerate the adoption of high bandwidth IoT applications but require the building of new infrastructure and augmentation of existing infrastructure.

Spectrum allocation. As IoT adoption grows, spectrum concerns emerge. A 2017 U.S. Government Accountability Office report stated that "rapid increases in IoT devices that use large amounts of spectrum, called high-bandwidth devices, could quickly overwhelm networks, as occasionally happens with smart phones."[1557] Similarly, potential interference issues emerge for low bandwidth devices operating in the unlicensed IoT frequency bands as additional devices come online. While not an immediate concern with the FCC, growth of high bandwidth IoT applications and devices operating in the low bandwidth unlicensed band will require the allocation of additional spectrum.

Connectivity technologies. Future connectivity technologies must support the likely tens of billions of connected devices. A 2022 research report of current IoT connectivity technologies identified some technical shortcomings that compromise this ability, including high signaling overhead, wireless resource scarcity and inefficient wireless resource usage.[1558] Research to develop new technologies that can address the existing shortcomings is important to enable deployment of IoT at scale. This report cited four promising technologies of Compressive

---

[1555] See note 1543

[1556] "Task Force for Reviewing the Connectivity and Technology Needs of Precision Agriculture in the United States", FCC Precision Agriculture Connectivity Task Force, November 10, 2021. Link

[1557] "Internet of Things: FCC Should Track Growth to Ensure Sufficient Spectrum Remains Available," Report to Congressional Requesters GAO 18-71, U.S. Government Accountability Office, November 2017. Link

[1558] "IoT Connectivity Technologies and Applications: A Survey," J. Ding, M. Nemati, C. Ranaweera and J. Choi., arXiv:2002.12646, IEEE Access (Volume: 8) 2020, February 28, 2020. Link

© Strategy of Things, 2025. All rights reserved.

Sensing, Non-Orthogonal Multiple Access, Massive Multiple Input Multiple Output and Machine Learning-assisted IoT Connectivity.[1559]

Energy efficiency. A 2022 study of IoT wireless communication technologies identified energy-efficiency as a challenge. [1560] [1561] IoT devices consume electricity during their operation. From a sustainability perspective, the total energy consumed by the tens of billions of IoT devices operating continuously is significant. Reducing energy consumption reduces grid demand as well as extending the useful life of those IoT devices that use non-rechargeable batteries. The study cited an example of "a reliable and energy saving data transmission solution for cloud-based IoT systems."[1562] Research into future connectivity technologies that support energy-efficient communications would help address this challenge.

Interference. As the number of devices grows, concerns about interference increase. This is of particular concern for low bandwidth IoT devices that communicate in unlicensed bands such as LoRaWAN and Sigfox. This issue was noted by the U.S. GAO in its 2017 report which recommended that the FCC track the growth of these IoT devices.[1563] While the FCC will consider adding additional spectrum to alleviate congestion issues, research is needed to alleviate communications interference within existing frequency bands. For example:

> Spectrum sharing techniques, such as that implemented in the Citizens Band Radio Service (CBRS) for the narrow band within the 3.5 GHz band, is one approach that facilitates the shared use of the spectrum. Another technique is cognitive radio, an approach that enables IoT devices to sense the spectrum usage of surrounding users, determine what unused spectrum exists and connect and communicate through the available spectrum. Extracted from Section 23.3.2

Other approaches examine minimizing the impact of interference within existing bands. For example, one study proposed interference aware power control to "maximize the channel capacity and devices attended while guaranteeing link channel Quality of Service (QoS)."[1564]

Sixth Generation (6G). Finally, while 5G deployments are ongoing in the United States, 6G is in the early stages of standards development with the first release of specifications expected in

---

[1559] ibid.

[1560] "Wireless Communication Technologies for IoT in 5G: Vision, Applications and Challenges," Q. Khanh, N. Hoai, et al. Cyber-Physical Mobile Computing, Communications and Sensing for Industrial Internet of Things and Industry 4.0 2021. February 7, 2022. Link

[1561] "Energy Efficiency in Short and Wide-Area IoT Technologies—A Survey," E. Zanaj, G. Caso, et al., March 19, 2021, Technologies 2021, 9(1), 22; Link

[1562] See note 1560

[1563] See note 1557

[1564] "Interference-Aware Power Control for Spectrum Sharing Massive-IoT Communications," A. Anzaldo and A. Andrade. In: Bravo, J., Ochoa, S., Favela, J. (eds) Proceedings of the International Conference on Ubiquitous Computing & Ambient Intelligence (UCAmI 2022). UCAmI 2022. Lecture Notes in Networks and Systems, vol 594. Springer, Cham. Link

© Strategy of Things, 2025. All rights reserved.

2028 and commercial launch expected by 2030.[1565] When released, 6G connectivity will have several advantages over 5G. These include terabit speeds instead of 5G's gigabit speeds, 1 millisecond latency, ubiquitous coverage due to its integration with satellites, AI integration and energy efficiency.[1566] These capabilities will have an overall transformational impact on IoT.

A report from the Center for New American Security cites the strategic importance of U.S. leadership in 6G over China.

> *Given the fundamental importance to the digital economy of communications networks and the standards that govern them, the more successful Beijing's policies are, the greater the challenge for tech-leading democracies to maintain their economic competitiveness. There is also the specter of norms. If these are dominated by illiberal actors, their power to shape how networks are used and to manipulate data flows poses threats to liberal democratic values the world over.* [1567]

The report makes a number of recommendations for the U.S. federal government to consider. Recommendations related to research and development opportunities include:

- Expand research and development funding for 6G technologies.
- Leverage existing capabilities for testing, verification and experimentation of 6G technologies.
- Open additional experimental spectrum licenses to accelerate R&D.
- Enact R&D funding to solve challenges for rural 6G development.
- Expand the platforms for Advanced Wireless Research Program (NSF).

The federal government has always played an integral role in facilitating and enabling IoT connectivity in a variety of ways, from research, grants, spectrum management and policies. Research opportunities exist in improving performance of existing and niche connectivity methods, spectrum sharing and management, interference management, energy efficient connectivity approaches and Beyond 5G technologies. These efforts complement current industry efforts to deploy, operate and optimize services.

Achieving ubiquitous connectivity at the most appropriate service level is a long-term multi-stakeholder effort with active participation from connectivity service providers, technology developers and manufacturers, regulators, academia and government. The federal government plays a key role in facilitating connectivity through a variety of actions. This role and representative actions are discussed in Section 24.

23.2. Intelligence Gaps

[1565] "3GPP commits to develop 6G specifications," J.P. Tomás, RCR Wireless, December 6, 2023. Link

[1566] "What is 6G? Everything you need to know," S. McCaskill, TechRadar, December 20, 2020. Link

[1567] "Edge networks, core policy: Securing America's 6G future," M. Rasser, A. Riikonen and H. Wu. Center for New American Security, December 2, 2021. Link

© Strategy of Things, 2025. All rights reserved.

One of the core capabilities of IoT systems and devices is to sense, collect and analyze data of the physical environment to allow users to make informed decisions and take relevant actions. The intelligence capabilities, however, of these systems and devices varies. Some systems, such as air quality sensors and vibration sensors collect and route data to cloud-based servers in remote data centers for processing and analysis. Other systems, such as autonomous vehicles where low latency processing is a requirement, process and analyze data on the system so that it can take action immediately.

In the second stage of IoT evolution (discussed in Section 22.1.2), the system's intelligence capabilities evolve from analyzing data to support human decision-making to analyzing data and taking action in real-time without human involvement. Enabling and supporting the intelligence capabilities of IoT requires a multitude of technologies, from low latency connectivity methods, AI and machine learning algorithms, data management to microprocessors capable of running the algorithms.

Our research identified intelligence-related gaps across several industries. For example, AI usability was identified as a challenge in insurance, retail, transportation and logistics and healthcare. Data management, which supports and facilitates the intelligence capabilities of IoT, was identified in the renewable energy and transportation and logistics industries. While not directly identified as a gap in the insurance, retail and healthcare industries, data management is a fundamental enabler for the adoption and use of artificial intelligence in those industries. Intelligent device capabilities, which includes the processing and analysis of data on IoT devices, were identified as a challenge in agriculture and cities.

Our research identified a number of technology infrastructure gaps related to intelligence in IoT. These gaps fall across a number of broad areas, including:

- Data management challenges
- Challenges that affect trusting AI
- Challenges involving intelligent device capabilities

Each of these is discussed below.

© Strategy of Things, 2025. All rights reserved.

23.2.1. Intelligence: Data management

> Research firm IDC estimated that by 2025, there will be 55.9 billion IoT devices generating 79.4 zettabytes (ZB) of data. For comparison purposes, 1 ZB represents 30 billion 4K movies.[1568] While a large portion of the data will be video, other IoT data producers include industrial/automotive/navigation, household/wearables, medical, industry terminals (ATMs, point of sale, ticketing) and other applications like gaming, AR/VR, RFID readers and other devices.[1569] Extracted from Section 23.3.2

Managing the volumes of data collected from IoT devices and systems is a major challenge. As IoT scales, so does data management complexity.

The IoT data collected comes in a variety of types, formats and sizes. It resides and operates in a distributed environment, with data processed on the device, in moving vehicles, and on edge servers and in remote servers in the cloud. Some data are time-sensitive and must be processed immediately while others are stored for future actions. In addition, data may be required to comply with industrial, state and national regulations.

Robust data management capabilities simplify these challenges and help unlock the value of IoT by enabling massive amounts of data to be collected, processed, stored, discovered, queried and analyzed. Without these capabilities, IoT deployments face challenges such as data silos, scalability issues and compromised data integrity. In some industries, including healthcare, robust data management is required to comply with strict data privacy regulations.

In addition, robust data management and governance are foundational for artificial intelligence powered IoT systems.[1570] Robust data management ensures the availability, accessibility, quality and security of data, laying a foundation for AI applications to generate effective decisions and relevant outcomes. Moreover, well-managed data facilitates the development of more accurate and reliable AI models, leading to better predictions, better recommendations and automation of various operations.

For example, the smart electric grid is reliant on information and data to operate and optimize its performance. The data it needs comes from a variety of diverse and siloed sources, such as Advanced Distribution Management Systems (ADMS), Supervisory Control and Data Acquisition (SCADA), Geographic Information Systems (GIS), Advanced Metering Infrastructure (AMI) and Distributed Energy Resource Management Systems (DERMS).[1571] An increasing amount of data comes from IoT systems, including real-time streaming sensor data from wind turbines, solar panels, batteries, inverters and smart utility meters. The inability, however, to manage the growing amounts of data threatens the operation and automation of the

---

[1568] "Seagate Is the First Company to Ship 3 Zettabytes of Hard Drive Storage," M. Humphries, PC Mag, April 8, 2021. Link

[1569] "How You Contribute to Today's Growing Datasphere and its Enterprise Impact," D. Reinsel, IDC Blog, November 4, 2019. Link

[1570] "Data management and governance key to successful AI use," S. Catanzano, TechTarget, February 13, 2024. Link

[1571] See note 1416

© Strategy of Things, 2025. All rights reserved.

grid, lessens the effectiveness of both analytics and AI to plan and optimize grid operations as well as slowing regulatory compliance and innovation of a potentially autonomous grid.

The growing real-time stream of information produced by an increasing number of smart systems and IoT devices poses challenges in aggregating, securing, storing and distributing the data. These data are at varying levels of quality and accuracy and require additional processing and limits how it can be used by AI models. Syntactic and semantic interoperability challenges hinder integration and sharing of the data for use by AI models and automated systems.

The lack of data management capabilities slows the adoption, operation and value realization of IoT and AI-enabled IoT. For example:

- **Inability to harness data to unlock and maximize value.** IoT devices collect vast amounts of data in various formats. Without effective data management capabilities, organizations struggle to process, store, analyze and derive actionable insights from this flood of data. As a result, they may be overwhelmed by the volume and complexity of the data, impeding their ability to extract value from IoT deployments. Incomplete, outdated, missing and inaccurate data leads to flawed analyses, poorly informed decision-making, ineffective and delayed responses and automated actions. This undermines the trustworthiness of IoT systems and diminishes their value proposition for organizations seeking to leverage data-driven insights.
- **Inability to scale IoT.** As deployments scales, so will the number and variety of heterogeneous devices. Heterogeneity brings complexity and challenges to IoT networks. The data collected from these devices may be stored and processed on the device itself, on mobile devices or in the cloud. The devices collect different data, utilize different formats, have different characteristics and process data from various sources and storage types. The lack of standardized data formats, interfaces and APIs complicates data exchange and integration efforts. This fragmentation creates data silos and hinders sharing.
- **Increased security and privacy risks.** IoT devices and systems collect a variety of data from equipment condition to images of people. Some of the data collected require additional levels of protection and treatment, such as medical data, personally identifiable information and other sensitive information. Inadequate data management exposes IoT systems to potential security breaches and privacy violations. Without proper encryption, access controls and data governance policies in place, sensitive information collected by IoT devices may be susceptible to exploitation by malicious actors, leading to reputational damage along with regulatory and legal liabilities.
- **Increased compliance and regulatory risks.** In regulated industries such as healthcare, finance and utilities, organizations must comply with stringent data protection regulations and industry standards. Inadequate data management capabilities can expose organizations to compliance risks, audit failures and regulatory sanctions. Without proper data governance, organizations may struggle to demonstrate compliance with data privacy laws such as GDPR, HIPAA or PCI-DSS, undermining trust and credibility among customers, partners and regulators.
- **Increased operational inefficiencies and costs.** IoT data management is complex and challenging. Poor data management increases operational costs. Organizations may invest

© Strategy of Things, 2025. All rights reserved.

in unnecessary storage, struggle with data integration and face compliance challenges.

One perspective of the future evolution of data management is informed by eight trends identified by data observability software company Monte Carlo.[1572] These trends are:

> Data management supports and complies with increasing regulatory requirements.
>
> Data governance plays a more prominent and integrated role in data management.
>
> Data meshes require that data management support the decentralization of data, with "distributed data products, owned by independent cross-functional teams oriented around data domains."
>
> Decentralization of data requires data access governance that enables "restricting access only to those who need it as well as applying the right security measures and preventing breaches."
>
> Automation of data transformation with no-code tools enabling less technical data professionals to perform these activities.
>
> Increasing need to perform real-time processing of data streams.
>
> AI-based applications to simplify data management.
>
> Observability supports data management systems in understanding the health and state of data.
>
> Extracted from Section 21.3.1.3

Data management technologies are evolving to support the increasing volume and velocity of data generated by IoT. For example, legacy data warehouses store data on servers using traditional Relational Database Management Systems (RDBMS) while modern data warehouses store data in the cloud to store, process and analyze massive amounts of data from multiple sources in various formats.

As IoT devices and systems become distributed, the data are decentralized as not all data are stored in the cloud. Data management systems must be able to seamlessly access all data no matter their location. One area of innovation is data fabrics, an emerging approach that uses a network-based architecture to connect various disparate cloud databases and provides virtual access to massive volumes of data not possible with legacy data warehouses.

While there are extensive industry development efforts and solutions around data management, novel and innovative "beyond big data" data management technologies are needed to facilitate the evolution of IoT and enable a hyperconnected and autonomous economy and society.

Furthermore, the convergence of AI with IoT and the likely pervasiveness in the economy creates a need to accelerate the development of "beyond big data" data management approaches and technologies.

[1572] See note 1417

© Strategy of Things, 2025. All rights reserved.

Given the strategic importance of data management to IoT in enabling powerful AI models and AI-enabled IoT systems, potential opportunities for the federal government to augment and accelerate industry efforts may include:

- **Scalable and efficient data storage.** Innovative and more effective approaches are needed to manage the increasing volumes of data. For example, distributed storage architectures, compression techniques and data deduplication methods to improve storage efficiency.
- **Real-time data processing.** Research into ways to enhance real-time and energy efficient processing of IoT-generated streaming data including advanced algorithms, edge computing and in-memory processing techniques is relevant.
- **Security and privacy.** Research into methods and approaches to protect a diverse set of data that are increasingly stored on distributed devices, mobile and edge systems, as well as data that are streamed to other systems is important. Opportunities to consider include encryption techniques, access control mechanisms and privacy preserving analytics.
- **Data quality assurance methodologies.** Approaches to ensure the accuracy and reliability of IoT-generated data, such as developing calibration techniques for sensors, anomaly detection algorithms and data validation processes are required.
- **Data governance.** Data oversight and management is increasingly important as separate parties own their data which are subject to a variety of industry and government regulations. New approaches and mechanisms are needed to govern changes as data are increasingly distributed and decentralized.
- **Lifecycle management of IoT data.** As new IoT applications emerge and industry adoption increases, the management of the distributed and decentralized data, from attribution, traceability, collection, storage, processing, analysis and archiving becomes more important.
- **Data fabric architectures.** As data sources and creators are increasingly decentralized and distributed on a massive scale, future scalable architectures to interconnect and access this data are required.

23.2.2. Intelligence: AI trust

The use of AI in combination with IoT devices and systems enables users to extract insights from volumes of data. Furthermore, AI models running on IoT devices analyze data streams in real-time, identify patterns, predict outcomes, make intelligent decisions and may take autonomous action without human supervision. AI-driven analytics enable continuous learning and adaptation, allowing IoT systems to evolve and improve over time, leading to more accurate predictions and better resource utilization.

Despite its transformational potential, artificial intelligence faces several challenges that slow its broader adoption and scaling. Our research identified the lack of use of artificial intelligence as a gap in insurance, retail, healthcare and transportation and logistics sectors. AI is also an important capability in agriculture, smart cities and renewable energy.

© Strategy of Things, 2025. All rights reserved.

> In a 2019 survey conducted by LexisNexis Risk Solutions of 300 insurance carrier professionals, 62% of respondents are "applying, piloting or planning AI and ML initiatives." Among these AI/ML adopters, "86% agree it's important to explain to consumers and regulators how AI and ML is used. In addition, 55% are concerned about trust in how analytical models are used, with 26% ranking it as one of their top three concerns. Almost three quarters (71%) of adopters are concerned about bias in AI and ML models." Extracted from Section 6.3.1.

In the healthcare industry there is only modest adoption of AI with less than 5% of healthcare organizations using AI tools. One reason is the lack of transparent and explainable models as discussed earlier in Section 19.3.1.3.

Algorithm predictive capability is another challenge that may lead to inaccurate outcomes. Some applications require AI models to analyze multiple data parameters as well as collect large volumes of data over a long period of time before the model can be considered sufficiently trained.

> In the insurance industry, obtaining enough information so insurers can actually make sound risk decisions is the biggest challenge. It may take years for an insurance company to get enough performance data or loss information from a specific device or a wide range of devices. Extracted from Section 16.3.1.

> "IoT will level the playing field or at least make it much more fair. The complication is you need large datasets in order to provide actuarially sound measurements and risk assessment of this. You have to have robust datasets so you are able to control for the other variables that might actually be out there. You have to have a historical data set to provide the type of modeling that justifies your point of view."
> Ryan Briggs, Vice President, Automotive and Mobility Solutions, Swiss Re. Extracted from Section 16.3.1.

AI trustworthiness is a common concern identified in our research. The outcomes produced may not be explainable, nor fair or ethical, leading to a lack of trust. Some AI models employ "black box" approaches, such as deep learning, that "produce decisions and outcomes that are not easily explained as compared to their less powerful and accurate "white box" counterparts such as linear and decision tree methods."[1573]

[1573] As discussed in Healthcare Section 19.3.1.3

© Strategy of Things, 2025. All rights reserved.

> The models may not always be peer reviewed nor shared with others because of intellectual property concerns. The inability to explain outcomes makes it difficult for physicians, regulators and others to determine whether a model is safe, usable and supports efficacious outcomes. Extracted from Section 19.3.1.3

Another cause of poor algorithm predictive performance is the inability of the IoT device to collect a representative set or enough of the appropriate data, leading to data bias. The biased data may be used to train AI models, which in turn can lead to inaccurate or improper outcomes when the AI models analyze data outside the range of the training set.

In the transportation and logistics industry, our research showed that the "reluctance of the various industry participants to share data creates incomplete data sets used to train the AI models, resulted in algorithmic bias."[1574]

Data privacy concerns, specifically in healthcare, may result in patients withholding data that may be used to develop AI models. This leads to models being trained with less representative sets of data.[1575]

AI trust challenges hinder future functionality and usefulness, adoption, scaling, value realization and delivery in a number of ways including:

- **Poor and limited functionality.** Intelligent IoT systems monitor the cyber-physical environment to create insights and support automated and human-led actions. A system's inability to process, analyze or interpret the data properly or in a timely manner leads to poorly informed conclusions and decisions, incorrect or inappropriate actions and poor and inconsistent results.

  For example, poor data management may lead to low quality data for training AI and machine learning models, resulting in inaccurate or unintended results. IoT devices employing microprocessors that have limited capabilities to execute AI algorithms compromises real-time analysis and limits functional performance.
- **Create poor outcomes that erode user trust.** AI challenges can erode user trust in IoT devices and services. For example, when AI algorithms that use facial recognition camera systems fail to accurately interpret data this can lead to incorrect actions or recommendations that diminishes user confidence.

  At the other extreme, AI algorithms may interpret the surrounding conditions and execute actions that may not be easily explained or justified. This loss of user trust slows adoption of AI-enabled IoT solutions and limits where these solutions are deployed and how much "autonomy" they are given.
- **Create unsafe actions and conditions.** The complexity of IoT environments often necessitates AI models that can adapt to dynamic conditions with a myriad of responses and actions. The AI models may, however, exhibit unexpected or unintended behavior if they encounter scenarios not covered during training.

[1574] As discussed in Transportation and Logistics Section 8.3.1.3

[1575] As discussed in Healthcare Section 9.3.1.3

© Strategy of Things, 2025. All rights reserved.

In other cases, algorithms may be trained with biased datasets, resulting in decisions and actions or lack of actions, which may not be accurate or safe for a given situation. These unsafe conditions and actions may lead to accidents, injury and loss of human life and escalate the potential of greater harm and damages.

- **Hinder automation and limit the value provided to users.** Other technology challenges slow the use of intelligence in IoT systems and limit the ability to monitor and process large volumes of data, analyze and make informed decisions and automate and control processes.

  For example, devices with low power microprocessor chips may not be able to run complex AI algorithms to monitor large scale complex industrial processes in real time. As a result, the IoT systems may be relegated to simple functions or operations, such as monitoring and reporting on operational conditions, while processing and analysis is done off-device later.

  In other cases, where there is an inability to use IoT systems to monitor and automate operations, human intervention is required. This slows down the processes and increases operational costs.
- **Hinder the future development of "smarter" IoT.** For IoT to support growth and autonomous operations and applications, its intelligent capabilities must continue to develop. Future applications, such as IoT device swarms, which are clusters of more than 100 IoT devices that operate collectively as one to perform certain tasks, but with each device operating individually, require autonomous operating capabilities. The inability to address these gaps will prevent existing and future IoT technologies and applications from developing.

AI trust challenges are complex and involve multidisciplinary factors. These challenges, however, must be addressed before AI can be adopted in a broader way with IoT. At an aggregate level, our research identified some representative AI opportunities for the federal government to facilitate its scaling and usage in IoT. These include:

- **Development of ethical AI algorithms.** The convergence of AI with IoT enables fully autonomous operations, rapid responses to complex incidents without human intervention and augmentation of humans in high skilled operations. The use of AI in IoT, however, raises questions of fairness, privacy, ethics, maleficence, accountability and transparency.

> For example, AI algorithms can yield inaccurate results for certain demographic groups. A study conducted through NIST's Face Recognition Vendor Test program of 189 algorithms from 99 developers found higher rate of false positives for Asian and African American faces, compared with Caucasian faces. Extracted from Section 17.3.1.2

The use of AI based facial recognition camera systems may lead to improper conclusions and actions against certain demographic groups. And AI algorithms for autonomous vehicles can potentially follow a different set of actions based on the country that trained

© Strategy of Things, 2025. All rights reserved.

the system.

For example, a machine ethics survey of 2.3 million people from 233 countries and territories, published in Nature magazine, found that moral principles guiding a driver's decision vary by country.[1576] Respondents were posed with 13 scenarios in which someone's death was inevitable and asked to choose who to spare in situations that involved a mix of variables: young or old, rich or poor, more or fewer people. In countries with strong government institutions, drivers were more likely to hit people who were crossing the road illegally than in nations with weaker government institutions. In countries with significant gaps between rich and poor, drivers chose to kill lower status persons more than those in countries with less significant gaps.

The Pew Research Center and the Elon University Imagining the Internet Center posed a question to 602 technology innovators, developers, business and policy leaders, researchers and activists:[1577]

By 2030, will most of the AI systems being used by organizations of all sorts employ ethical principles focused primarily on the public good?

Over two-thirds (68%) selected the option stating that organizations will not be employing ethical principles in AI systems.

Creating ethical AI algorithms is complex and involves multiple technical and non-technical disciplines. Continued research, development and innovation to address some of the key challenges is necessary for the continued and widespread adoption of AI in IoT.

- **Explainable AI tools and processes.** For AI controlled operations to be trusted and adopted at scale, its users must be able to understand and assess the AI algorithm's decision-making processes, its alignment and precision to target outcomes under a variety of planned and unplanned conditions and its consistency in creating and acting on the outcomes. Users may want this understanding to gain confidence, reduce liability risks from unintended consequences and to comply with regulations.

  Explainable AI is defined as the "set of processes and methods that allows human users to comprehend and trust the results and output created by machine learning algorithms."[1578] Continued research in the design, development and deployment of innovative tools and operations is needed to overcome some of the challenges facing explainable AI, including evaluation metrics, scalability, model suitability,

[1576] "Self-Driving Car Dilemmas Reveal That Moral Choices Are Not Universal", A. Maxmen, Nature, October 24, 2018. Link

[1577] "Experts Doubt Ethical AI Design Will Be Broadly Adopted as the Norm Within the Next Decade," L. Rainie, J. Anderson, E. Vogels, Pew Research Center, June 16, 2021. Link.

[1578] "What is Explainable AI?", V. Turri, Software Engineering Institute, Carnegie Mellon University, January 17, 2022. Link

© Strategy of Things, 2025. All rights reserved.

interpretability and explanation communications.[1579]

23.2.3. Intelligence: Intelligent device capabilities

On-device and edge processing of data are increasingly common and are needed for applications that are autonomous, latency sensitive or operate in an area with unreliable service. Other edge applications include IoT device swarms and ambient IoT use cases that require contextual information from other nearby devices.

Our research has identified intelligent device capabilities to support intelligent IoT as a top challenge in both agriculture and smart cities. Edge computing remains, however, a critical enabler in industries where AI-enabled applications are used. This includes healthcare, transportation and logistics and renewable energy.

Challenges in intelligent devices that slow adoption, scaling and value realization include:

- **Inability to perform complex tasks and operations:** IoT devices are resource-constrained and lack the computational, storage and power capacity to perform complex tasks and applications. On-device processing is limited to simple tasks and those that are supported by the processor's capabilities. This performance limitation restricts what some IoT devices can do functionally and how and where they can be used. For example, battery powered IoT devices are limited to transmitting small amounts of data, such as equipment condition data on an infrequent basis.
- **Increased complexity and costs:** Technical challenges in IoT edge computing significantly increase both the complexity and costs associated with IoT deployments and maintenance. These limitations require specialized hardware and software optimizations to process data efficiently at the edge, which can increase infrastructure and development costs.

  Furthermore, ensuring real-time data processing, security and scalability across diverse edge devices complicates system management, leading to higher operational costs. The devices may not be able to handle increasing data loads or support additional devices, leading to performance bottlenecks and degraded user outcomes.
- **Increased security risks:** Edge devices often lack robust security measures such as encryption and advanced firewalls due to resource limitations, making them vulnerable to attacks such as malware infiltration or data breaches. For example, hackers gained access to a casino's network by hacking into an Internet connected aquarium thermometer in the casino's lobby.[1580]

  Inadequate security features compromise data privacy, integrity and system reliability, undermining trust in IoT solutions and hindering their adoption.

[1579] "Explainable AI (XAI): A Systematic Meta-Survey of Current Challenges and Future Opportunities", W. Saeed and C. Omlin, November 11, 2021. Link

[1580] "Casino Gets Hacked Through Its Internet-Connected Fish Tank Thermometer," W. Wei, The Hacker News, April 16, 2018. Link

© Strategy of Things, 2025. All rights reserved.

- **Increased energy consumption:** As IoT devices and edge servers are deployed in increasing numbers, particularly those systems that run complex applications and cannot be powered by batteries, the amount and cost of electricity to power these systems increases. The need for constant power to support data processing, storage and communication at the edge increases operational costs making IoT solutions less sustainable and economically feasible.

  This issue is particularly pronounced in remote locations or in industries with energy constraints, where high consumption strains resources and complicates scaling efforts. The increased energy demands also limits battery-powered IoT devices, reducing their efficiency and lifespan.

While there are existing industry development efforts and solutions for the development of intelligent devices, these efforts are focused on short term objectives. To enable and support a future scaled up, hyperconnected and autonomous IoT ecosystem, the federal government would do well to focus on research and commercialization of innovative IoT technologies. A representative set of innovation areas include:

- **Increase device processing capabilities.** As more IoT applications shift to the edge, the complexity and intensity of the workloads processed is expected to increase. For example, IoT applications that need real time sensor fusion or AI enabled systems require substantial edge processing abilities. Processor development for edge applications, regardless of whether that processing occurs on the devices or on servers, must continue to increase their ability to support complex and process intensive workloads.[1581]

  Neuromorphic processing, inspired by the brain's architecture, offers significant research and innovation opportunities for IoT.[1582] By mimicking neural networks, neuromorphic chips can process data more efficiently and with lower power consumption compared to traditional processors. One area of opportunity for neuromorphic processing is in industrial radar applications.[1583] This advance is particularly beneficial for IoT devices, which often operate under power constraints and require real-time data processing at the edge.

  Innovations in neuromorphic computing can lead to smarter, more autonomous IoT systems capable of complex decision-making and adaptive learning, enhancing applications in areas such as smart cities, healthcare and industrial automation.
- **Reduce power consumption of microprocessors.** Smarter IoT devices incorporate more capable microprocessors and microcontrollers. More capable processors, however, consume more power. In many cases, the power supplied for these IoT devices is from

[1581] "Intel Thinks IoT Devices Are Going to Get a Lot More Powerful", A. Braun, IoT Tech Trends, April 10, 2019. Link

[1582] "Neuromorphic computing: The future of IoT," H. Joshi, Financial Express, March 3, 2024. Link

[1583] "NeuroRadar: A Neuromorphic Radar Sensor for Low-Power IoT Systems," K. Zheng, K. Qian, et. al. SenSys '23: Proceedings of the 21st ACM Conference on Embedded Networked Sensor Systems. Pages 223 – 236. Link

© Strategy of Things, 2025. All rights reserved.

batteries. Low power AI capable processors that can operate on battery operated devices[1584] must be developed to support both current and future needs.

- **Develop energy harvesting technologies.** Battery powered IoT devices have a limited lifetime. With billions of IoT devices to be deployed, replacing those batteries is neither realistic nor practical. For example, replacing batteries on thousands of soil moisture sensors on farm fields.

  In addition, disposal of billions of batteries is a looming environmental waste issue. Energy harvesting technologies can augment or replace batteries in IoT devices.[1585] While today's energy harvesting technologies are limited to augmenting battery life in select IoT applications, developments could yield solutions that remove the need for batteries.
- **Development of AI algorithms capable of running on resource constrained IoT devices.** Research in the development of algorithms that can operate on resource constrained devices is critical to the creation of new applications and scaling of IoT.

  For example, Tiny Machine Learning, or TinyML, is a subset field of machine learning that incorporates techniques and methods to run and operate algorithms specifically on resource constrained devices such as microcontrollers.[1586] This increases the functionalities and capabilities of IoT applications running on these devices.

  Research into the development of more computationally efficient algorithms also benefits edge and cloud data centers. The energy consumed by high power processors and servers running computationally intensive AI models is significant. The development of more efficient algorithms that run on these servers provides opportunities for energy and cost savings. As the adoption and deployment of AI-enabled IoT systems increase, the energy savings are likely to become significant.

23.3. Hyper-Deployed gaps

An IoT-enabled economy and society, teeming with billions of interconnected devices working autonomously and collaboratively across industries and communities, is a vision enabled by the evolution of the Internet of Things as described in Sections 22.1.3 and 22.1.4

The current IoT technology infrastructure, however, is not ready to support such a massive, complex ecosystem. For example, existing networks are already challenged to detect, manage and mitigate security threats, but to do so effectively in a future network infrastructure with billions of new devices requires a new paradigm of an adaptive, autonomous self-defending, self-healing network. Similarly, the AI-enabled decisions and outcomes created by IoT devices today

[1584] "Designing Ultra Low Power AI Processors", A. Mutschler, Semiconductor Engineering, April 9, 2020. Link

[1585] "Energy Harvesting Starting to Gain Traction", J. Koon, Semiconductor Engineering, April 18, 2022. Link

[1586] "What is Tiny ML and Why Does It Matter?", J. Riberio, December 22, 2020. Link

© Strategy of Things, 2025. All rights reserved.

experience issues with accuracy, explainability and trust. These issues must be fully resolved in a future economy and society reliant on autonomous and connected devices and systems.

The envisioned future "hyper-deployed IoT" economy and society require a technological infrastructure different from the current structures. This infrastructure must support billions of heterogeneous connected IoT devices and systems reliably and predictably. It must allow for the seamless exchange of data and information and do so such that it can be made available and acted upon in a timely manner. It must support an economy where intelligent autonomous systems and human AI collaboration are the norm. It must protect against a variety of known and yet to be discovered future cybersecurity threats and autonomously contain and mitigate the impact of these threats. The algorithms used to analyze and act on the collected data must do so in a way that is accurate, fair and explainable.

Our inability to develop and deploy the technologies enabling this future infrastructure hinders the IoT functionality and usefulness, adoption, scaling, value realization and delivery in a number of ways including:

- **Slows IoT evolution.** Existing technologies may be based on legacy approaches that are technologically obsolete, designed for a different set of requirements and capabilities and cannot extend to support future needs or are nearing end of life. Without the foresight and fundamental research to develop future technologies, IoT applications and systems are "stuck" at current levels and cannot innovate or evolve.
- **Limits the number of devices connected and what they can do.** The IoT ecosystem is comprised of heterogeneous devices and systems that impose unique requirements and complex needs on the supporting technology infrastructure. These systems have varying bandwidth requirements. Some have specific latency requirements while other applications require high processing power. The inability of the infrastructure to support this variety of conflicting requirements prevents users from adopting and integrating IoT devices and systems. In other cases, users may limit how many and what types of devices are connected to address performance and reliability issues.
- **Hinders the economy-wide and society-wide realization of benefits.** IoT-enabled systems, such as those in smart cities and supply chains, require "network effects" (i.e., scale of users) to create value. More users leads to more connected systems and data which leads to more value.

  For example, future smart cities may be comprised of thousands of unique IoT applications and systems working together to create daily outcomes for residents and businesses. Future generation IoT technology infrastructure is necessary to support the deployment and operation of billions of IoT devices across the economy and society. Without these advances, the number of devices and systems integrated and operated is limited, leading to limited benefits and suboptimal value provided.

Substantial investments in research and development are needed to enable the advances required for an infrastructure capable of supporting this number of devices. While industry participants conduct a variety of research and development efforts on key technologies, they are not well

© Strategy of Things, 2025. All rights reserved.

suited to bring about these advances in future generation infrastructure. Much of the industry's efforts are focused on extending their current technology investments and intellectual property portfolios. These efforts are focused on driving incremental advances to meet existing market needs, extending the functionality and capability of existing investments in IoT technologies with short term return on investment potential.

This mentality is echoed in the 1997 book by Professor Clayton Christensen ,"The Innovator's Dilemma: When New Technologies Cause Great Companies to Fail", which surmises that "the next generation product is not being built for the incumbent's customer set and this large customer set is not interested in the new innovation and keeps demanding more innovation with the incumbent product."[1587] Although innovative start-up companies may offer novel approaches, their efforts are focused on well-defined near-term market needs to generate the revenue they need to survive.

Because of this, the federal government plays a significant role in developing and supporting the research and facilitating the advances that will lead to an appropriate IoT technology infrastructure. Some of this research is fundamental and explores uncharted topics beyond the immediate commercial interests of industry. Other research may be high risk and involve novel approaches that demand substantial financial backing, a long-term perspective and have uncertain outcomes.

To support the continued evolution, scaling and full realization of the value created by IoT described in the evolution framework in Figure 22-1, this report has identified several critical technology areas for further research and innovation. Each of these is discussed below.

23.3.1. Hyper-Deployed: Enabling an IoT data ecosystem

One of the foundations of the future digital economy and society is the massive volumes of data generated by billions of smart devices and IoT-enabled systems. These data are distributed and decentralized as it is produced, consumed, stored and managed on fixed and mobile devices and on edge devices as well as on servers and cloud data centers.

The data are owned, used and managed by a variety of parties, including individuals, business organizations, cities and communities along with government agencies. These data may be proprietary or public and may be used exclusively by the data owner or may be monetized and shared with others to realize benefits and outcomes.

The future IoT data ecosystem is envisioned to be a highly interconnected network where data generated by IoT devices and systems is seamlessly shared, monetized and utilized across various sectors. An IoT data ecosystem is needed to support this digital economy and society. One of the key features of this ecosystem is its decentralized nature, allowing data to be processed and analyzed closer to where it is generated, thus reducing latency and improving efficiency.

The European Union's (EU) European Data Strategy aims to create a robust data ecosystem by establishing a single market for data, ensuring that data flows freely and securely across sectors

[1587] "The Innovator's Dilemma", Wikipedia. Link

© Strategy of Things, 2025. All rights reserved.

and member states.[1588]This strategy offers valuable insights into how the United Sates can approach the creation of its own IoT data ecosystem.

The strategy is based on creating common data spaces, which share common data infrastructures and governance frameworks that facilitate data pooling, access and sharing. These data spaces make more data available for economic and societal use while keeping control in the hands of the data generators. Initial data spaces include agriculture, energy, health, manufacturing, mobility (transportation) and nine other economic areas.[1589]

In the United States, efforts like the National Institute of Standards and Technology's (NIST) Smart Grid Interoperability Framework show the way for a more integrated IoT data ecosystem for energy areas. [1590]This framework focuses on ensuring interoperability and security in the smart grid. By establishing standards and guidelines, NIST aims to create a cohesive environment where data from various sources can be integrated and utilized.

To support an effective IoT ecosystem, an advanced cloud, edge and IoT infrastructure that can manage the unique requirements of IoT data is necessary. The European Cloud, Edge IoT Continuum provides a model for how this infrastructure can be designed to support seamless data processing across different layers.[1591] Such a continuum would ensure that data are processed efficiently, balancing the centralized capabilities of cloud computing with the low-latency advantages of edge computing.

There are, however, a number of technical challenges to building such an IoT data ecosystem. One of the primary challenges is ensuring data quality and interoperability. With data being generated by a multitude of devices and systems, maintaining consistent data quality and ensuring that different data sources can seamlessly interact with each other are crucial. Additionally, data privacy and security concerns must be addressed as the sharing and monetization of data can expose sensitive information to risks.

Data sovereignty is an important challenge that ensures that the information produced within the country is retained by its owners and protected from external threats while fostering domestic innovation. In addition, the volume of data generated by IoT devices poses scalability issues. Efficiently storing, processing and analyzing these data require significant computational resources and innovative solutions.

The lack of universally accepted standards for IoT data management and integration slows the development of a cohesive ecosystem and additional research is needed to address these data ecosystem challenges.

23.3.2. Hyper-Deployed: Communications and network infrastructure

[1588] "European Data Strategy," European Commission. Link

[1589] "Common European Data Spaces," European Commission, updated July 3, 2024. Link

[1590] "NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 4.0", A. Gopstein, C. Nguyen, et al., U.S. National Institute of Standards and Technology, July 2020. Link

[1591] "The European Cloud, Edge and IoT Continuum Initiative," Cloud, Edge and IoT (CEI) Continuum. Link

© Strategy of Things, 2025. All rights reserved.

Research firm IDC estimated that by 2025, there will be 55.9 billion IoT devices generating 79.4 zettabytes (ZB) of data.[1592] For comparison purposes, 1 ZB represents 30 billion 4K movies.[1593] While a large portion of the data will be video, other IoT data producers include industrial, automotive, navigation, household, wearables, medical and industry terminals such as ATMs, point of sale and ticketing along with gaming, augmented and virtual reality and RFID readers.[1594]

The traffic from these IoT devices ranges from small bits of data on a periodic basis to continuous streams of high bandwidth video traffic. The network must be able to support devices of all types, brands and models and variations of those models. Current communication networks and architectures are not designed to manage the needs of IoT at scale.

Some IoT data are time sensitive and must be acted upon immediately, while other data are stored for future analysis. Some data that support critical applications, such as public safety and require a reliable communication network.

To support time-sensitive and critical applications, some data are processed in servers integrated into the network near the point of use (edge) and in vehicles (mobile edge), while other data are sent to remote data centers (cloud). In addition, the network infrastructure must be resilient against cyberattacks, introduced through known and undiscovered vulnerabilities from the IoT devices.

New processes and technologies for configuring, managing, operating and maintaining the hyperconnected network will be necessary. For example, automation will evolve to autonomous maintenance and operations with the use of AI technologies that support network operations.[1595] Continuous innovation is required to address communications network scaling and operation challenges. Some representative areas for innovation include:

- Spectrum sharing and management
- Network infrastructure to support AI and complex IoT applications
- Fault tolerant and resilient network infrastructure
- Self-defending adaptive network security
- Management of the distributed IoT network at scale
- Optimizing and maintaining performance and Quality of Service under continuously varying conditions
- Improving middleware to support scaling

[1592] "How You Contribute to Today's Growing DataSphere and Its Enterprise Impact," D. Reinsel, IDC Blog, November 4, 2019. Link

[1593] "Seagate Is the First Company to Ship 3 Zettabytes of Hard Drive Storage," M. Humphries, PC Mag, April 8, 2021. Link

[1594] "How You Contribute to Today's Growing Datasphere and its Enterprise Impact," D. Reinsel, IDC Blog, November 4, 2019. Link

[1595] "How AI is Changing the Role of Network Managers and Teams", J. Edwards, Network Computing, July 15, 2021. Link

© Strategy of Things, 2025. All rights reserved.

Each of these is discussed below.

23.3.2.1. Spectrum sharing and management.

There is a finite amount of wireless spectrum available for IoT applications. In dense urban environments, this can become problematic as the number of IoT devices scales up and data traffic volumes grow, leading to network congestion and radio frequency interference.

Spectrum sharing techniques, such as that implemented in the Citizens Band Radio Service (CBRS) for the narrow band within the 3.5 GHz band, is one approach that facilitates the shared use of the spectrum. Another technique is cognitive radio, an approach that enables IoT devices to sense the spectrum usage of surrounding users, determine what unused spectrum exists and connect and communicate through the available spectrum. Managing these "transactional" connections at scale with traditional models is not possible. Innovation and development of AI and ML algorithms is vital to support the administration, billing, resource management and operation of IoT devices in increasingly complex scenarios.[1596]

23.3.2.2. Network infrastructure to support AI and complex IoT applications

A 2021 survey of 211 data scientists, AI/ML practitioners and systems architects revealed that 42% of respondents reported challenges with their companies' AI infrastructure and compute capacity.[1597] This is not surprising as AI and autonomous IoT applications impose high performance requirements for communications networks. These requirements include:

- **High throughput, low latency.**[1598] AI models analyze large amounts of data sourced from sensors and devices. For example, algorithms trained and deployed for use ("inference models") stream and process the data from a variety of sensors, often in real time, for immediate action.
- **Distributed computing resources.** Depending on the application, processing for AI applications is performed in cloud data centers, near the point of data collection (edge) or on the device. In other cases, AI models may be distributed to multiple nodes over the network for processing. These nodes may collaborate with each other to add processing resources and to improve model accuracy.[1599] Network infrastructure supporting AI applications may incorporate network fabrics that are flexible and composable, instead of rigid point-to-point architectures.
- **Scalability of resources.** Compared to traditional IT workloads processing static and structured data, AI workloads process "free flowing" data that can be structured and

[1596] "Spectrum Sharing Schemes from 4G to 5G and Beyond: Protocol Flow, Regulation, Ecosystem, Economic", M. Parvini et al., IEEE Open Journal of Communications Society, 10.1109/OJCOMS.2023.3238569, February 15, 2023. Link

[1597] "Run:AI State of AI Infrastructure Survey 2021," Run:AI blog, Run:AI, October 26, 2021. Link

[1598] "High-Performance Networking to Support Critical Workloads for AI and ML", M. Pierce, Redapt blog, July 16, 2020. Link

[1599] "What is Distributed AI?", W. Chong et al, IBM, December 8, 2021. Link

© Strategy of Things, 2025. All rights reserved.

unstructured and that are computationally intensive and dynamic in nature.[1600] The dynamic nature of the AI workloads requires the scaling of compute resources from the existing node or from nearby nodes.

- **High performance computing.** Complex AI workloads require parallel processing of multiple tasks on multiple servers. These servers are often networked together to form High Performance Computing (HPC) clusters, containing 100,000 servers or more. HPC clusters require specialized hardware capable of high bandwidth, low latency operations for networking, memory, storage and file systems.[1601]

AI and autonomous IoT applications impose challenges on the communications network infrastructure. Further research and innovation are necessary to develop the network to meet these needs. Example areas of needed continued research include network interconnect architectures to support scalability and high bandwidth needs,[1602] computation offloading to edge and mobile edge to address resource and latency needs,[1603] transport designs for distributed AI training[1604] and AI workload and network joint optimization for resource allocation.

23.3.2.3. Fault tolerant and resilient network infrastructure

The ability of the network infrastructure to tolerate faults, remain functional and resilient is critical to the operation of IoT applications that are expected to last for years. As additional IoT devices with varying levels of quality and performance levels are integrated into the network, they introduce operating conditions and faults that could disrupt operations.

These conditions and faults affect the operations that the IoT application is managing and could potentially spread to other processes through a chain of cascading failures. Even if detected immediately, it is not always possible to repair the fault or to do so in a timely manner. For example, in a continuous production environment for chemical processing, repairs can only be made during infrequent planned downtimes. In other cases, the IoT devices may be in remote areas that are not easily accessible or it may be economically unfeasible to replace a unit.

Systems resilience, a key capability of sustainable IoT networks, is accomplished through a combination of design and functional redundancy, fault tolerance and operational adaptation. For example, some devices contain software written in “safe” programming languages[1605] and developed using rigorous software development methodologies, while others may not be as conscientiously developed.

During operation, some devices may be capable of tolerating errors, while others propagate errors. Some devices are operating with the latest firmware updates, while others are running

---

[1600] “How AI Will Change Network Infrastructure,” A. Cole, Enterprise Networking Planet, October 25, 2018. Link

[1601] “What is High Performance Computing (HPC)?”, IBM. Link

[1602] “Interconnection Networks”, ScienceDirect. Link

[1603] “Computation Offloading”, ScienceDirect. Link

[1604] “Meta Launches New Research Award Opportunity in Networking for AI at NSDI 2022”, Meta Research, April 5, 2022. Link

[1605] “Memory Safe Programming Languages Are on the Rise. Here's How Developers Should Respond”, l. tung, ZDNET, January 25, 2023. Link

© Strategy of Things, 2025. All rights reserved.

outdated versions or cannot be patched. Finally, the IoT devices may be operating in networks that may be outdated, misconfigured or incompatible.

Despite these potential issues, the networks the IoT devices operate in is expected to be reliable, stable, scalable, predictable and resilient. The resilient network must be able to defend, detect, remediate and recover from faults. It must also be able to then further diagnose and refine its responses to fault conditions.[1606]

The need for reliability and stability requires the communications networks to support heterogeneity in both the device quality and the network configurations, be adaptive to the actual state of resources on the device, support the specific device reliability requirement and the current state of the operating physical environment for the device.

A key areas of research to develop and refine the methodologies considers algorithms and tools to detect and recover from the various failure mechanisms, such as correlated failures, unpredictable failures, debugging failures and human caused errors.[1607]

Other areas of research include understanding and integrating the role of context or situational awareness in detecting and diagnosing faults, the role of people in the specification and design of resilient systems and the use of network function virtualization in resilient systems.[1608]

Finally, the integration of autonomic network management (self-configuration, self-healing, self-optimization, self-protection) with Software Defined Networking (SDN) is another area for further innovation and development.[1609] As IoT networks continue to grow in size and become more complex, continued research into the development of existing and innovative approaches, including those that employ Service-Oriented Architecture (SOA)[1610] and AI[1611] is necessary to ensure future systems resilience.

23.3.2.4. Self-defending adaptive network security

IoT devices introduce new attack surfaces that can be exploited to breach the network. A 2021 blog for cybersecurity professionals, Kratikal, stated that IoT devices suffered 5,200 cyberattacks a month.[1612] With the number of IoT devices expected to scale to 55.9 billion by 2025, the number of cyberattacks are expected to grow. This is exacerbated by the rise of AI facilitated

---

[1606] "Architecture and Design for Resilient Networked Systems," D. Hutchison and James P.G. Sterbenz, Computer Communications, Volume 131, 2018, Pages 13-21, ISSN 0140-3664. Link

[1607] "New Frontiers in IoT: Networking, Systems, Reliability and Security Challenges", S. Bagchi et al, DOI 10.1109/JIOT.2020.3007690, IEEE Internet of Things Journal. Link

[1608] "Architecture and Design for Resilient Networked Systems," D. Hutchison and James P.G. Sterbenz, Computer Communications, Volume 131, 2018, Pages 13-21, ISSN 0140-3664. Link

[1609] "Self-healing and SDN: Bridging the gap", L. Ochoa-Aday et al, Digital Communications and Networks, Volume 6, Issue 3, 2020, Pages 354-368, ISSN 2352-8648. Link

[1610] Zhou, S. (2015). Supporting Fault Tolerance in the Internet of Things. UC Irvine. ProQuest ID: Zhou_uci_0030D_13722. Merritt ID: ark:/13030/m5cc5mzg. Link

[1611] "Design and Implementation of Fault Tolerance Technique for Internet of Things (IoT)," 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), 2020, pp. 154-159, doi: 10.1109/CICN49253.2020.9242553, S. Kumar, P. Ranjan, P. Singh and M. R. Tripathy. Link

[1612] "Cyber Threats Haunting IoT Devices in 2021", D. Meharchandani, Kratikal blog, September 21, 2021. Link

© Strategy of Things, 2025. All rights reserved.

cyberattacks.[1613] The ability to detect, mitigate and recover from this number of cyberattacks using existing approaches and tools is untenable. New innovative approaches and solutions are needed.

One such potential innovative approach is the self-defending adaptive network. A self-defending and adaptive network "defends itself from security breaches. It is a system that knows and recognizes the level of threat faced by an intrusion across a network. It uses a new method of machine learning to track threats, which can include ransomware, code hijackers, intrusion and illegal entry, theft and unauthorized use. Such a network uses a set of modules that can be added or removed to operate and achieve specified goals. It can change its behavior by modifying network devices."[1614]

To be successful, self-defending and adaptive networks must "be effective in an unstructured, unstable, rapidly changing, chaotic, adversarial environments; able to learn in real-time and under extreme time constraints, using only a few observations that are potentially erroneous, of uncertain accuracy and meaning, or even intentionally misleading and deceptive." [1615] Continued areas of research and innovation are needed in three enabling areas:

- Software control that enables adaptive operations, including the creation and deployment of network services.
- Programmable infrastructure that combines software, cloud native virtual network functions with the hardware to respond to changing needs.
- Algorithms that process the data streams and provide the necessary analysis and insights which is used by the software and programmable infrastructure to take the appropriate actions.[1616]

23.3.2.5. Management of the distributed IoT network at scale

With billions of devices, routers and servers of all types soon operating in a multi-layer architectural environment, the professional's ability to monitor, manage, operate and support this infrastructure over its life cycle is a complex undertaking.[1617] In addition to the hardware, managing the software that the hardware operates is equally complex. While automation of the management tasks is a necessity, the scale of massive IoT networks and distributed nature of the heterogeneous devices and components adds complexity. New models, approaches and tools to manage, orchestrate, automate and support resources, activities and schedules are critical.

[1613] "FBI Warns of Increasing Threat of Cyber Criminals Utilizing Artificial Intelligence," Federal Bureau of Investigation, May 8, 2024. Link

[1614] "What are Self-Aware and Self-Defending Adaptive Networks?", B. Kommadi, Open Source for U, November 3, 2021. Link

[1615] "Intelligent Autonomous Agents are Key to Cyber Defense of the Future Army Networks," A. Kott, U.S. Army Research Laboratory, pre-print version of the article appearing in the the Cyber Defense Review journal, Fall 2018. Link

[1616] See note 1614.

[1617] "Edge Management: The Next Big IoT Challenge", J. White, Embedded Computing Design, April 19, 2021. Link

© Strategy of Things, 2025. All rights reserved.

23.3.2.6. Optimizing and maintaining performance and Quality of Service under continuously varying conditions

The network operator and data center's ability to detect workload demand and allocate appropriate resources to collect, process and store the data, whether on a scheduled or dynamic basis, is crucial to IoT performance. This is made more complex by the addition of new devices of varying capabilities to the environment. These devices may consume existing resources, drop in and out of the network (e.g., mobile devices, etc.) and have varying resource demands and availability. Advanced resource allocation algorithms and methodologies must continually be developed to support the rapidly scaling IoT environment.

23.3.2.7. Improving middleware to support scaling

The IoT operational environment is characterized by diverse devices connecting to each other and on-premise, edge and cloud servers through a variety of communications protocols and exchanging data in a variety of formats. Some of the data are processed on the device, while other data are processed on the gateway and on servers in remote data centers. As more IoT devices are added to the network of the future, the ability of these devices to be integrated into the network and interoperate with existing and older devices and systems is critical to scaling.

Middleware, the software that sits between increasingly diverse and heterogeneous devices and applications and allows them to communicate with each other, is essential to the integration and scaling of IoT networks. Middleware, however, must also evolve to support future IoT infrastructure needs.

For example, the middleware must reside in the cloud as well as on resource constrained edge gateways and devices. The middleware of the future must support development of context specific applications for new types of devices, dynamically discover and connect to new devices and services that can come online and leave at any time and ensure the security and privacy of the connected devices.[1618]

23.3.3. Hyper-Deployed: Advanced computing paradigms

Complexity grows as the number of deployed IoT devices increases. To support all these devices and their unique requirements, the initial device to cloud architecture is quickly evolving to a multi-layer distributed architecture of cloud data centers, local edge servers, processors in routers and gateways and fixed and mobile (e.g., cars and drones) devices.

There is no "one size fits all" architecture and the requirements of the specific IoT applications will determine what architecture works best. For example, applications that are latency sensitive or operate in an area with unreliable connectivity service may process data on the device or on a nearby edge server. Applications with large number of devices may aggregate and process the collected data in local gateways, instead of sending the data to a remote cloud data. Applications, such as IoT device swarms, requiring contextual information for processing may obtain that information by connecting and communicating directly with other nearby devices.

[1618] "IoT Middleware: A Survey on Issues and Enabling Technologies", IEEE Internet of Things Journal. PP. 1-1. 10.1109/JIOT.2016.2615180, Ngu, Anne & Gutierrez, Mario & Metsis, Vangelis & Nepal, Surya & Sheng, Quan. (2016). Link

© Strategy of Things, 2025. All rights reserved.

IoT operates in an expansive ecosystem of interconnected heterogenous devices collecting, processing and exchanging data in real-time across the economy and society. It integrates several computing paradigms, including distributed computing, context-aware computing and swarm intelligence, to create intelligent and adaptive systems. These paradigms form the core of IoT architectures, but as this field continues to expand, several open research challenges need to be addressed to fully realize their potential.

The interplay between distributed computing, context-aware computing and swarm intelligence drives the development of intelligent IoT systems capable of handling complex, dynamic environments. Distributed computing provides the infrastructure for these systems to scale, while context-aware computing enables them to adapt to real-time environmental data. Swarm intelligence offers a decentralized approach to collaboration, allowing large networks of IoT devices to work together without centralized oversight.

The combined use of these paradigms holds significant promise for the future of IoT. In smart cities, they can work together to enhance urban infrastructure, improve public safety and reduce environmental impact. In industrial IoT, they can optimize manufacturing processes, predictive maintenance and supply chain management. As technology advances, the integration of distributed computing, context-aware computing and swarm intelligence will continue to drive innovation and efficiency in IoT systems.

23.3.3.1. Distributed computing

Distributed computing provides the backbone of IoT, allowing devices across vast networks to share workloads, process data in parallel and maintain robust system functionality even when individual nodes fail. By spreading tasks across a network of interconnected devices, distributed computing enhances scalability, performance and resilience in IoT applications.

A number of challenges exist for distributed computing, including resource allocation and management, fault tolerance and reliability and latent and real-time processing. These were briefly discussed in Section 23.3.2. Representative areas of potential innovation for distributed computing in IoT were highlighted in Section 17.3.1.3 for smart cities. These are intelligent caching (positioning and storage of content and data on the network to alleviate traffic congestion and latency issues), collaborative edge computing (sharing of computing tasks and resources with nearby edge servers) and cooperative and sustainable load balancing (balancing of workload between servers to avoid performance issues, excessive energy usage and high operating costs).

23.3.3.2. Context-aware computing

Context-aware computing empowers IoT systems to adapt their behavior based on real-time environmental and user-specific information. By leveraging data from sensors and devices, context-aware systems optimize operations and offer personalized responses to dynamic conditions. This adaptability is crucial for creating intelligent systems in smart homes, cities, healthcare and industrial automation.

Section 17.3.1.2 discussed one specific example of the application of context-aware computing in a smart city, the concept of context aware privacy. In this discussion, context-aware privacy considers the location, environment and situation to adjust how smart city IoT systems collect, process and share information. Context-aware systems perform a series of functions, including

© Strategy of Things, 2025. All rights reserved.

context acquisition (collecting data from sensors and systems), context representation (transforming the collected data into a standardized format for sharing), context storage (store data for use over its lifecycle), context interpretation (determine high level situational context from data) and context adaptation (respond based on the context).[1619] Opportunities for further research and innovation in context-aware computing include:[1620]

- **Context definition.** Frameworks for identifying parameters determining and defining a situation or context.
- **Context-aware models.** Context-aware architectures, standards and tools.
- **Sensing context data**. Devices for sensing and collecting data about the environment.
- **Predicting context**. Techniques to predict context based on the data collected and the defined context.
- **Representing and storing context information**. Standardized approaches to facilitate context interpretation and context sharing.
- **Information inferring context and adapting system behavior**. Interpret context and adapt responsive behavior and systems.
- **Evaluation of context aware systems**. Criteria and measures for quality control and end-user satisfaction of context-aware products.
- **Privacy control.** Protection of contextual information collected from participating entities.

23.3.3.3. Swarm intelligence

As IoT adoption scales and the number of devices grows, IoT will transition from devices working individually to create individual outcomes to a collection of IoT devices working together to create an overall outcome. Information from one device will be communicated locally to another device, where it will be processed to take a certain course of action. These IoT swarms may act independently of people in the background or may act collaboratively with people in various ways.

Each IoT device may be acting on its own, performing its individual tasks, but collectively, the devices will be acting with an intelligence that transcends the intelligence of each device. The United States Department of Defense successfully demonstrated a swarm of 106 inexpensive micro-drones for missions that would have been performed by a small number of large expensive drones.[1621] The individual micro-drones were not pre-programmed, but together functioned as a system and demonstrated collective decision making, adaptive flying formation and self-healing.

Key benefits of these intelligent swarm IoT systems include robustness against individual failures, the ability to be self-organizing instead of predefined, adaptive to changes and

[1619] See note 757

[1620] See note 757

[1621] "Department of Defense Announces Successful Micro-Drone Demonstration", United States DoD Press Release, January 9, 2017. Link

© Strategy of Things, 2025. All rights reserved.

decentralized control.[1622] Collective intelligence is a new technology and is immature at this time. Some challenges and gaps that need to be addressed include the development of higher processing capability microprocessors that can run the swarm AI algorithms, the lack of a platform for swarm applications, operations with limited connectivity and the lack of development of required algorithms for various operating scenarios.[1623]

23.3.4. Hyper-Deployed: Facilitating human centric IoT systems

Although IoT connects "things" and machines with other "things" and machines, its value is felt and realized by people. In a future hyperconnected world with billions of smart devices, IoT is embedded and integrated transparently into all aspects of our lives where we use it in our work, our studies, our recreation and our homes. While this "ambient intelligence" world is a vision of the future, human centric IoT is necessary for this vision to become reality.

Consider today's smart phones. A smart phone is an IoT device and many people rely on its maps feature to direct them to a place where they have never been before, along a route that minimizes their transit time.

Despite this, some drivers prefer to use GPS navigation devices instead of the maps feature on their smart phones. GPS navigation devices have larger screens, which makes it easier to read for drivers who may be driving in traffic conditions where they can only take their eyes off the road for a fraction of a second. Others are concerned about their privacy and do not wish to be tracked, while others may have a mobile phone with data limits.

In addition, some prefer the GPS navigation unit as it is well integrated into their car's auto pilot system and offers a seamless driving experience. As we move towards a hyperconnected world with billions of IoT devices, research and innovation in human centric considerations in several areas are critical in driving user adoption and value realization.

Representative areas for future consideration are discussed below.

23.3.4.1. Design for human-AI interaction and collaboration

As adoption of AI-enabled IoT systems becomes more prevalent, some activities normally done by humans will be performed autonomously by AI systems. The role of humans will evolve to jobs where both humans and AI systems are needed to complete a task safely and accurately.

According to analysis conducted by the McKinsey Research Institute, nearly 50% of current work activities could be automated with currently demonstrated technologies and 60% of current jobs have more than 30% of activities that can be automated.[1624] As these technologies are adopted, the jobs will change. As automation augments human workers it will lead to increases in productivity, efficiencies and safety along with decreased operational costs.

[1622] "The Collective Power of Swarm Intelligence in AI and Robotics", T. McClean, Forbes, May 13, 2021. Link

[1623] Interview notes. Dr. Kiju Lee, Texas A&M University, December 16, 2021

[1624] "AI, Automation and the Future of Work: Ten Things to Solve For", J. Manyika and K. Sneader, McKinsey Global Institute, June 1, 2018. Link

© Strategy of Things, 2025. All rights reserved.

For example, collaborative robots (cobots) work alongside operators to manufacture products in a factory.[1625] According to market research firm ABI Research, the cobot market will expand at a projected CAGR of 32.5%, from $600 million in 2021 to $8 billion by 2030.[1626] Another example of human-AI collaboration is intelligent driver assistance systems for truck drivers.[1627]

Human-AI collaboration requires both to "work together as partners to achieve a common goal, sharing a mutual understanding of the abilities and respective roles of each other."[1628] The AI system must be enabled to take the most appropriate actions based on an understanding of the current task and real time assessment of the situation by observing the users, predicting their actions and anticipating their needs. Successful collaboration requires the development of new techniques, methods and components to enable a tightly coupled perception-action integration between humans and the AI system.[1629]

For replicable and successful collaboration between humans and AI-enabled IoT systems, continued research is necessary to understand how AI systems can most effectively augment humans, how AI systems can enhance what humans do best and how to redesign operations and algorithms to support the collaboration.

Some characteristics that impact collaboration for AI systems include interaction modes, adaptability, performance predictability and explainability.[1630] For humans, characteristics such as the age of the operator, any specific needs of the operator along with culture and language expectations, impact human-AI-IoT collaboration.

23.3.4.2. Enabling generative AI for IoT

AI systems offer transformative opportunities for IoT, capitalizing on the synergy between intelligent data generation, processing and interaction with IoT devices. However, adoption of AI systems faces a number of significant challenges due to the resource constraints of IoT devices and the complexity of generative models.[1631]

One major challenge is the high resource demands of generative AI models, which typically consist of billions of parameters. IoT devices, such as wearables and sensors, often have limited memory and computational power, making it difficult to run these large AI models locally. Techniques such as model compression, quantization and parameter pruning are being explored, but these often lead to trade-offs in model accuracy and performance. Additionally, on-device

[1625] "Cobots Improve Productivity, Shifting Workers Away From Dirty, Dangerous and Dull Jobs", J. Campbell, International Society of Automation, November/December 2019. Link

[1626] "Cobot Market to Grow to $8b By 2030, Report Finds", Collaborative Robot Trends, June 4, 2021. Link

[1627] "Trucking's ADAS Technologies Still Have Many Barriers to Overcome", C. Commendatore, Fleet Owner, October 6, 2021. Link

[1628] "A Simple Guide to Collaborative AI", AI-on-Demand Platform. Link

[1629] See reference 1628.

[1630] "Human - AI Collaboration Framework and Case Studies", Partnership on AI, September 2019. Link

[1631] "IoT in the Era of Generative AI: Vision and Challenges," X. Wang, Z. Wan et al., January 2024. Link

© Strategy of Things, 2025. All rights reserved.

inference is problematic because IoT applications frequently require real-time responses, which are difficult to achieve given the limited processing capabilities of these devices.

Other challenges include prompt engineering, especially for IoT applications that involve multimodal data, such as video, audio and sensor input. Designing efficient and contextually relevant prompts for generative AI to respond to real-world IoT scenarios is complex. Furthermore, offloading parts of the generative model's computation to nearby edge servers or the cloud introduces difficulties in workload partitioning and maintaining efficient communication while minimizing latency.

23.3.4.3. Facilitate trust

Human-AI collaboration breaks down or becomes less productive if one or both sides do not execute as expected. For example, an intelligent driving assistance system may apply the brakes on a truck if it detects stopped traffic ahead on the road. But if the system applies the brakes one time and does not in other times, the driver cannot rely on it to work. The driver may not use it, or only use it under certain conditions. In other situations, the AI system may work as designed, but people are not able to explain why it works and why it did what it did.

To develop more trustworthy human-AI collaboration, a holistic approach to understanding trust is needed. In the defense industry, research and development efforts have emphasized technology-centric approaches, such as making AI systems more transparent, explainable and reliable, in order to build trust into the human-AI collaboration.[1632] This approach may result in instances of trust, where one team in one situation will trust the AI, but perhaps other teams in other instances will not.

The human side of collaboration is equally important. Factors such as age, gender and cultural background may affect trust. Finally, the conditions in which the human-AI collaboration operate is another factor, with people over-trusting a machine's recommendations in high stress scenarios.

23.3.4.4. Facilitate accessibility and inclusion

Despite the value that IoT provides, its benefits may not be available or accessible to everyone. For example, many cities are implementing "smart parking" technologies that help drivers find open parking spaces by communicating that information on a smart phone app. However, 11% of U.S. adults have non-smart cellphones[1633] and do not have access to this information. In addition, there are those with smart phones who do not have the appropriate parking app. To address this challenge, some cities employ on-street digital signage to broadly communicate parking information.

This simple example illustrates a wider challenge. No matter how prevalent and connected IoT is, the real world is filled with people who cannot fully access the benefits of a fully connected society. People who have low vision cannot access and interact with information displayed on monitors and smart phone screens. Non-English speakers cannot interact with applications

[1632] "Building Trust In Human-Machine Teams", M. Konaev and H. Chahal, Brookings Tech Stream, February 18, 2021. Link

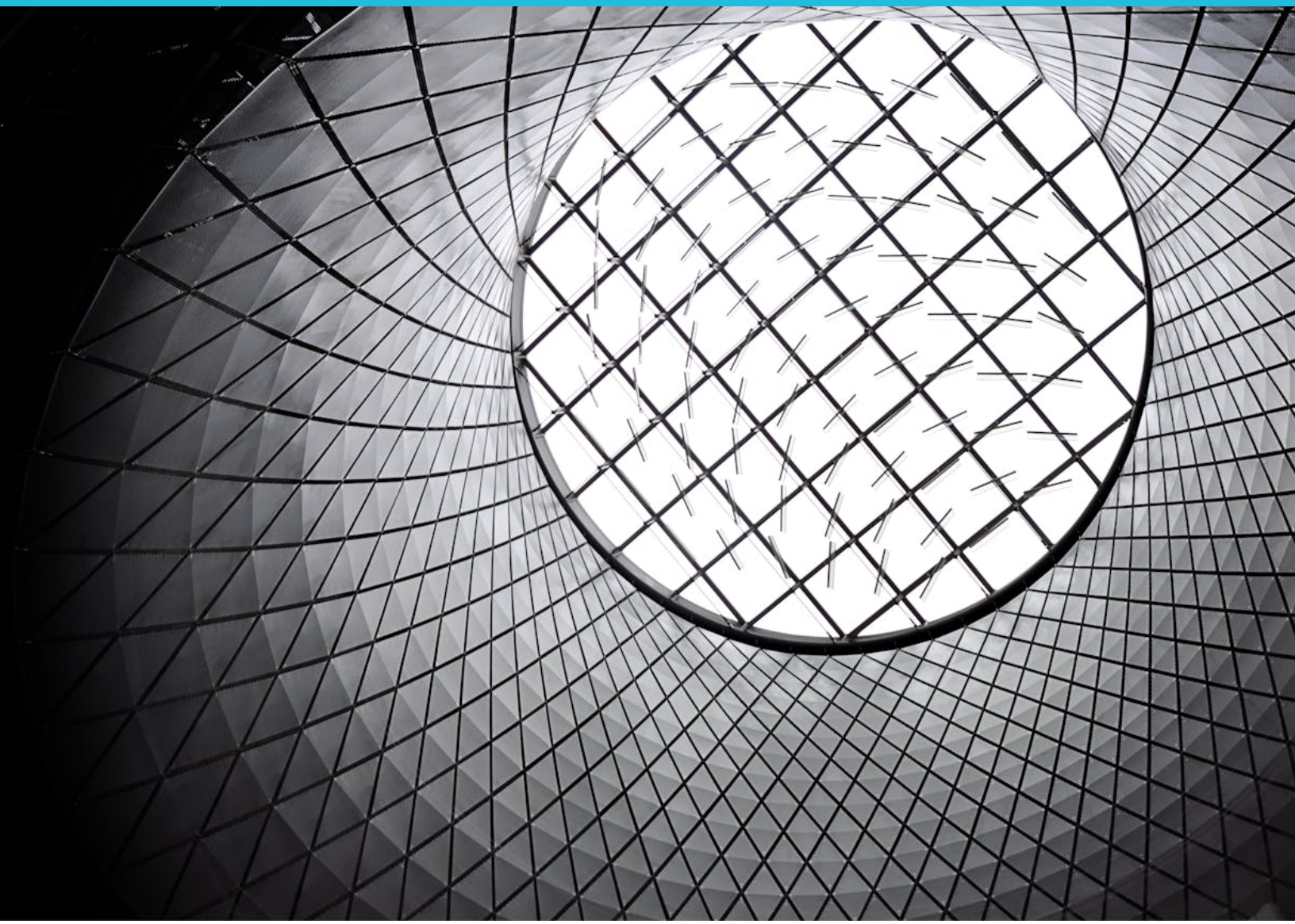
[1633] Mobile Fact Sheet, Pew Research Center, April 7, 2021. Link

© Strategy of Things, 2025. All rights reserved.

written in English. People with low digital literacy struggle to perform complex operations, while those with poor reading proficiency struggle to use text-based applications. People in a rush, under stress, or at the end of a long working day, struggle and get flustered with phone menu-based customer support systems.

To be inclusive and accessible to as many people as possible, a connected society must develop interaction models and user interfaces that are intuitive, easy to use and program and consistent with the way people expect to interact with human-AI and IoT systems. Interactions may be performed through gestures, voice, neural scans, proximity through wearable devices or other as yet unknown means. As human-AI collaborations become more common, continued research and innovation in enabling more effective user experiences and user interaction is required to realize their benefits.

© Strategy of Things, 2025. All rights reserved.



Appendix: Government Opportunities to Address Gaps

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

© Strategy of Things, 2025. All rights reserved.

24. Appendix: Government Opportunity to Address Gaps

As new technologies are discovered and their practicalities explored, they can diffuse into the broader economy if they can provide material benefits. Figure 24-1 below shows a historical view of how earlier consumer technologies found their place in the economy.

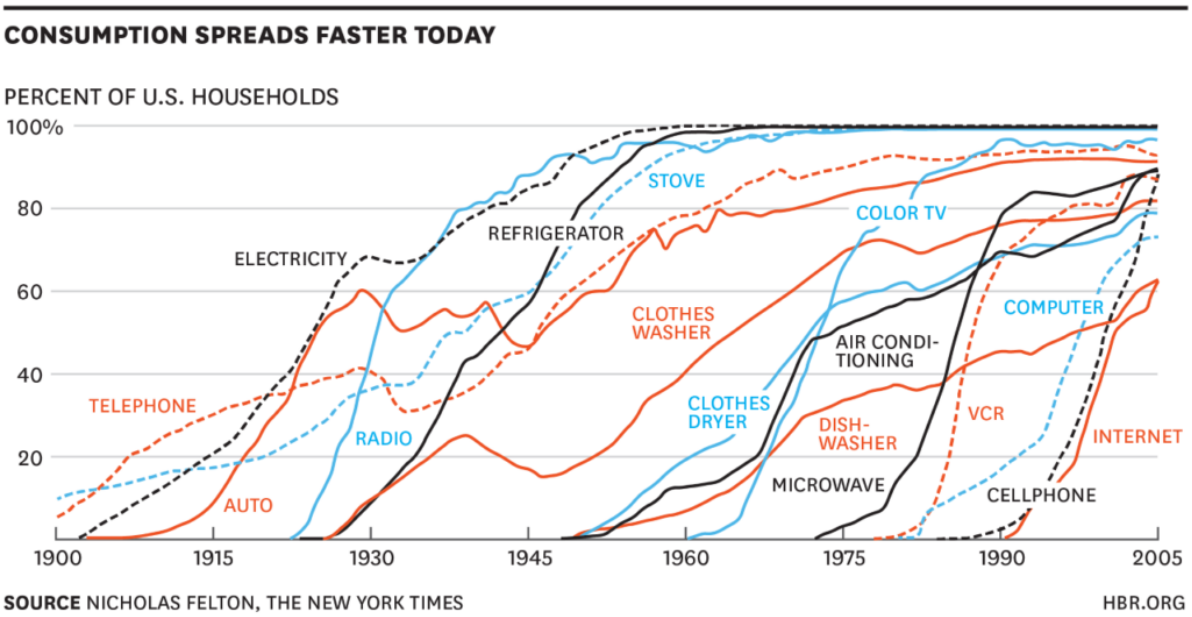


Figure 24-1: Technology Diffusion

These curves represent the rate at which new technology is embraced by the market.[1634] Initially, a small percentage of early adopters utilize the new technology. These early adopters are often risk-takers, willing to experiment with innovative solutions despite potential uncertainties. This phase is critical for validating the technology's viability and functionality.

As the technology gains market traction and matures, rapid adoption driven by consumers' increased awareness and realization of benefits occurs. These benefits include increased productivity, cost savings and enhanced safety. Adoption reaches a tipping point when the technology is widespread and integrated into everyday use.

Upon reaching the tipping point, the rate of consumers' adoption slows and reaches a plateau as the technology becomes ubiquitous, reaching its maximum penetration within the market. Further adoption is limited and comes from technology latecomers.

The rate and extent of technology diffusion can be influenced by several factors, such as the availability of supporting infrastructure, the type of benefits as well as safety and risk, which all can play a role in facilitating the spread of a technology's adoption.

[1634] "The Pace of Technology Adoption is Speeding Up," R. McGrath, Harvard Business Review, November 25, 2013. Link.

© Strategy of Things, 2025. All rights reserved.

Government policies and actions, including research and development, regulations and legislation and workforce development can also slow or advance this technology diffusion. For example, policies promoting digital skills development increase the pool of adopters able to use and adapt to new technologies. On the other hand, onerous regulations may increase the price of the technology and reduce its affordability for the adopter wanting to purchase.

24.1. IoT considerations for policymakers

While IoT offers significant and transformational outcomes, several factors must be considered to help facilitate its scaling into the economy and civil society. Policymakers play an important role in driving adoption and acceleration of IoT in ways that industry cannot do. Factors that government policymakers should consider supporting include the following:

- **Technology maturity.** IoT is not one technology, but a variety of disparate standards, hardware, software and connectivity technologies at different levels of maturity and adoption. Furthermore, IoT is converging with adjacent technologies, such as blockchain and artificial intelligence, which are also at various levels of maturity. To support effective adoption of IoT overall, policymakers can align governmental actions with the technology maturity stage to drive effective outcomes.
- **Cybersecurity**. IoT devices create new attack surfaces and expose vulnerabilities that can be exploited by cybercriminals. This can lead to breaches of IoT systems and the broader integrated IT networks with unauthorized access and data theft. This can disrupt businesses, critical infrastructure and lead to compromised safety. In addition, IoT devices can be "hijacked" and used in attacks on other systems. Policymakers should consider actions to facilitate IoT that are safe to use and to scale.
- **Data privacy, ownership and governance**. IoT devices collect and generate large volumes of data, raising questions about consent, ownership, access, usage, sharing and control. To prevent abuse and promote fair data governance practices, policymakers should consider actions around data ownership and usage rights and responsibilities.
- **Interoperability and Standards.** The IoT ecosystem comprises a diverse array of devices from different manufacturers, operating on various protocols and platforms with a range of users. Furthermore, to have a functional ecosystem, IoT must be able to integrate and interoperate with legacy technology systems with proprietary protocols. To ensure seamless communication and compatibility between devices and systems, policymakers should consider actions around the challenge of establishing interoperability standards.
- **Liability and Accountability.** Liability concerns arising from known and unknown outcomes for owners and users slow the development and adoption of IoT systems. This is further exacerbated by artificial intelligence used in autonomous systems, where actions taken by algorithms are not always transparent or explainable. Policymakers should consider undertaking actions that facilitate and clarify responsibility and ensure accountability for any harm caused by IoT devices or networks.
- **Regulatory Frameworks**. Existing regulatory frameworks may not adequately address the unique challenges posed by employing innovative IoT technologies, especially those that operate in regulated industries such as healthcare, insurance and energy. To address issues such as cybersecurity, data protection, safety, consumer rights and environmental

© Strategy of Things, 2025. All rights reserved.

impact in the context of IoT, policymakers need to adapt existing regulations or develop new ones.

- **Ethical and Social Implications**. IoT deployments can have profound societal impacts, affecting employment, healthcare, transportation and urban planning. The outcomes provided may not be accessible, equitable or inclusive. To ensure efficacious outcomes, policymakers should consider actions that address ethical and socio-economic concerns, including issues related to surveillance, discrimination, inequality and the digital divide.
- **International collaboration and coordination.** IoT ecosystems operate across national borders, requiring international cooperation and coordination among policymakers to address regulatory gaps, harmonize standards and facilitate cross-border trade and data flows while respecting sovereignty and cultural differences.
- **New and emerging business models**. IoT changes and creates new innovative business models and ecosystems. For example, some businesses that sell hardware may sell digital services, information and "IoT as a service." Policymakers would do well to consider undertaking actions that facilitate the development, adoption and operation of these new business models into the economy.

24.2. Framework for IoT policymaking

This section proposes a framework to examine government policymaking actions to address IoT technology infrastructure gaps identified in this research. The gaps identified are complex and, in many cases, long running. Addressing these gaps will require both individual agency and coordinated interagency action.

The framework, shown below in Figure 24-2, focuses on five areas that the U.S. federal government can consider to facilitate the resolution of the IoT technology infrastructure challenges. These examples illustrate what had been done elsewhere for both IoT and non-IoT technologies and do not represent an endorsement of its success or efficacy.

© Strategy of Things, 2025. All rights reserved.

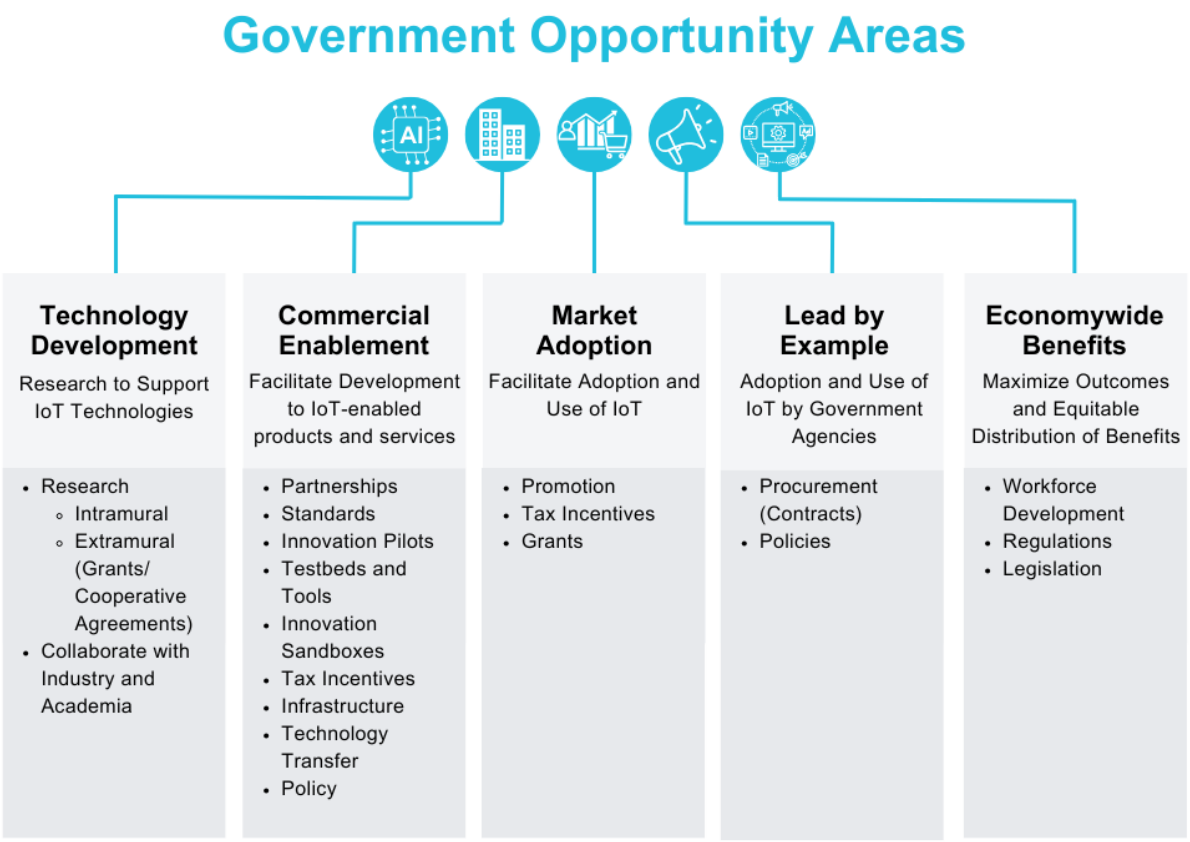


Figure 24-2: Government Assistance Areas

The remainder of this section discusses the five areas of Technology Development, Commercial Enablement, Market Adoption, Lead by Example and Accelerate Value Realization.

24.2.1. Technology development

The technology development category refers to government actions that advance the state and development of promising innovations through basic and applied research.

Research is fundamental to the United States' ability to develop and advance new technologies and innovations. A number of federal organizations conduct and support research, including the National Science Foundation (NSF), the National Institute of Standards and Technology (NIST), the Department of Energy (DOE), the Department of Defense (DoD) and the Department of Transportation (DOT).

In addition to these organizations, research is also funded by several Advanced Research Projects Agency (ARPA) organizations. These agencies, modeled after the Defense Advanced Research Projects Agency (DARPA), include ARPA-E (energy), ARPA-H (healthcare), ARPA-I (infrastructure) and IARPA (intelligence) and fund breakthrough, high-risk and high reward research.

The federal government supports research in several ways, including conducting research through its network of national laboratories and Federally Funded Research and Development

© Strategy of Things, 2025. All rights reserved.

Centers (FFRDCs), funding and supporting research through industry and universities and transferring federal research to market (technology transfer).

Figure 24-3 below shows some examples of government support for technology development.

Approach	Description	Example
Research – intramural	Basic and applied research conducted through U.S. national labs and federally funded research and development centers	• SunShot Initiative (DOE)[1635]
Research - university	Basic and applied research conducted through universities. Research is supported through grants.	• LUCI: Laboratory University Collaboration Initiative[1636]
Research - industry	Basic and applied research conducted through industry. Some research is done in collaboration with universities. Research is supported through grants and contracts.	• Small Business Innovation Research (SBIR)[1637] • United States Advanced Battery Consortium grant award from DOE Vehicle Technologies Office[1638]
Technology Transfer	Facilitate access to federally funded research and technology and bring to market through licensing and Cooperative Research and Development Agreements (CRADAs) and licensing	• The Federal Technology Transfer Act (FTTA)[1639] • NIST TMAP (Technology Maturation Accelerator Program)[1640] • Lab-to-Market (L2M)[1641]

Figure 24-3: Technology Development Examples

24.2.2. Commercial enablement

Commercial enablement refers to U.S. government activities and initiatives that facilitate the commercialization of products and services. This includes supporting the technologies developed through federal intramural research, industry and university research as well as independent

[1635] "The SunShot Initiative." Link

[1636] "LUCI: Laboratory University Collaboration Initiative", 2024. Link

[1637] SBIR-STTR website. Link

[1638] "Selection for Battery Research and Development Consortium," Office of Energy Efficiency and Renewable Energy, Vehicle Technologies Office. January 18, 2024. Link

[1639] The Federal Technology Transfer Act (FTTA). Link

[1640] "Taking an Innovation from Lab to Market," M. Child, NIST, November 10, 2020. Link

[1641] "Lab-to-Market", NIST. Link

© Strategy of Things, 2025. All rights reserved.

industry efforts. The federal government supports the commercialization of innovative technologies in several ways. These include the following:

- **Standards development.** Standards are needed to ensure interoperability, safety and quality across industries. Except for those pertaining to health, safety and the environment, the U.S. approach to standards development is "industry leads, government supports." In this capacity, the federal government provides the foundational research and development necessary to establish technical standards.

  It participates in standard-setting organizations, both domestically and internationally, to advocate for American interests and ensure that U.S. standards are harmonized with global practices.

  Finally, the government incorporates consensus standards into federal regulations and procurement processes to facilitate broader adoption and adherence.
- **Tax incentives.** The government incentivizes businesses to commercialize innovative products and services through a variety of vehicles including tax incentives.

  For example, the Research and Experimentation (R&E) tax credit offers "a dollar-for-dollar credit against the taxpayer's federal income tax liability, which yields companies a twofold benefit. First, the deduction in the year the expenditure is paid and second, the tax credit."[1642]
- **Partnerships.** The federal government convenes and fosters collaborative partnerships between government, universities and industry to facilitate the commercialization of new innovations and technologies. These partnerships help disseminate and share knowledge, foster industry collaboration and build community.
- **Testbeds and tools.** The federal government has established several platforms that are accessible and available to universities and industry to evaluate theories, tools and new technologies.
- **Innovation sandboxes.** Innovations may be transformative and they may have unforeseen outcomes. Sandboxes are safe testing environments for businesses that enable new innovations, business models and services to be piloted within boundaries established by regulators.
- **Infrastructure.** The federal government plays a significant role in enabling infrastructure that scales and supports the economy.

  For example, the federal government specifies and makes available spectrum for wireless connectivity. Innovators and solutions providers use this spectrum to develop, build and market the value-added services and products around this spectrum.
- **Technology transfer**. Innovations developed through federal research and through some grants (SBIR) are brought out of the lab and made available to industry through licensing and Cooperative Research and Development Agreements (CRADAs) and other

[1642] "R&E Tax Credit is a 'Smart' Incentive for Industry 4.0 Companies to Improve Financial Performance," T. Finerty, S. Russell. MiMfg Magazine. March 2019. Link

© Strategy of Things, 2025. All rights reserved.

technology transfer methods.

Figure 24-4 below shows some examples of commercial enablement support.

Approach	Description	Example
Partnerships	The U.S. government fosters partnerships to stimulate economic development, often in overlooked communities	• AI and Emerging Technology Partnership: The United States Patent and Trademark Office (USPTO) has established this partnership to foster and protect innovation in Artificial Intelligence and other emerging technologies (ET). [1643]
Standards	Setting standards that underpin economic prosperity across the country.	• The United States Government National Standards Strategy for Critical and Emerging Technology (USG NSSCET).[1644]
Innovation pilots	Supporting innovation pilots by investing in research & development (R&D), entrepreneurial ecosystems, talent pipelines and incentives for intellectual property commercialization, providing capital, tools and resources to entrepreneurs.	• The Semiconductor Technology Pilot Program launched by the United States Patent and Trademark Office (USPTO). This program was designed to support the Creating Helpful Incentives to Produce Semiconductors (CHIPS) Act of 2022.[1645] • National Artificial Intelligence Research Resource (NAIRR).[1646]
Testbeds and tools	Platforms for testing of theories, tools and new technologies.	• NIST National Fire Research Laboratory (NFRL). • Public Safety Communications Research (PSCR).

[1643] " USPTO AI/ET Partnership: Public Symposium on Artificial Intelligence and Intellectual Property ", March 2024. Link

[1644] May 2023. Link

[1645] "Semiconductor Technology Pilot Program." Link

[1646] "National Artificial Intelligence Research Resource Pilot", U.S. National Science Foundation. Link

© Strategy of Things, 2025. All rights reserved.

Approach	Description	Example
Innovation sandboxes	Safe testing environments in which innovators can see their inventions play out with certain regulatory leeway and appropriate consumer and user protections.	• Regulatory sandbox for blockchain.[1647] • Unmanned Aircraft System (UAS) Integration Pilot Program (IPP).[1648]
Tax incentives	Provides tax incentives to stimulate economic growth, attract and retain businesses and promote investment in specific industries and regions.	• Research and Development (R&D) Tax Credit.[1649]
Infrastructure	Invests in infrastructure to stimulate economic growth, improve the quality of life and ensure the efficient functioning of the economy	• The Bipartisan Infrastructure Law. This law directs $1.2 trillion of federal funds towards transportation, energy and climate infrastructure projects, most of which are distributed via state and local governments.
Technology Transfer	Facilitating the transition of federally funded innovations from the laboratory to the marketplace, improving the efficacy of its innovation process and ensuring that these lab-developed technologies find use in the commercial marketplace.	• Accelerate the Procurement and Fielding of Innovative Technologies (APFIT).[1650]
Innovation Grants	Through agencies like the Economic Development Administration (EDA) which provides grants to stimulate economic growth, attract and retain businesses and promote investment in specific industries and regions.	• Grants.gov[1651] provides a centralized location for grant seekers. It provides information on over 1,000 grant programs.

Figure 24-4: Commercial Enablement Examples

24.2.3. Facilitate market adoption

[1647] "EU and U.S. Regulatory Sandboxes: Groundbreaking Tools for Fostering Innovation and Shaping Applicable Regulations", Insights, Jones Day, April 2023. Link

[1648] "UAS Integration Pilot Program," Federal Aviation Administration. Link

[1649] "NSIGHT: Financing Innovations in Emerging Technologies With R&D Tax Credits", August 2020. Link

[1650] "For emerging tech, DoD funds $100M in new projects to help bridge 'valley of death'," J. Gill, Breaking Defense, July 20, 2022. Link

[1651] Link

© Strategy of Things, 2025. All rights reserved.

Facilitate market adoption refers to the set of actions that help drive market awareness, interest and the ability to adopt new technologies. Innovative and emerging technologies, such as IoT, face market adoption challenges. Technology buyers fall along an adoption continuum, from visionary early-adopters trying the "latest and greatest" to laggards who are the last to adopt.

The behavior as described above is attributed to many factors, including lack of awareness, technology maturity, risk concerns, change resistance and lack of resources. Slow adoption cycles often hurt small businesses and start-ups who develop these technologies as they often do not have the financial or marketing resources to sustain slow market take-up.

The federal government plays an important role in facilitating market adoption through awareness and incentives along with supportive types of funding and resources. These include:

- **Promote awareness.** The federal government, with its credibility and broad reach to industry, academia, state and local governments and the media helps to increase visibility of and interest in these innovative technologies both within the government and the market.

  Collectively, the federal government produces thousands of publications each year on a variety of topics, speaks on and participates in various industry programs, connects U.S. businesses with overseas opportunities and adopts these technologies into its operations. This visibility helps to educate, drive awareness, create opportunities for and increase confidence in the new technologies.
- **Tax incentives.** Market adoption and scale can be accelerated through a variety of tax incentives that reduce the investment burden and increase return on investment.

  For example, to facilitate the adoption of electric vehicles, the federal government offers consumers a tax credit of up to $7,500[1652] and small businesses up to 30% of purchase costs.[1653] Similarly, the federal government offers small businesses a tax credit of up to $5 per square foot of building space for implementing energy efficiency improvements[1654] and tax deductions for energy efficient commercial buildings.[1655]

  State governments may have their own incentives, ranging from "tax credits or rebates to fleet acquisition goals, exemptions from emissions testing or utility time-of-use rate reductions."[1656]
- **Funding.** The federal government offers several general loan and grant programs to support investment, some of which are targeted to an administration's priority areas. One such grant program is the Advanced Transportation Technology and Innovation

[1652] "Credits for new clean vehicles purchased in 2023 or after," Internal Revenue Service. Link

[1653] "Fact Sheet: How the Inflation Reduction Act will help small businesses," The White House, September 12, 2022. Link

[1654] ibid.

[1655] "Energy efficient commercial buildings deduction," Internal Revenue Service. Link

[1656] "State Policies Promoting Hybrid and Electric Vehicles", A. Igleheart, National Conference of State Legislatures, August 2023. Link

© Strategy of Things, 2025. All rights reserved.

(ATTAIN) program where the federal government may share up to 80% of project costs for highway infrastructure projects.[1657]

- **Resources.** Innovative technologies often require specialized expertise and resources that adopters may not possess. Government resources and expertise help close this gap. One example is the NIST Manufacturing Extension Partnership, located in all fifty states and Puerto Rico, which works with small and medium sized U.S. manufacturers to help them grow by providing resources to reduce costs, improve productivity and efficiency and other services.[1658]

Figure 24-5 below provides examples of government facilitating market adoption.

Approach	Description	Example
Promotion	Increase awareness of innovative technologies through publications, research, industry, academia and media outreach. Promote U.S. businesses to overseas markets.	• US Trade and Development Agency (USTDA). • US Department of State Innovation Roundtables.
Tax incentives	Financial incentives, such as tax credits and deductions to increase technology adoption. Technologies, behaviors or capabilities that meet targeted goals.	• Tax rebates. • EV tax credits.[1659] • Tax deductions for energy efficient buildings.[1660]
Funding	Financial offers such as loans and grants, apart from tax incentives, which help adopters procure technologies, services and capabilities targeted by the federal government.	• Advanced Transportation Technology and Innovation.[1661] • Advanced Digital Construction Management Systems.[1662]

[1657] "Grant Programs," U.S. Department of Transportation Federal Highway Administration. Link

[1658] "Manufacturing Extension Partnership (MEP),." U.S. National Institute of Standards and Technology. Link

[1659] See note1652

[1660] See note 1655

[1661] See note 1657

[1662] "Biden-Harris Administration Announces $34 Million in Grants to 10 States for Advanced Digital Construction Technologies That Save Time and Money," Press Release, U.S. Department of Transportation Federal Highway Administration, November 16, 2023. Link

© Strategy of Things, 2025. All rights reserved.

Approach	Description	Example
Resources	Resources and solutions to help facilitate market consideration and adoption.	• NIST MEP.[1663]

Figure 24-5: Facilitate Market Adoption Examples

24.2.4. Lead by example

Lead by example refers to a set of actions that the federal government can undertake to signal both support and interest. In 2021, the federal government spent $645 billion in contracts for products and services, up from $513 billion in 2017.[1664]

This substantial buying power allows the federal government to influence and drive desired outcomes. The government can utilize direct procurement, implementation of contracting policies and innovation pilots to support market developments. Each of these is discussed below.

- **Procurement.** The federal government can increase market adoption of innovative technologies by procuring innovative and emerging technology solutions for internal use. For example, the Central Intelligence Agency (CIA) awarded a $600 million contract to Amazon Web Services (AWS) for single client private cloud.[1665] While providing the CIA with innovative capabilities, this contract award signaled the CIA's confidence in the technology to the market.

  For many years, the pace of cloud adoption was slowed by concerns over data security. But when the Central Intelligence Agency awarded a $600 million contract to Amazon Web Services, Inc., in 2013 to move some of the nation's most sensitive information into the cloud, it was widely viewed as a seminal moment for the fledgling industry.[1666]

- **Policies.** The federal government's buying power can be used to develop and implement procurement policies, which in turn drives targeted outcomes. For example, to facilitate cybersecurity practices among its contractor community, the Department of Defense (DoD) implemented Defense Federal Acquisition Regulation Supplement (DFARS) 2019-D041, effective November 30, 2020.

  This policy "mandates all defense contractors to perform self-assessments of their cybersecurity using the NIST CSF (SP) 800-171 DoD Assessment Methodology to

[1663] See note 1658

[1664] "Federal Contract Spending in the Last 5 Years," K. Bernal, GovConWire, May 25, 2022. Link

[1665] "Amazon Wins $600 Million CIA Cloud Deal As IBM Withdraws Protest," K. McLaughlin, CRN, October 30, 2013. Link

[1666] "CIA's move to cloud a game changer for public sector," M. Albertson, Silicon Angle, June 16, 2017. Link

© Strategy of Things, 2025. All rights reserved.

qualify for new defense contracts and renewals of current contracts."[1667]

Similarly, to encourage the development of solutions based on consensus standards, the federal government can specify and procure solutions that have been built to those standards.

- **Innovation pilots.** Innovative and emerging technologies offer the potential for transformational outcomes to support the mission and day-to-day operations of various federal agencies. Pilot projects help agencies understand the capabilities of the innovative technologies, evaluate their feasibility for a variety of use cases and help define the requirements for procurement and scaling. For example, the U.S. National Science Foundation has piloted the use of blockchain to make its grants review and awards process more efficient.[1668]

  Furthermore, these pilots signal to the broader market and industry the federal government's interest and willingness to consider these technologies in its operations.

Figure 24-6 below provides examples of government leading by example.

Approach	Description	Example
Procurement	Purchase of products and services for internal agency use.	• CIA award to AWS.[1669]
Policies	Rules that support the procurement of products and services.	• DFARS Case 2019-D041.[1670] • Small Business Set-Asides.[1671] • Executive Order 14057 (Catalyzing Clean Energy Industries and Jobs Through Federal Sustainability).[1672]

[1667] "The Interim DFARS Rule and What It Means for You," KDH Consulting. Link

[1668] "NSF explores blockchain for grants management," S. Friedman, Route Fifty, December 3, 2018. Link

[1669] See note 1665

[1670] "Executive Summary. Interim DFARS Rule 2019-D041, Assessing Contractor Implementation of Cybersecurity Requirements", J. Tenaglia, Office of the Undersecretary of Defense. Link

[1671] "Set-aside procurement," U.S. Small Business Administration. Link

[1672] "Executive Order on Catalyzing Clean Energy Industries and Jobs Through Federal Sustainability," The White House, December 8, 2021. Link

© Strategy of Things, 2025. All rights reserved.

Approach	Description	Example
Pilots	Proof-of-concept and experimental projects to determine feasibility and understand requirements.	• Robotic Process Automation and Distributed Ledger Technology pilots for U.S. Bureau of the Fiscal Service.[1673] • NSF Grants Community Blockchain.[1674]

Figure 24-6: Lead by Example Examples

24.2.5. Broaden economywide benefits

Broaden economywide benefits refers to policymaking activities that remove structural barriers to scale value realization and facilitate equitable distribution of outcomes while minimizing negative outcomes such as compromised safety, cybersecurity or misuse. Potential activities include workforce development, infrastructure development, regulations and legislation.

While market adoption is necessary for the diffusion of IoT technologies into the economy and civil society, it does not mean that its benefits are always fully enabled or realized. Some examples of its limitations include:

- Remote patient monitoring enables doctors to monitor patients outside of clinical settings and allows for early detection and treatment of health problems. These benefits, however, are not available to those in rural communities that have no or limited broadband infrastructure and to those who cannot afford broadband services.
- Small businesses make up 99.9% of all businesses, employ 46.4% of private sector workers and 39.4% of private sector payroll.[1675] While IoT can help these small businesses become more productive, efficient and competitive, they lack the infrastructure, expertise and capital to adopt and operate these solutions.
- Asset tracking is a priority IoT use case in the transportation and logistics industry. Despite this, end-to-end supply chain visibility remains one of the industry's biggest challenges due to a lack of data sharing.

Figure 24-7 below provides examples of government policymaking actions supporting and accelerating value realization.

[1673] "Bureau of the Fiscal Service Launches Two Innovative Pilot Projects," Bureau of the Fiscal Service, October 2, 2017. Link

[1674] See note 1668

[1675] "Frequently Asked Questions About Small Business 2023," Office of Advocacy, U.S. Small Business Administration, March 7, 2023. Link

© Strategy of Things, 2025. All rights reserved.

Approach	Description	Example
Workforce development	Initiatives and actions supporting workforce development, from strategy to programs.	• Regional Technology and Innovation Hubs (Tech Hubs).[1676] • National Cyber Workforce and Education Strategy.[1677] • Highway Funding for Workforce Development.[1678] • STEM Challenge Grants.[1679]
Legislation	Legal instruments that establish requirements or prohibitions.[1680]	• HIPAA (Health Insurance Portability and Accountability Act). • FD&C Act section 524B (Ensuring Cybersecurity of Devices). • Internet of Things Cybersecurity Improvement Act of 2020. • Bilateral Infrastructure Law.
Regulations	Legal instruments published by executive branch agencies to clarify their interpretation of a law and how it will be implemented.[1681]	• "Medical Device Data Systems, Medical Image Storage Devices and Medical Image Communications Devices" (FDA regulation).[1682]
Pilots	Experimental initiatives to address specific challenges	• Freight Logistics Optimization Works (FLOW) data exchange pilot.[1683]

[1676] "Regional technology and innovation hubs (Tech Hubs)," U.S. Economic Development Administration. Link

[1677] "National cyber workforce education strategy," Office of the National Cyber Director, The White House, July 31, 2023. Link

[1678] "Highway Funding for Workforce Development", U.S Department of Transportation Federal Highway Administration. Link

[1679] "EDA's STEM Talent Challenge Grants: Workforce Funding for the Innovation Economy", 2023. Link

[1680] "Introduction to U.S. Law and Policy," Pubic Health Emergency, U.S. Department of Health and Human Services. Link

[1681] ibid.

[1682] "Medical Device Data Systems, Medical Image Storage Devices and Medical Image Communication Devices; Mobile Medical Applications: Guidances for Industry and Food and Drug Administration Staff; Availability" Federal Register, February 9, 2015. Link

[1683] See note 918

© Strategy of Things, 2025. All rights reserved.

Approach	Description	Example
Resources	Resources and solutions to help adopters optimize and increase value from innovations	• NIST MEP.[1684]

Figure 24-7: Accelerate Value Realization Examples

24.3. Prior IoT studies

A non-exhaustive search showed that there is a well-established literature on the role of government in supporting technological development and IoT.[1685] A search through the academic literature using keywords and proximity along with searches in the wider internet provided a selected list of prior studies and initiatives from both the United States and the European Union.

24.3.1. USA studies

Figure 24-8 overleaf highlights some of these studies.

[1684] See note 1658

[1685] Google Scholar returned around 4 million results for a search on the "role of government in technology." Link This reduced to 167,000 hits when IoT was added to the search criteria. Link

© Strategy of Things, 2025. All rights reserved.

Study	Findings
Fostering the advancement of the internet of things[1686]	The study identified four areas of existing government support: • **Enabling Infrastructure Availability and Access.** Support the physical and spectrum-related assets needed to support IoT growth and advancement. • **Crafting Balanced Policy and Building Coalitions.** Removing barriers and encouraging coordination and collaboration; influencing, analyzing, devising and promoting norms and practices that will protect IoT users while encouraging growth, advancement and applicability of IoT technologies. • **Promoting Standards and Technology Advancement.** Ensuring that the necessary technical standards are developed and in place to support global IoT interoperability and that the technical applications and devices to support IoT continue to advance. • **Encouraging Markets.** Promoting the advancement of IoT through departmental usage, application, iterative enhancement and novel usage of the technologies.
Guiding the IoT to safety: The Internet of Things and the role of government as both user and regulator[1687]	Government plays three roles, as IoT end user, infrastructure provider and regulator. Striking the right balance between these goals and then developing appropriate policies to achieve them, is the main challenge facing officials dealing with emerging technologies. • **IoT end user.** Government can leverage the role of end user/buyer to drive change. • **Infrastructure provider.** Government can enable transparency as both as an end user and infrastructure provider to reduce uncertainty and increase market confidence. • **Regulator.** The government must address bottlenecks in communication and the analysis of data.

[1686] "Fostering the Advancement of the Internet of Things", Dept of Commerce Green Paper, January 2017. Link

[1687] "Guiding the IoT to Safety", Deloitte University Press. Link

© Strategy of Things, 2025. All rights reserved.

Study	Findings
Why Countries Need National Strategies for the Internet of Things[1688]	The work makes the broad case for government support for IoT technologies covering market failures, equity issues, the need for innovation friendly regulation and how governments can support interoperability.
What roles should the government play in fostering the advancement of the internet of things?[1689]	The paper proposed four broad policy principles: ● Develop a consistent, coordinated regulatory framework. ● Adopt a light regulatory approach. ● Regulation based on strong evidence. ● Avoid country specific regulations. And seven areas to accelerate IoT innovation: ● Facilitate development of international standards. ● Address spectrum issues. ● Promote a security by design approach. ● Protect consumers' data. ● Promote adoption of IPv6. ● Much public sector data freely available. ● Advocate free data flow across borders.

Figure 24-8: IoT Studies

24.3.2. EU studies

The European Union provides a range of initiatives and studies to support the development of IoT. A non-exhaustive search provided the following indicative list.

- **Digital Skills and Jobs Coalition.** This initiative by the European Commission aims to improve digital skills and promote employment opportunities in the digital economy. It includes a focus on IoT-related skills, such as data analytics and cybersecurity.
- **Erasmus+.** This program provides funding for education, training and youth activities in Europe. It includes opportunities for IoT-related training and courses, such as the "IoT and Industry 4.0" course offered by the Technical University of Cluj-Napoca in Romania.
- **European Network of Living Labs (ENoLL).** This network includes over 200 living labs across Europe that provide a platform for testing and validating IoT technologies in

[1688] "Why Countries Need National Strategies for the Internet of Things", Joshua New & Daniel Castro, December 2015. Link

[1689] "What Roles Should the Government Play In Fostering the Advancement of the Internet of Things?", Telecommunications Policy, Volume 43, Issue 5, 2019, Pages 434-444, ISSN 0308-5961, Gwanhoo Lee

© Strategy of Things, 2025. All rights reserved.

real-world settings. It includes opportunities for education and training in IoT-related skills and technologies.

- **SynchroniCity.** Focused on developing a global IoT market for smart cities by creating a common framework for data sharing and interoperability
- **IoF2020.** Developing IoT solutions for the agriculture industry such as smart farming systems and precision agriculture techniques
- **Digital Services Tax.** Under consideration to tax digital businesses that generate significant revenues in the EU but have a limited physical presence in the region
- **Horizon 2020**: Provides funding for research and innovation projects. The program offers funding options for IoT-related projects, including grants and loans. The IoT European Large-Scale Pilots Programme is part of Horizon 2020 and aims to support large-scale pilot projects for IoT applications in various sectors, including smart cities, agriculture and healthcare.
- **Radio Equipment Directive (RED).** This directive regulates the sale and use of radio equipment in the EU, including IoT devices that use radio frequencies for communication. It sets requirements for electromagnetic compatibility, safety and other technical standards.
- **Directive on Security of Network and Information Systems (NIS Directive)**. This directive came into effect in May 2018 and sets cybersecurity requirements for operators of essential services and digital service providers, including those that use IoT devices.
- **Regulation of Data Protection.** The General Data Protection Regulation (GDPR) protects the privacy and personal data of individuals.
- **IoT European Platforms Initiative (IoT-EPI).** A collaboration between the European Commission and several IoT platform providers.
- **Alliance for Internet of Things Innovation (AIOTI)**: This is a partnership between the European Commission and industry stakeholders. The focus is on driving IoT innovation in Europe and creating a market for IoT solutions.
- **IoT Security Foundation (IoTSF).** A non-profit organization based in the UK that aims to promote security in IoT. The foundation collaborates with partners across Europe to develop best practices and standards for IoT security.
- **IoT Acceleration Consortium (IOTAC).** A partnership between several Japanese and European organizations. The focus is on accelerating the development and adoption of IoT technologies through collaboration between the two regions.

24.4. Government opportunities to address key gaps

This section discusses the gaps identified in our research and maps them to the framework discussed earlier. Industry-specific gaps were identified in Sections 0 to 21. Section 22 identified several future technology gaps, that if addressed, support the evolution of IoT.

These individual gaps were then analyzed from a cross industry perspective, aggregated, prioritized and mapped against our predicted IoT evolution model described in Section 22.1.

© Strategy of Things, 2025. All rights reserved.

These consolidated gaps are further organized into three categories: Core, Intelligence and Hyper-Deployed. These gaps and their mapping are shown below in Figure 24-9.

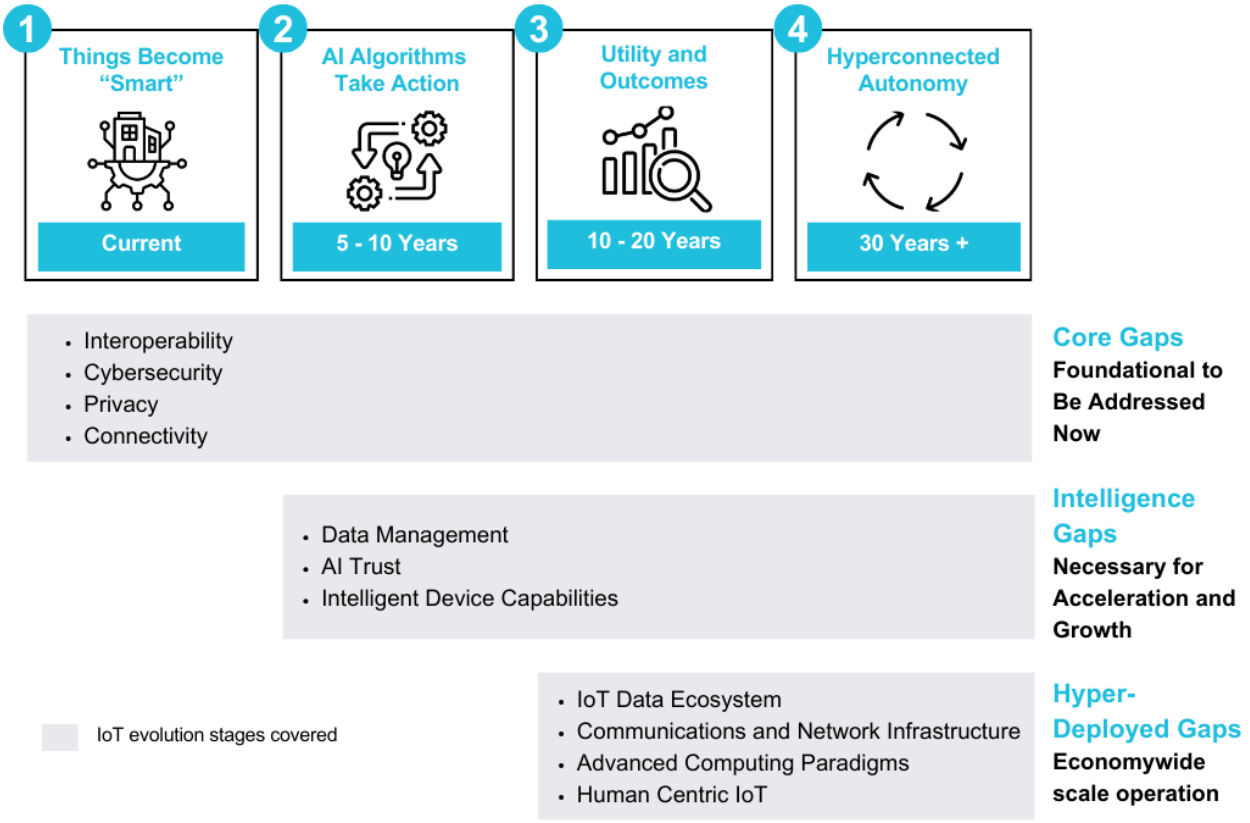


Figure 24-9: IoT Technology Infrastructure Gaps Mapped Against Four Stages of IoT Evolution

The consolidated and grouped gaps are mapped against the government opportunities framework as discussed in Section 24.2. These opportunities are discussed in the following subsections for each gap within the Core, Intelligence and Hyper-Deployed categories.

For each category, the potential government opportunities considered are organized into the five opportunity groups as shown in Figure 24-10.

Examples of government actions corresponding to each group are discussed briefly in Sections 24.4.1 to 24.4.3.

The remainder of this subsection discusses the policy actions from the perspective of each of the categories.

24.4.1. Government opportunities: Core gaps

The core category represents foundational IoT technology infrastructure gaps that should be addressed in the near term. They cover basic and foundational gaps that affect multiple industries. To be included as a core gap the technology needs to meet four criteria. These are:

- Affects multiple industries.
- Hinders current state of IoT functionality, adoption, scaling and value delivery.

© Strategy of Things, 2025. All rights reserved.

- Necessary for stages 2, 3 and 4 functionality and evolution.
- Provides an opportunity for government to play a strategic enabling role.

These gaps, along with a set of actions aligned to the framework are highlighted in Figure 24-10. The gaps that could be addressed in the near term include interoperability, cybersecurity, privacy and connectivity.

	Possible Government Opportunity				
IoT Gap (Core)	Develop Technology	Commercial enablement	Facilitate Market Adoption	Lead by Example	Broaden Economy wide Benefits
Inter-operability	Research	Standards Testbeds Partnerships	Promotion Grants	Procurement	
Cybersecurity	Research	Partnerships Standards	Promotion	Procurement Policies	Regulations Workforce
Privacy	Research	Standards Partnerships	Promotion	Procurement Policies	Legislation Regulations Workforce
Connectivity	Research	Infrastructure Policy	Promotion Grants	Procurement	Regulations

Figure 24-10: Core Gaps: Government Opportunities

24.4.1.1. Interoperability

This study's research identified interoperability as a gap in seven of the nine industries studied. Interoperability challenges hinder and prevent the ability of IoT devices to connect, communicate and collaborate with each other and with other systems in the industry ecosystem. Furthermore, interoperability challenges will hinder the scaling and evolution of the future IoT.

Interoperability is a long-running challenge. Achieving interoperability requires a long-term multi-stakeholder effort with active participation from buyers, manufacturers, consultants, academia and government. Some barriers to achieving interoperability include:

- **Limited focus of standards efforts.** Interoperability challenges are broad in scope. Many existing organizations, standards bodies and consortiums, focus on specific interoperability gaps, industries and functional areas.
- **Resistance to open and industry consensus standards.** Some solution providers promote proprietary protocols because they are well entrenched in legacy systems or they believe are technically superior. Others believe that open standards may lead to commoditization by making it easier for competitors to enter the market. Maintaining these protocols gives them a customer "lock in" advantage and above average profit margins.

© Strategy of Things, 2025. All rights reserved.

- **Regional standards.** Standards vary geographically, in compliance with country or regional approaches, policies and regulations. Harmonization of the different standards between regions is required, although it is a lengthy process.
- **Different implementations of standards.** While standards provide a common language or protocol that enables different systems to communicate with each other, how those standards are implemented determines the level of interoperability. Implementation differences may be due to interpretation of the standard, errors in implementation or intentional deviations from the standard for proprietary reasons.

Interoperability is a long-running challenge and the government has been involved with some of the activities identified above in Figure 24-10 for many years. There are, however, select opportunities where acceleration is possible. Some examples include:

- **Specification of interoperability needs in infrastructure and related grants.** Billions of dollars of "once in a lifetime" grants, arising from the Bipartisan Infrastructure Law, the Inflation Reduction Act and the CHIPS Act are available to industry and communities. These federal grants represent an opportunity for the federal agencies to specify and incorporate IoT systems and include provisions to consider those solutions and technologies that are built to industry consensus and open standards.
- **Specify interoperability requirements for IoT solutions for internal procurements.** The federal government has significant buying power and procures billions of dollars of products and services every year for use in agency operations. The federal government would do well to consider incorporating interoperability requirements for solutions and technologies that are built to industry-consensus and open standards.
- **Research the use and risks of Artificial Intelligence to facilitate interoperability.** AI models can assist in establishing semantic interoperability by its algorithms understanding the meaning of data elements. Ontology-based approaches, where AI models understand the relationships between different concepts, can be used to map and align data schemas, enabling seamless communication between systems. AI can help translate communication protocols between different systems, enabling different protocols to effectively communicate and exchange information. AI-powered systems can dynamically adapt to changes in the environment or data formats, ensuring continuous interoperability even as systems evolve.

24.4.1.2. Cybersecurity

Cybersecurity is core to the operation of IoT and the connected systems. Breaches of cybersecurity can lead to operational disruptions, loss of sensitive data and compromised IoT and system operation. These impacts are amplified as IoT systems are increasingly integrated into the economy, leading to a loss of trust and resistance to adoption and scaling. This study's research identified cybersecurity as a gap, appearing in four of the nine industries studied and frequently mentioned as an area of concern in the remaining five industries.

Many industries have cybersecurity concerns and these issues are long-running challenges experienced across many industries. It is difficult to fully eliminate cybersecurity risks for several reasons. These include:

© Strategy of Things, 2025. All rights reserved.

- **Wide range of devices and systems supporting diverse applications**. IoT devices come in various forms and have various capabilities, ranging from smart home appliances, wearables to industrial sensors. Most networks and environments have devices from multiple vendors. Each device type has its own unique specifications, hardware and software configurations, making it difficult to implement a one-size-fits-all security solution. In addition, the larger the multi-vendor and device environment, the more difficult it is to continuously manage, track and secure each of the devices.
- **Resource Constrained Devices**. Many IoT devices have limited computing power, memory and battery life. This restricts their ability to implement robust security measures such as encryption, authentication and intrusion detection, leaving them vulnerable to attacks.
- **Large numbers of unpatched devices**. The number of IoT devices in use is vast and growing. This makes it challenging for manufacturers and users to keep track of and manage all the devices on their networks and ensure they are properly secured. Some devices may lack over-the-air update capabilities, while others are in remote and hard-to-reach locations that make software updates impossible.
- **Legacy Systems**. There are millions of connected legacy devices that are built on outdated or proprietary operating systems and software platforms. Many of these systems were not built with cybersecurity in mind. Furthermore, other devices have reached end of life but are still in use and do not receive regular security updates or patches. This leaves them vulnerable to known exploits and other vulnerabilities.
- **Interoperability Issues**. IoT devices often need to communicate with each other and with other systems and services. Ensuring secure communication and interoperability between devices from different manufacturers can be complex and prone to vulnerabilities.
- **Lack of Standards**. The IoT industry lacks standardized security protocols and best practices, leading to inconsistencies in security implementations across different devices and manufacturers.
- **Human Factors**. IoT and connected devices may be exposed to vulnerabilities due to a variety of reasons. For example, the devices may be installed, integrated and configured improperly. Users may not have implemented the latest IoT cybersecurity best practices. Additionally, IoT devices are often deployed in physically unsecured environments where they may be easily tampered with or physically compromised.
- **Evolution of Threats**. Cyber threats targeting IoT devices are evolving, with attackers exploiting new vulnerabilities and attack vectors. This requires continuous monitoring and adaptation of security measures to stay ahead of emerging threats.

Our research and analysis identified areas where the federal government can facilitate cybersecurity as shown above in Figure 24-9. Select opportunities where acceleration is possible include:

- **Specification of cybersecurity provisions in smart infrastructure and related grants.** The previously discussed grants (BIL, IRA, CHIPS) represent an opportunity to specify cybersecurity measures and requirements.

© Strategy of Things, 2025. All rights reserved.

- **Grow the cybersecurity workforce.** The National Cyber Workforce Education Strategy[1690] was released in 2023 although implementing it will take time and funding. In addition, the previously discussed grants partially support the development of a cybersecurity workforce.
- **Specify cybersecurity requirements for IoT solutions for internal procurements.** The federal government should consider incorporating or expanding cybersecurity requirements and provisions into their procurements, where they have not done so already.
- **Research the use and risks of Artificial Intelligence to facilitate cybersecurity.** In addition to analyzing vast amounts of data to identify suspicious patterns and anomalies, AI has the ability to predict potential vulnerabilities and threats before they are exploited.
- **Fund research in advanced cybersecurity methods.** Representative examples include lightweight encryption algorithms, alternative approaches to cryptography such as "friendly jamming" that works with resource constrained devices, lightweight quantum safe algorithms, integration of blockchain with IoT and the use of privacy enhancing technologies in IoT.

24.4.1.3. Privacy

Privacy concerns appeared as a gap in four of the nine industries examined here. Privacy challenges include the unauthorized collection, storage and use of data, unauthorized disclosure of private information through theft and data sharing, as well as the misuse of private information. These challenges are exacerbated as IoT systems are increasingly integrated into the economy, leading to a loss of trust and resistance to IoT adoption and scaling. Figure 24-10 above shows some areas where the federal government can help to facilitate privacy.

Providing and maintaining privacy is a complex long running challenge for IoT systems and devices and it is difficult to achieve for several reasons. These include:

- **Fragmented regulatory environment**. Although there is no national comprehensive privacy legislation implemented in the United States, a number of states have some level of privacy legislation. For example, the California Consumer Protection Act (CCPA) requires companies operating in California to provide consumers with transparency and control of their personal data. Other states, such as Colorado, Hawaii, Louisiana, Illinois, Maine, Nevada, North Dakota, Texas and Virginia have also recently enacted data privacy laws.[1691]

  Further, data flows across borders. Different jurisdictions have varying regulations and cultural norms regarding data privacy protections. IoT products offered in the European Union must comply with the EU's General Data Protection Regulation (GDPR). This complicates efforts to harmonize data standards and enforce them consistently on an international basis. The different regional regulations create a challenge for IoT solution

[1690] See note 1677

[1691] "Data Use, Privacy and Technology", National Association of Insurance Commissioners, February 22, 2022. Link

© Strategy of Things, 2025. All rights reserved.

vendors as well as adopters, who must navigate the different legal requirements to stay in compliance.

In addition, privacy protection is subject to industry level regulations in some industries. For example, medical devices administered by healthcare providers must comply with HIPAA. Similarly, the insurance industry is regulated at the state level, resulting in differences that vary state by state. Insurance companies in California offering insurance products based on vehicle telematics can only consider mileage and not driver behavior as risk factors.[1692]

- **Continuing risk of cybersecurity attacks.** Cybersecurity breaches of IoT devices and systems allow cybercriminals to access and steal personal, confidential and proprietary data. This leads to the theft and disclosure of data, resulting in identity theft, financial fraud, loss of intellectual property and reputational damage. The risks of data theft will continue as cybersecurity threats evolve. As discussed in Section 23.1.2, cybersecurity threats are a long-running challenge across multiple industries and difficult to eliminate for a variety of reasons.
- **Organizations are incentivized to collect, use and share data.** The value provided by data creates incentives for individuals and organizations to prioritize data collection and sharing over user privacy. IoT systems collect data that have valuable benefits for users, solution providers and other third-parties.

  For example, retailers use IoT collected data to monitor how shoppers move around their stores, informing managers where to place the right types of merchandise to maximize sales. Insurance companies use the data collected from in-vehicle sensors to determine the driving behavior of their policyholders to price their insurance products better and reduce underwriting risk. Cities use cameras to detect crime in public areas and identify suspects. For IoT solution providers, monetizing the collected data diversifies revenue sources and increases profitability.

  The rise of big data collection and the use of artificial intelligence have led to the collection and analysis of vast amounts of personal information. AI algorithms often rely on extensive datasets to function effectively, raising concerns about how to balance innovation with privacy protection.
- **Inadequate Consent Mechanisms**. Unlike websites which offer a way for users to allow or decline tracking, there is no practical way for subjects and users to provide meaningful consent for data collection in the IoT context. For example, there is no meaningful way for a shopper or a city resident to give consent to be tracked in a store or in a city downtown, as well as to specify what they would allow to be tracked. In addition, current consent mechanisms are presented in lengthy legalese on a “take it or leave it” basis at the point of interaction. Many users are unaware of the extent to which their IoT devices collect and share data. Even if they are aware, they may not have sufficient control over

[1692] Research interview with Ryan Briggs, Vice President, Automotive and Mobility Solutions, Swiss Re, October 5, 2022

© Strategy of Things, 2025. All rights reserved.

how their data are used or shared, as privacy settings may be buried in complex user interfaces or be difficult to customize.

- **Deanonymization through data aggregation**. IoT devices generate data at a massive scale and these data are often aggregated with data from other sources to derive insights or provide personalized services. While IoT data may have been collected in a manner that is not be personally identifiable or is anonymized during processing, the aggregation of data from various sources may lead to the deanonymization and identification of individuals and their behaviors, posing significant privacy risks.

Ensuring and maintaining privacy is a complex challenge and governments have been involved with many of these activities. Some examples of opportunity to protect privacy include:

- **Enact a national comprehensive privacy legislation.** Privacy laws in the United States are currently a mix of federal and state laws covering specific topics.[1693] At the federal level, there are HIPAA (healthcare), FCRA (credit), FERPA (education records), GLBA (consumer financial), ECPA (communications), COPPA (child data), VPPA (VHS rentals) and the FTC Act (app/website privacy).

  At the state level, three states, California, Colorado and Virginia, have comprehensive data privacy laws.

  Enacting a national level comprehensive privacy law promises to help reduce confusion, simplify compliance and alleviate IoT privacy concerns.
- **Promote and advocate for Privacy by Design.** This concept emphasizes integrating privacy into products, services and system designs from the start.

  While privacy-by-design is incorporated as one of three core principles of the FTC privacy framework[1694] and its principles inform the NIST privacy framework,[1695] adoption of privacy by design concept in the United States is not widespread. Many organizations still prioritize functionality and convenience over privacy considerations, especially in sectors where data-driven decision-making and targeted advertising are prevalent.

  Additionally, smaller organizations with limited resources may struggle to implement comprehensive privacy by design practices.

  While national comprehensive privacy legislation is being considered, ongoing efforts are

[1693] "The state of consumer data privacy laws in the U.S. (and why it matters)," T. Klosowski, Wirecutter, September 6, 2021. Link

[1694] "Privacy By Design and the New Privacy Framework of the U.S. Federal Trade Commission," E. Ramirez, Public Statement, United States Federal Trade Commission, June 13, 2012. Link

[1695] "The NIST Privacy Framework: A Tool for Improving Privacy through Enterprise Risk Management", U.S. National Institute of Standards and Technology, January 2020. Link

© Strategy of Things, 2025. All rights reserved.

needed to raise awareness, provide guidance and incentivize organizations to prioritize privacy in their operations.

- **Fund and conduct technology research to address IoT privacy challenges.** While legislation and privacy by design may address some privacy challenges, research in new privacy protection technologies is needed due to the ongoing growth and integration of IoT devices into the economy and civil society.

  Continuing research is required to develop innovative technologies and methods, including advanced encryption techniques, privacy-preserving data analytics, decentralized architectures and user-centric privacy controls tailored to the unique challenges posed by IoT systems. These privacy protection technologies are needed to foster trust among users, encourage widespread adoption of IoT technologies and realize the potential of the IoT ecosystem while maintaining user privacy and autonomy.

24.4.1.4. Connectivity

IoT systems and other smart equipment rely on connectivity to send their data to edge servers and remote data centers in the cloud for processing and storage. While connectivity challenges were identified in agriculture and manufacturing, the lack of connectivity availability and service in rural and underserved communities affects other local industries operating in those areas. For example, the lack of connectivity prevents the development of IoT enabled healthcare services in those communities. For this reason, connectivity challenges have been included as a core gap.

Connectivity challenges are multi-dimensional in nature and challenging to solve due to various factors, including:

- **High infrastructure investments.** Extending broadband coverage to underserved or unserved areas often requires significant infrastructure investment including laying fiber-optic cables, deploying wireless towers or upgrading existing network infrastructure. The cost of deploying broadband infrastructure can be prohibitive, particularly in rural or remote areas with low population density.
- **No "one size fits all" approach.** Population densities, geographic and terrain constraints, usage applications, regulatory issues, technical capabilities and cost effectiveness considerations dictate what approaches are used by IoT infrastructure providers. For example, fiber provides high capacity and reliability but is expensive to build and deploy. Wireless approaches work well in areas with high population densities. Satellite use is ideal for remote and rural areas but suffers from latency, bandwidth and capacity constraints. Niche approaches such as TV white spaces and powerline communications fill the gaps where other approaches are not suitable for specific application areas. These approaches have limitations in terms of speed, latency and reliability compared to traditional fiber broadband.
- **Market economics.** In areas with low population density or limited market demand, broadband providers and wireless carriers are reluctant to invest in infrastructure deployment due to concerns about the profitability of serving these areas. The high upfront costs and uncertain return on investment can deter private sector investment in underserved regions.

© Strategy of Things, 2025. All rights reserved.

- **Funding and incentives.** Government funding programs, such as grants, subsidies and tax incentives play a crucial role in accelerating broadband deployment in underserved areas. For example, the Bipartisan Infrastructure Law provides $65 billion in funding to address connectivity challenges of which a portion is allocated to build infrastructure while the rest is used to lower the cost of Internet service.[1696] Securing adequate funding and designing effective incentive mechanisms to encourage private sector investment in broadband infrastructure is however, another challenge. California is facilitating the creation of private sector "last mile" services in underserved areas by building a $6 billion middle mile fiber network for last mile connections.[1697]
- **"Last Acre" coverage.** Bringing broadband to a community is rarely sufficient. Many IoT applications need to operate in areas where wireless coverage is not available. For example, agricultural fields span thousands of acres but have no wireless coverage even if there is broadband at the farmhouse. Other applications requiring "last acre" connectivity include environmental monitoring, forest monitoring and management and remote infrastructure monitoring for electrical, oil and water infrastructures. Market economics, geography and terrain along with technical considerations of various approaches hinder the resolution of this issue.

  There is no one universal "last acre" connectivity protocol for IoT devices. Technical considerations dictate which protocol should be used. For example, a moisture sensing device on a farm connects to the Internet through a low power long range connectivity network using LoRaWAN, LTE-Cat M1 or NB-IoT protocols. A video-based application requires higher bandwidth and throughput and connects through a 4G/LTE network.

  "Last Acre" considerations also need to ensure that both the connectivity service is available and that the appropriate service protocols are available to support IoT applications in the field.
- **Spectrum challenges**. As the use of IoT grows and new IoT applications emerge, concerns about spectrum availability arise. Spectrum is finite and inadequate regulatory frameworks, spectrum allocation policies and funding mechanisms slow efforts to expand access to connectivity and increase IoT adoption. Addressing spectrum policy and regulatory barriers requires coordinated action at the local, state, national and international levels.

Figure 24-10 above shows some areas where there are opportunities for the federal government to facilitate connectivity. Key policymaking opportunities to address connectivity challenges include:

- **Service availability.** Ensuring reliable and ubiquitous connectivity remains a challenge, particularly in remote or rural areas where private carriers are not present or available.

  Policymaking opportunities could focus on ubiquitous connectivity coverage, expanding

[1696] See note 313

[1697] See note 1435

© Strategy of Things, 2025. All rights reserved.

both broadband infrastructure and affordability of service. The Bipartisan Infrastructure Law provides a unique opportunity and funding to close the "digital divide." The "Last Acre" Act, introduced by Senators Deb Fischer and Ben Ray in 2023, aims to bring connectivity coverage to the field in support of precision agriculture.[1698]

- **Spectrum.** IoT devices operate on wireless networks, competing for limited radio frequency spectrum. Although spectrum challenges are less of an issue in rural communities, they are critical in dense urban areas. Spectrum allocation becomes an ever-present issue as the increasing number of IoT devices exacerbates congestion and interference problems.

  Efficient spectrum management and allocation policies are needed to accommodate the growing demand for IoT connectivity while minimizing interference and ensuring fair access for all users.
- **Technology.** To support the scaling and evolution of IoT use in its many permutations, research is needed to develop and refine new and existing communications and connectivity technologies. These will help address the infrastructure gaps of broadband ubiquity and "last acre" coverage as well as the evolving connectivity capabilities to address future IoT needs.

  Research opportunities exist in improving the performance of existing and niche connectivity methods, spectrum sharing and management, interference management, energy efficient connectivity approaches and the Beyond 5G (6G) technologies.

  Other areas include spectrum-efficient communication technologies, innovative network architectures, security and privacy enhancements and interoperability standards.
- **Regulatory Frameworks and Standards.** Regulatory frameworks and standards promote the development and deployment of IoT connectivity technologies, foster innovation and safeguard public interests.

  Regulatory agencies such as the Federal Communications Commission (FCC) and the National Telecommunications and Information Administration (NTIA) enact rules and standards to ensure spectrum efficiency, interoperability, security and privacy in IoT networks.
- **International Collaboration and Coordination.** International collaboration and coordination efforts are essential to harmonizing spectrum policies, promoting global interoperability standards and addressing cross-border challenges in IoT connectivity.

  Through participation in international forums, conferences and standards bodies, the government can collaborate with international partners to develop common frameworks, resolve regulatory conflicts and facilitate seamless connectivity for IoT devices worldwide.

[1698] See note 1554

© Strategy of Things, 2025. All rights reserved.

24.4.2. Government opportunities: Intelligence gaps

The Intelligence category represents key IoT technology infrastructure gaps that need to be addressed to enable an intelligent and autonomous future IoT. To be included as an intelligence gap the technology needs to meet four criteria. These are:

- Basic and foundational gap that hinder value realization from data.
- Necessary for stage 3 and 4 functionality and evolution.
- Affects multiple industries.
- Opportunity for government to play a strategic enabling role.

The gaps that meet these criteria are:

- Data management
- AI trust
- Intelligent device capabilities

24.4.2.1. Data Management

Adequate data management was identified as a gap in transportation and logistics and renewable energy. However, in its robust form, it is also an enabler for the three other industries of insurance, retail and healthcare where the use of artificial intelligence was identified as a gap.

As IoT scales, the ability to manage the collected data is critical. Robust data management capabilities help unlock the value of IoT by enabling massive amounts of data to be collected, processed, stored and analyzed. Without these capabilities, IoT deployments face many challenges such as data silos, scalability issues and compromised data integrity.

Furthermore, robust data management becomes foundational for the deployment of artificial intelligence systems. Robust data management helps ensure the availability, accessibility, quality and security of data, laying a foundation for the use of AI applications to generate effective decisions and relevant outcomes. Moreover, overall well-managed data facilitates the development and use of more accurate and reliable AI systems, leading to better predictions, recommendations and automation across various domains.

Addressing data management challenges for IoT is not easy and is complicated by a number of factors. These include:

- **Exponential growth in data volume and velocity.** As billions of IoT devices are added across the economy and society, the massive amounts of streaming data generated require data management technologies to innovate and evolve. These technologies must not only be robust enough to handle the scale and speed at which information is produced but must also make that information available to systems that need to act on it in real-time. In addition, as more devices are adopted, data aggregation and analysis are made more difficult as the devices create data in diverse formats and protocols, requiring the development of advanced tools and strategies to process the data.
- **Privacy considerations.** The collection and use of Personally Identifiable Information (PII) is a long-running concern for IoT. These concerns are further amplified as IoT data

© Strategy of Things, 2025. All rights reserved.

are increasingly used to train and refine AI algorithms. As more IoT devices become AI-enabled, these concerns continue to escalate. Ensuring that these data are handled in a way that respects user privacy is a complex task. Limiting the data used to train AI may result in biased and non-representative data sets, resulting in poor model outcomes. Furthermore, varying privacy laws and regulations, which can differ significantly between regions, complicate the collection, treatment and processing of IoT data.

- **Security.** IoT devices are resource constrained and often operate in environments with limited security measures, making them vulnerable to cyberattacks. For instance, many IoT devices lack robust encryption protocols, leaving data exposed to potential breaches. The volume of data generated by these devices further complicates the task of securing it, as traditional security measures may not scale effectively.
- **Interoperability.** This is a long running challenge for IoT. The IoT ecosystem is highly fragmented and heterogeneous, with numerous manufacturers and platforms. As IoT adoption grows and new use cases appear, interoperability challenges will continue to escalate. While there are many efforts around the development of standards, interoperability challenges will continue. These challenges make it difficult to integrate devices and systems, extract and share data seamlessly.
- **Regulatory compliance.** The rapid pace of IoT innovation often outstrips the development of regulatory frameworks. This lag can create uncertainty for businesses and government agencies as they may not have clear guidelines t. Additionally, the global nature of IoT means that compliance with international regulations is necessary, adding another layer of complexity. Regulations may be enacted on a local or regional level, resulting in inconsistent or conflicting regulations that affect the treatment of data.

There are extensive existing industry efforts to develop commercially available market solutions from a variety of data management solution providers. However, the convergence of AI with IoT and the future pervasiveness across the economy creates a sense of urgency to accelerate the development of "beyond big data" data management approaches and technologies for users and researchers. Given the strategic importance of data management to IoT, the federal government would do well to focus on research and commercialization enablement efforts around novel and innovative "beyond big data" technologies and architectures that support the future of a scaled up, hyperconnected, decentralized and autonomous IoT ecosystem (Figure 24-11).

Some example and representative areas for federal research to augment and accelerate industry efforts discussed previously in Section 23.2.1 include:

- **Scalable and efficient data storage.** Innovative and more effective approaches are needed to manage the increasing volume of data. For example, distributed storage architectures, compression techniques and data deduplication methods to improve storage efficiency.
- **Real-time data processing.** Research into ways to enhance real-time and energy efficient processing of IoT-generated streaming data including advanced algorithms, edge computing and in-memory processing techniques is relevant.
- **Security and privacy.** Research into methods and approaches to protect a diverse set of data that are increasingly stored on distributed devices, mobile and edge systems, as well

© Strategy of Things, 2025. All rights reserved.

as data that are streamed to other systems is important. Opportunities to consider include encryption techniques, access control mechanisms and privacy preserving analytics.

- **Data quality assurance methodologies.** Approaches to ensure the accuracy and reliability of IoT-generated data, such as developing calibration techniques for sensors, anomaly detection algorithms and data validation processes.
- **Data governance.** Data oversight and management is increasingly important as separate parties own their data which are subject to a variety of industry and government regulations, such as HIPAA (healthcare), and the Gramm-Leach-Bliley Act (consumer financial information). New approaches and mechanisms are needed to govern changes as data are increasingly distributed and decentralized.
- **Lifecycle management of IoT data.** As new IoT applications emerge and industry adoption increases, the management of the distributed and decentralized data, from attribution, traceability, collection, storage, processing, analysis and archiving becomes more important.
- **Data fabric architectures.** As data sources and creators are increasingly decentralized and distributed on a massive scale, future scalable architectures to interconnect and access this data are required.

24.4.2.2. AI Trust

Our research identified the trust of AI as a gap in the insurance, retail, healthcare and transportation and logistics industries. It is also an important capability in the industries of agriculture, smart cities and renewable energy.

The integration and use of AI algorithms with IoT devices and systems enables users to extract insights from the collected data. The use of AI in this capacity enables IoT devices to analyze data streams in real-time, identify patterns, predict outcomes, make intelligent decisions and take autonomous action without human intervention.

The convergence of artificial intelligence use with IoT enhances the efficiency, responsiveness and agility of overall IoT deployments. This enables proactive maintenance, resource optimization and personalized user experiences.

Further, where employed, AI-driven analytics enable continuous learning and adaptation, allowing IoT systems to evolve and improve over time, leading to more accurate predictions and better resource utilization.

Despite its transformational potential, establishing trust in AI-enabled IoT systems is complex due to a variety of technical, human and societal factors. Some major complicating factors include:

- **Human reluctance and resistance.** People factors complicate the deeper integration and use of AI with IoT. For example, people are concerned with the loss of control when AI is used to manage and automate critical operations because they are taken “out of the loop” for decision-making and overriding key actions. Another factor is the perception of bias and fairness. Even when AI operates without human intervention, its outcomes can reflect societal inequalities, creating a perception that AI is biased. Finally, a lack of transparency in how a “black box” AI model arrived at a decision and course of action creates uncertainty and suspicion in AI and its outcomes.

© Strategy of Things, 2025. All rights reserved.

- **Unclear and uncertain accountability and liability.** In cases where AI makes decisions autonomously, such as in IoT applications for autonomous vehicles or smart industrial systems, determining responsibility when things go wrong is unclear. If an AI-enabled IoT system makes a harmful decision, it's often difficult to determine who is accountable: the developer of the AI, the manufacturer of the device or the user? This ambiguity creates trust issues, as users are uncertain about who will take responsibility in case of failure or harm. Many of the frameworks, policies, best practices and regulations have not yet been developed as the technology and use cases continue to evolve.
- **Lack of standardized guidelines for AI development and deployment.** Without clear standards, there is inconsistency in how AI and AI-enabled systems are designed, tested and implemented, leading to varying levels of reliability and safety. This inconsistency makes it difficult for users to trust that AI systems will perform as expected, especially in critical applications like healthcare or autonomous vehicles. Additionally, the lack of standards complicates efforts to ensure transparency and accountability as there are no uniform benchmarks for explainability or ethical considerations. As a result, users and stakeholders may be hesitant to fully embrace AI technologies, fearing potential biases, privacy violations or unpredictable behavior.
- **Ethical dilemmas arise from AI outcomes.** AI systems can embed biases, amplify inequalities and produce unintended harmful outcomes. AI models learn from historical data, which often reflects existing societal biases. If these biases are not properly addressed, AI systems can reinforce discrimination based on race, gender, age or socioeconomic status. Moreover, ethical dilemmas emerge when AI systems make decisions that affect people's lives, such as in criminal justice, hiring or healthcare.

  Deciding how to program AI systems to align with diverse ethical values and ensure fairness across different populations is complex, especially when ethical principles vary between cultures and contexts. Furthermore, the lack of clear legal and regulatory frameworks for AI governance exacerbates these challenges.

Our research and analysis identified broad areas where the federal government has the potential to facilitate trust in artificial intelligence. Figure 24-11 shows areas where the federal government could address AI trust challenges and includes:

- **Research and development**. As AI technology advances across various fronts, continued U.S. research is necessary to maintain global AI leadership and ensure the development of safe, ethical, fair, transparent and explainable AI.
- **Governance and oversight.** The federal government should play a leading role in research on establishing effective governance frameworks and structures to oversee AI adoption, thus ensuring transparency, accountability and ethical use.
- **Privacy and security.** AI adoption and use relies on a continuous pipeline of collected data for training and model development. Data collected from IoT systems that are employed in many areas will likely be subject to privacy concerns and restrictions. Taking a balanced approach to AI-driven insights and privacy protections and unauthorized use of data is a key challenge.

© Strategy of Things, 2025. All rights reserved.

- **Bias and fairness.** AI algorithms have the potential to lead to results that are inaccurate, biased, irrelevant or discriminatory. The underlying processes in how data are collected and algorithms tested are fundamental. Addressing bias, fairness and ethical use is a key challenge.
- **Workforce considerations.** The use of AI may translate to job displacement and the creation of new roles in which human-AI collaboration is essential. In addition, development of a skilled AI workforce is necessary to complement innovation acceleration and deliver on the promise of economic and social benefits.
- **Interagency coordination.** Coordinating efforts across agencies to promote consistency and sharing is important to policy development.
- **International cooperation.** Current and future AI use cuts across international borders. For the United States, collaborating with other nations is important to set global standards, prevent misuse and address cross-border challenges.
- **Regulatory framework.** AI use and deployment is advancing into aspects of our industry, government and society. Crafting federal policies that encourage innovation while safeguarding against the possible risks posed by AI applications is an important role for U.S. policymakers.

24.4.2.3. Intelligent device capabilities

Our research identified limited device capabilities as a gap in enabling and supporting the ability of IoT devices to process and analyze data. On-device and edge processing of data is increasingly common and is required for applications that are autonomous, latency sensitive or operate in an area with unreliable service. Other applications requiring on-device and edge processing include IoT device swarms and ambient IoT use cases that require contextual information obtained by communicating with other nearby devices.

Section 23.2.3 discussed some specific and needed capability gaps. This includes the need for AI-ready processors capable of supporting complex applications while minimizing power consumption and efficient AI algorithms capable of operating on resource constrained devices.

Developing IoT devices capable of supporting AI is challenging due to several factors:

- **Physical limitations.** IoT devices running AI models require microprocessors that have significant processing capabilities. However, as microprocessors become more powerful, they require more energy to operate, which is a significant constraint for devices powered by batteries. In addition, more powerful microprocessors generate more heat, which may not be easily dissipated due to the device's small size and could affect the device's operating performance and life. Developing viable AI capable IoT devices requires balancing multiple trade-offs.
- **Complex programming requirements.** Developing lightweight algorithms for resource-constrained IoT devices is challenging. Algorithms must be designed to operate efficiently with limited computational resources while minimizing energy usage and supporting real-time data processing with limited ability to store data. Leading edge advances in model compression techniques, efficient neural network architectures and hardware acceleration are needed.

© Strategy of Things, 2025. All rights reserved.

- **High upfront development costs.** Developing low-cost AI-capable microprocessors for IoT devices is expensive. The costs primarily come from research and development, fabrication and the need for specialized hardware and software tools. To reduce these costs, advances such as improved design methodologies, more efficient AI algorithms and better fabrication techniques are needed.

While there are existing commercial development efforts and solutions for the development and use of intelligent devices from semiconductor and microprocessor suppliers, these efforts are focused on short term objectives. To enable and support a future scaled up, hyperconnected and autonomous IoT ecosystem, the federal government would do well to support and focus on the research and commercialization of advanced approaches.

Our study's research and analysis identified broad areas where the federal government can play a central role to facilitate the development of intelligent devices as shown below in Figure 24-11. Some examples include:

- **Research and development.** One focus that the federal government already employs is to fund and perform basic and applied research on the enabling technologies and infrastructure needed for the United States. An emphasis on IoT infrastructure and enabling technologies promises to have ripple effects across the economy and broader societal benefits. These areas of research may not necessarily be an area of focus for industry as they are concentrated on nearer term research investments and outcomes. (Research)
- **Leverage tech hubs to innovate.** As one example of a federal initiative, the government has established thirty-one tech hubs across the country. These "tech hubs" bring together private industry, state and local governments, institutions of higher education, labor unions, tribal communities and non-profit organizations"[1699] to make transformative innovation investments. (Research, Commercial enablement)
- **Incentivize industry collaboration.** There are government incentives for existing federal programs. Here, the government can and does provide similar incentives for industry players to collaborate with research institutions and startups on IoT R&D projects. For example, the NSF Regional Innovation Engines facilitate the development of ecosystems that collaborate on innovation around certain critical areas.[1700] Available methods include tax incentives, grants or public-private partnership programs that encourage knowledge sharing and technology transfer. (Research, Commercial enablement)

[1699] "FACT SHEET: Biden-Harris Administration Announces 31 Regional Tech Hubs to Spur American Innovation, Strengthen Manufacturing and Create Good-Paying Jobs in Every Region of the Country," Fact Sheet, The White House, October 23, 2023. Link

[1700] "About NSF Engines." U.S. National Science Foundation. Link

© Strategy of Things, 2025. All rights reserved.

	Potential Government Opportunities				
IoT Gap (Stage 2)	Develop Technology	Commercial enablement	Facilitate Market Adoption	Lead by Example	Broaden Economy wide Benefits
Data Management	Research Technology Transfer	Partnerships Standards Pilots Testbeds			
AI Usability	Research Technology Transfer	Partnerships Standards Pilots Testbeds Sandboxes Infrastructure Policy	Promotion Tax incentives	Procurement	Workforce Development, Regulations
Intelligent Device Capabilities	Research Technology Transfer	Partnerships Standards Pilots Testbeds Infrastructure	Promotion	Procurement	

Figure 24-11: Intelligence Gaps: Government Opportunities

24.4.3. Government opportunities: Hyper-Deployed gaps

The future IoT-enabled economy and society may contain billions of interconnected devices working autonomously in a secure and trusted manner. To realize the Hyperconnected Autonomy future described in Section 22.1, today's communication networks and infrastructures need to develop characteristics to support real-time autonomy and complex IoT applications at scale, become fault tolerant and resilient and be able to defend and heal against security threats.

The technological developments seen as necessary to support this future state IoT infrastructure are discussed in detail in Section 23. Key desired elements of these currently unavailable technologies are represented as gaps that need to be addressed to support a hyper-deployed IoT ecosystem. These technology infrastructure gaps include:

- IoT data ecosystem.
- Communications and network infrastructure.
- Advanced computing paradigms.
- Human centric IoT systems.

These hyper-deployed gaps were determined based on the following possible solution:

- Enabling infrastructure to equip future IoT at hyper-deployed.

© Strategy of Things, 2025. All rights reserved.

- Enabling infrastructure to support multiple industries.
- Forward looking innovations with limited industry activity.
- An opportunity for acceleration by governments.

Developing the next-generation technology infrastructure to support the hyperconnected and autonomous state of IoT is challenging for a variety of reasons. Some of these reasons include:

- **Development of technological innovations is a complex undertaking.** Technological advances are dynamic and sometimes evolve unpredictably. For example, the current state and use of AI. Many of these advances were made possible in recent years by the emergence of deep learning, particularly many layered neural networks, which has revolutionized AI by enabling machines to recognize patterns and make decisions with unprecedented accuracy.

  However, other promising innovations under development never reach viability for adoption because they are superseded by newer technological innovations or suffer limitations that make it technically unattractive. Still others employ proprietary technologies that slow wider acceptance.
- **High and risky investments with uncertain returns.** Developing next-generation technologies often entails risk and requires significant investment in research and development, infrastructure and skilled personnel. These investments may be used to develop unproven approaches and do not have a near term return on investment and limited applicability to current technology portfolios. As a result, only the largest organizations, with a forward-looking mindset, can afford to prioritize and make long-term research and development investments in future technology.
- **Lack of skills and resources.** There is often a mismatch between the skills required for new technologies and the skills available in the workforce. The research and development of novel and innovative technologies often requires new expertise and knowledge. This skills and knowledge gap can slow the effective implementation and utilization of new technologies.

  Many next-generation technologies require expertise from multiple disciplines. For example, advances in wireless communications (like 5G and beyond) involve knowledge in hardware, software, network architecture and spectrum management.
- **Regulatory and standardization.** New technologies often outpace existing regulations and standards creating a lag between technological capability, standards and legal and policy frameworks. This can slow down the deployment and adoption of new technologies. For example, the advancement of AI technologies can potentially be hindered by concerns over safety, ethics, fairness and liability. Without a framework to address these concerns, AI technologies may never reach their envisioned potential and beneficial outcomes.

© Strategy of Things, 2025. All rights reserved.

Addressing these gaps requires forward looking actions by the federal government. Figure 24-12 below identifies some areas of opportunity in which the federal government might act and decisively change the present and future IOT landscape.

Key opportunities and considerations for the federal government to address challenges of building a future IoT technology infrastructure include:

- **Funding and performing research.** The technological innovations to enable the Hyperconnected Autonomy future may not yet exist although they may be envisioned by a scientist and experimented with at bench scale or at an early pilot stage.

  A key role for the federal government is to continue supporting scientific research, helping to establish a vision and providing supportive funding to create enabling technologies and infrastructure for IoT.

  As a general policy prescriptive, federal investments have previously and currently helped to accelerate development in research areas that may not be undertaken by private industry given their focus on near term returns, alignment with existing technology and current intellectual property portfolios.
- **Enable supporting infrastructure.** The future state of IoT relies on a modern communications and computing infrastructure to support AI deployment and autonomous IoT workloads at scale. These applications impose high performance requirements for IoT infrastructure as they are required to support high throughput, low latency traffic and distributed and scalable high performance computing resources. Without this IoT infrastructure in place, the full benefits of a hyperconnected autonomous future will not be realized.

  The opportunities for government involvement include facilitating infrastructure buildout comprising of spectrum allocation, funding public-private partnerships and policies and initiatives to facilitate access and availability. One current example of the federal government's role is in enabling FirstNet, a dedicated first responder network.
- **Development of policies and regulations for an emerging future.** While innovative and emerging technologies often bring transformational benefits, they are often accompanied by unforeseen outcomes. One key role that the government plays in research fields is in the development of frameworks, policies and regulations to help facilitate innovation and beneficial outcomes.

  Emerging technologies for a range of scientific fields, however, represent a challenge for policymakers because "they don't know what they don't know." One example of an acceleration opportunity for the federal government to undertake is the development of regulatory-innovation sandboxes that allow these innovations and policies to be tested and evaluated. These practices facilitate understanding, foster industry-government collaboration and inform the development of effective policies and regulations.

  Another area of opportunity for government action is research on the ethical, social and cultural implications of advanced and autonomous IoT technologies to inform policy and regulation development. Topics may include issues related to privacy, surveillance,

© Strategy of Things, 2025. All rights reserved.

discrimination, bias and inequality.

- **Build the future workforce.** The evolution of IoT requires a workforce capable of supporting, using and benefiting from hyperconnected and autonomous applications. While there are ongoing concerns that the unchecked proliferation of AI and autonomous applications will lead to job losses, interested parties understand that the new jobs created will require human-AI collaboration. For example, people and cobots work together today in a limited capacity to assemble and produce products.[1701] Section 23.3.4 discusses the need to design systems and solutions for human-AI collaboration.

  In anticipation of human-AI collaboration at scale, there exist opportunities for the federal government to consider strategies, policies investments and other actions and initiatives that build capability and skills in the future workforce.
- **Support standards development.** Implementation of standards and interoperability are critical to the realization of the hyperconnected and autonomous future state of IoT. The federal government supports standards development through research, development of frameworks, convening of stakeholders and facilitating industry cooperation to develop consensus standards.

  In addition, the federal government engages in multilateral forums, international organizations and bilateral agreements to harmonize standards, share best practices and coordinate regulatory approaches. While the federal government's approach to standards is "industry-leads, government supports", development of standards for the hyperconnected IoT autonomy provides opportunities for the government to play a more active role in matters pertaining to safety, liability and other major factors.

		Potential Government Opportunities			
IoT Gap (Stages 3 and 4)	Develop Technology	Commercial enablement	Facilitate Market Adoption	Lead by Example	Broaden Economy wide Benefits
IoT data ecosystem	Research Technology Transfer	Partnerships Standards Pilots Testbeds Infrastructure Policy	Promotion		Workforce Development

[1701] See note 1625

© Strategy of Things, 2025. All rights reserved.

	Potential Government Opportunities				
IoT Gap (Stages 3 and 4)	Develop Technology	Commercial enablement	Facilitate Market Adoption	Lead by Example	Broaden Economy wide Benefits
Communications and network infrastructure	Research Technology Transfer	Partnerships Standards Pilots Testbeds Infrastructure Policy	Promotion	Policies	Workforce Development
Advanced computing paradigms	Research Technology Transfer	Partnerships Standards Pilots Testbeds Infrastructure Policy	Promotion	Policies	Workforce Development
Human centric IoT	Research Technology Transfer	Partnerships Standards Pilots Testbeds Infrastructure Policy	Promotion	Policies	Workforce Development Regulations

Figure 24-12: Hyper-Deployed Gaps: Government Opportunities

© Strategy of Things, 2025. All rights reserved.

Appendix: Economic Analysis and Data Integration

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

© Strategy of Things, 2025. All rights reserved.

25. Appendix: Economic Analysis and Data Integration

This appendix details the economic analysis along with the method to integrate the data collected from desk research, interviews and the survey.

This analysis provides a ranking of the 25 single technology components based on their economic impact adjusted by the role of the public sector. This ranking is then used to estimate the impact of the most important IoT single infrastructure component. These single technology components are then combined to estimate the economic impact of addressing IoT infrastructure technology gaps that can be remedied by public investment in the United States.

The section covers:

- **Economic benefits of IoT to the United States.** Estimating the long-term economic impact of IoT in each of the selected industries. This figure is used to adjust the rankings provided by the data obtained from the survey, desk research and interviews.
- **Data integration for each industry.** The quantitative integration of all data collected from surveys, desk research and interviews.
- **All industry technical weighting.** The cumulative weighted results of the nine industries. These results are adjusted by both economic impact and the role of the public sector.
- **Sensitivity analysis.** A Monte Carlo analysis on the most important cross industry results which shows overlaps in the All Industry ranking.
- **Public sector investment.** An indicative estimate of the economic impact of a nominal public sector investment in the identified top single technology components.

25.1. Economic benefits of IoT for the United States

There is substantial uncertainty associated with estimates of the economic impact of IoT by industry by 2030. Edquist et al. (2019)[1702] suggest a value of $0.849 trillion. Mandel and Swanson (2017) suggest an additional 0.7% added to GDP growth equivalent to approximately $800bn over five years, although this study includes the impact of additional non IoT information. [1703] This compares with Manyika et al. (2015)[1704] estimated value of $USD 3.9 to 11.1 trillion worldwide which was updated in 2021 to between $5.5 and $12.6 trillion.[1705]

This study uses McKinsey values as they better map to the industry selections and are more detailed. Figure 25-1 below shows selected industry values from the 2021 study along with a

[1702] "The Internet of Things and Economic Growth in a Panel of Countries", Taylor & Francis Online, November 2019. Link

[1703] "The Coming Productivity Boom. Transforming the Physical Economy with Information", Mandel M., Swanson B.,2017. Link

[1704] "Unlocking the potential of the Internet of Things" , McKinsey Global Institute, June 2015. Link

[1705] "The Internet of Things: Catching Up to an Accelerating Opportunity.", McKinsey Alumni Center. Link

© Strategy of Things, 2025. All rights reserved.

mapping to the nine selected industries for this analysis. This provides a global estimate of $5,283bn for the selected industries which includes consumer surpluses.

	Low	High	Mean	1. Agriculture	2. Construction	3. Renewable energy	4. Insurance	5. Healthcare	6. Manufacturing	7. Retail	8. Smart Cities	9. Telecommunications	10. Transport
Manufacturing operations	460	1,290	875						100%				
Farm yield	250	520	385	100%									
Manufacturing: Predictive Ma	260	460	360						100%				
Health monitoring	240	1,200	720					100%					
Wellness	310	560	435					100%					
Construction operations	70	540	305		100%								
Oil and gas	80	300	190										
Construction maintenance	20	220	120		100%								
City traffic	100	390	245								100%		
Autonomous vehicles (City)	240	300	270								100%		
Congestion lanes	70	150	110								75%		25%
Retail self checkout	280	340	310							100%			
Promotions	60	190	125							100%			
Payments	140	180	160							100%			
Autonomous vehicles	140	250	195										100%
Defense	60	190	125										
Ship navigation	80	160	120										100%
Chore automation	290	580	435	0.2%	0.5%	2.0%	1.6%	1.3%	0.8%	1.0%		0.4%	0.4%
Energy management	130	230	180			100%							
Safety	20	20	20	0.2%	0.5%	2.0%	1.6%	1.3%	0.8%	1.0%		0.4%	0.4%
Insurance	130	140	135				100%						
Service improvements	90	140	115										100%
Shipping	40	70	55										100%
HR	110	260	185	0.2%	0.5%	2.0%	1.6%	1.3%	0.8%	1.0%		0.4%	0.4%
Augmented reality	30	100	65	0.2%	0.5%	2.0%	1.6%	1.3%	0.8%	1.0%		0.4%	0.4%
Activity monitoring	60	80	70	0.2%	0.5%	2.0%	1.6%	1.3%	0.8%	1.0%		0.4%	0.4%
Global value				386	429	195	148	1,165	1,241	603	598	3.3	515

Total	**5,283**

© Strategy of Things, 2025. All rights reserved.

Figure 25-1: IoT Value by Industry and Allocation ($US bn)[1706]

This global value needs to be adjusted to estimate the impact in the United States. Figure 25-2 below provides the sources that were used to adjust the global value in each industry by the US share. As a point of departure, the United States accounts for 24% of world GDP in 2022.[1707]

	U.S. global share	United States Market Share Source and Calculation
1.Agriculture	36%	Agriculture and food related industries contributed $USD 1.264 trillion.[1708] Global production is estimated at $USD S 3.5 trillion in 2021.[1709] This provides a U.S. share of 36%
2.Construction	25%	The global construction market is estimated at $6.4 trillion in 2020[1710] with a U.S. value of $1.589 trillion.[1711] This provides a U.S. share of 25%.
3.Renewable Energy	10%	The global renewable energy market is estimated at $1,977.6bn by 2030 based on a Compound Annual Growth Rate (CAGR) of 8.4%.[1712] This suggests a $US 882 bn market share in 2020 (1,977.6/1.084[10]) The U.S. market was estimated at $91.1bn in 2020.[1713] This provides a ratio of 10% (64/882).
4.Insurance	31%	The U.S. insurance industry generated premiums of $1.4 trillion in 2021 [1714] compared to 4.5 trillion globally.[1715] This provides a ratio of 31%.

[1706] Augmented reality, Activity monitoring and Safety percentages are allocated by percentage employment in the USA multiplied by U.S. share of world economy.

[1707] "US GDP as % of World GDP", YCharts, 2022. Link

[1708] "Ag and Food Sectors and the Economy", USDA, Economic Research Service. Link

[1709] "Statistical Yearbook", World Food and Agriculture, FAO UN, 2021. Link

[1710] "Size of the Global Construction Market From 2020 to 2021, with Forecasts from 2022 to 2030", Statistica. Link

[1711] "25 Essential U.S. Construction Industry Statistics: Data, Trends and More", Kolmar, C. June 2023. Link

[1712] "Renewable Energy Market to Garner $1,977.6 Bn, Globally, by 2030 at 8.4% CAGR": Allied Market Research, January 2022. Link

[1713] "Renewable Energy Market Size", Grand view research, 2021. Link

[1714] "20+ Interesting U.S. Insurance Industry Statistics [2023]: Insurance Facts, Margins and More", Zippia, J. Flynn, March 2023. Link

[1715] "Insurance", Statistica. Link

© Strategy of Things, 2025. All rights reserved.

	U.S. global share	United States Market Share Source and Calculation
5.Healthcare	48%	Worldwide healthcare expenditure is estimated at $9 trillion each year.[1716] USA expenditure is estimated at 4.3 trillion.[1717] This provides a 48% share for the United States.
6.Manufacturing	18%	The Brookings Institution estimates that the United States has a global market share of 18% in manufacturing.[1718]
7.Retail	19%	US retail expenditure is estimated at $5.57 trillion.[1719] This compares to worldwide expenditure of $29 trillion. A ratio of 19% is provided.[1720]
8. Cities	23%	The global smart city market is estimated at $1.22 trillion in 2022 with the U.S. contributing $280bn.[1721] This provides a ratio of 23%.
9.Telecoms	15%	Global market is estimated at $2.7 trillion[1722] with a U.S. share of $412 billion.[1723] This provides a ratio of 15%. Note that telecommunications is analyzed separately from the other industries and removed from the total.
10.Transportation	14%	In the U.S., the transportation and warehousing market size is estimated at $1.6 trillion[1724] in 2023. This compares to a global market of $11.1 trillion.[1725] This provides a ratio of 14%.

Figure 25-2: U.S. Global IoT Value Share Estimates

Figure 25-3 below applies these U.S. shares to the global value to produce a U.S. estimate of $ 1,419 bn of the value of IoT to 2030.

[1716] "Global Health Expenditure Database", WHO. Link

[1717] "NHE Fact Sheet", Historical NHE, CMS.gov, 2021. Link

[1718] "Global Manufacturing Scorecard: How the U.S. Compares to 18 Other Nations", West D. and Lansang C., July 10, 2018. Link

[1719] "U.S. Retail Sales Top $5,570 Billion", U.S. Census, January 2022. Link

[1720] "Total Retail Sales Worldwide (2023–2027)", Oberlo. Link

[1721] "Smart Cities Market Size, Share & Trends Analysis Report by Application, by Smart Governance, by Smart Utilities, by Smart Transportation, by Region and Segment Forecasts, 2023 – 2030", Grand View Research. Link

[1722] "Smart Cities Market Size, Share & Trends Analysis Report by Application, by Smart Governance, by Smart Utilities, by Smart Transportation, by Region and Segment Forecasts, 2023 – 2030", Skyquest, April 2023. Link

[1723] "United States (US) Telecom Operators Country Intelligence Report", GlobalData Report Store, September 2023. Link

[1724] "Transportation and Warehousing in the U.S. - Market Size 2005–2029", IBIS World, September 2023. Link

[1725] 2017 figure of 7.641 trillion inflated by a compound annual growth of 6.5% to provide a 2023 estimate. Link

© Strategy of Things, 2025. All rights reserved.

	1. Agriculture	2. Construction	3. Renewable energy	4. Insurance	5. Healthcare	6. Manufacturing	7. Retail	8. Smart Cities	9. Telecommunications	10. Transport
USA share of world	36%	25%	10%	31%	48%	18%	19%	23%	15%	14%
Value	139	106	20	46	557	223	116	137		74
% value	10%	8%	1%	3%	39%	16%	8%	10%		5%

Total	**1,419**

Figure 25-3: U.S. IoT Value Estimates by Selected Industry ($US bn)

25.2. Data integration by industry

The following sections provide details on the single technology assessments for each industry covering use case desk research, interviews and survey results. This information is then integrated using the methods detailed in Section 25.2.2. These results are then weighted by the industry economic contribution discussed above along with the role of the public sector to produce a ranked list for each industry. These weighted results are then summed to produce an economy wide ranked listing.

25.2.1. Classification presentation

Interviews and desk research for each industry provided additional information for the analysis. The analysis recorded each time a particular single technology component was highlighted as an issue and a judgment model was used to decide whether to include that issue in the analysis.

Figure 25-4 below shows example classification results from desk research. The selected single technology is included if it is mentioned in at least two of the use cases. In this example, the single technology component “H-4 1.Hardware: Edge Devices” would not be used to adjust the weighting. This ensures that only relevant technologies are used in the adjustment process.

© Strategy of Things, 2025. All rights reserved.

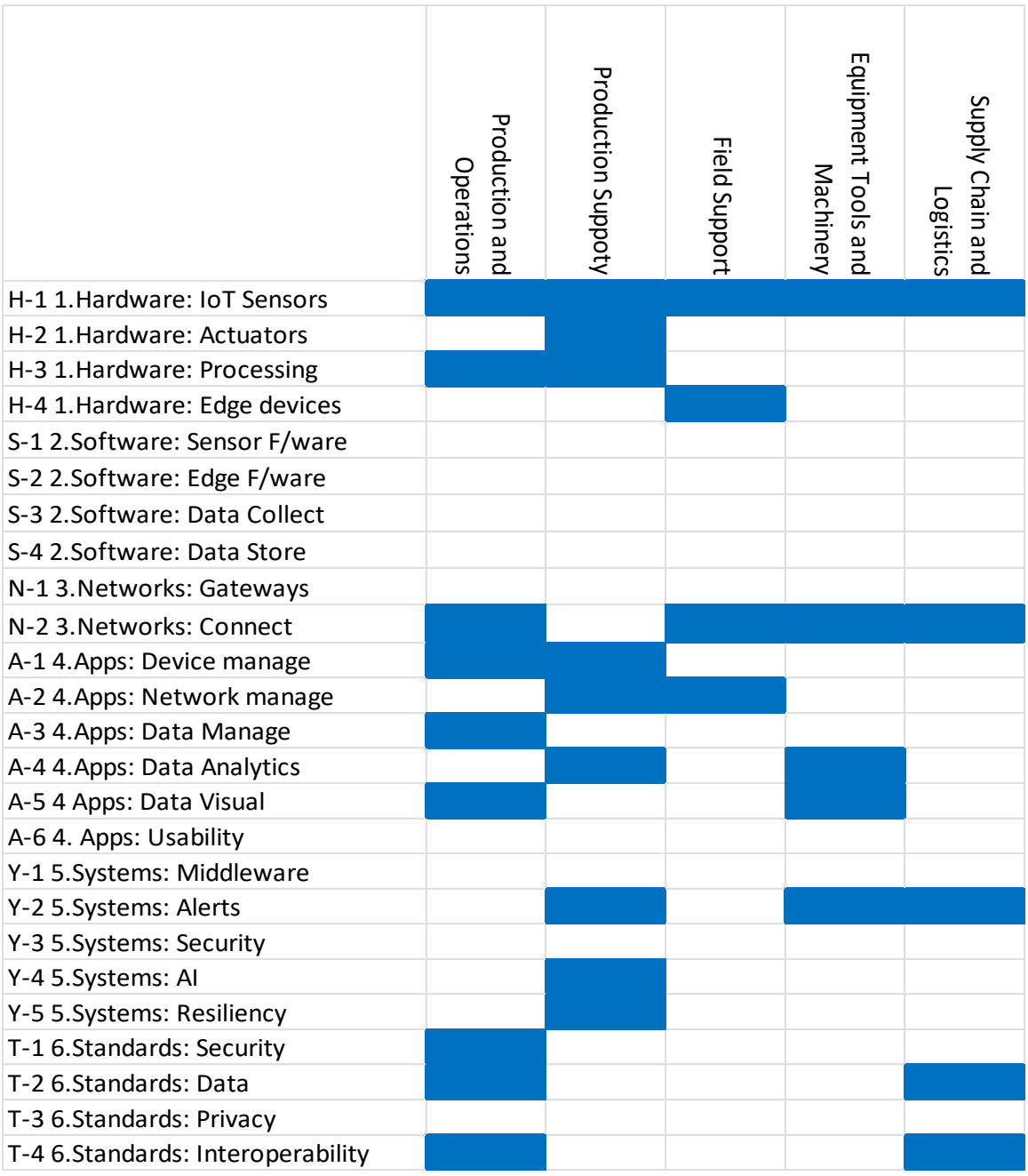


Figure 25-4: Single Technology Classification Example from Desk Research

Similarly, Figure 25-5 below provides an example result of the instances a particular single technology was highlighted in interviews with industry stakeholders. In this case the five indicated single technology components feed into the data integration.

© Strategy of Things, 2025. All rights reserved.

H-1 1.Hardware: IoT Sensors	
H-2 1.Hardware: Actuators	
H-3 1.Hardware: Processing	
H-4 1.Hardware: Edge devices	
S-1 2.Software: Sensor F/ware	
S-2 2.Software: Edge F/ware	
S-3 2.Software: Data Collect	
S-4 2.Software: Data Store	
N-1 3.Networks: Gateways	
N-2 3.Networks: Connect	
A-1 4.Apps: Device manage	
A-2 4.Apps: Network manage	
A-3 4.Apps: Data Manage	
A-4 4.Apps: Data Analytics	
A-5 4 Apps: Data Visual	
A-6 4. Apps: Usability	
Y-1 5.Systems: Middleware	
Y-2 5.Systems: Alerts	
Y-3 5.Systems: Security	
Y-4 5.Systems: AI	
Y-5 5.Systems: Resiliency	
T-1 6.Standards: Security	
T-2 6.Standards: Data	
T-3 6.Standards: Privacy	
T-4 6.Standards: Interoperability	

Figure 25-5: Single Technology Classification Example from Interviews

25.2.2. Data integration

The economic model uses data obtained through use cases, interviews, desk research and survey responses.

The survey was distributed over a three year period and some 450 responses were received. Solicitations to contribute to the survey were made through umbrella organizations, industry groups and leads from interviews and personal networks.[1726]

The model integrates the qualitative data with the quantitative data obtained from the surveys.

Given the uncertainty often associated with the IoT economic estimates, a simple explainable set of calculations is proposed to integrate these data. The data integration is performed by:

- Recording the percentage of survey respondents that indicated that a particular single technology is important.

[1726] The survey is available at https://www.surveymonkey.com/r/nist_general. Link

© Strategy of Things, 2025. All rights reserved.

- Reviewing interviews and desk research for both industry and use cases for comments that map to a single technology and recording if a particular technology maps well.
- Where there is more than one single technology mentioned in the interviews or desk research for use cases or industry the value is adjusted in the survey response by:
- New value = Old value * 1.25 + Average response [1727]
- Renormalize new values to 100%

Figure 25-7 overleaf shows an example of integrating these data to produce a normalized percentage for each of the single technologies.

- In this figure, columns 3 and 4 show whether a single technology was identified as an issue in the desk research for use cases and industry. The assessment was made and a "yes" = "1", "no" = blank recorded. Column 5 shows the same assessment made based on the stakeholder interviews. Column 6 totals the assessments made on each of these areas.
- Column 7 provides a tick if a particular single technology is mentioned in at least two of the areas of desk research use cases, desk research industry and interviews. Requiring the single technology to appear in at least 2 areas ensures that the most important single technologies are incorporated into the analysis.
- Column 8 provides the survey results for that industry. Here the value shows the percentage of respondents who chose a single technology component as important to operationalize a set of use cases.
- Column 9 applies the New Value formula mentioned above to incorporate the qualitative assessments.
- Finally, column 10 renormalizes the results to total 100%. Column 10 provides the relative weighting for each of the single technologies for that industry incorporating information from desk research on use cases and industries, interviews and surveys.

The normalized results in column 10 are then adjusted by economic importance and the role of the public sector to produce an individual industry analysis with a ratio ranked list of the top 10 single technologies as shown below in Figure 25-6 as an example.

[1727] Both an additive and multiplicative change is required. This adjusts both 0% responses (additive) and includes the scale of a non-zero response (multiplicative). This is the simplest method to incorporate qualitative research into the quantitative assessment and while arbitrary, provides an initial relative ranking of each of the singletechnologies.

The ratio between the additive (average) and multiplicative (1.25) constants does change rankings. to account for this a Monte Carlo analysis based on the range of IoT economic impact values and the ratio is shown in Figure 26-3.

© Strategy of Things, 2025. All rights reserved.

Rank	Technology	Weighting	Percentage
1	H-1 Hardware: IoT Sensors	0.00906	18%
2	T-4 Standards: Interoperability	0.00820	16%
3	H-4 Hardware: Edge devices	0.00549	11%
4	Y-4 Systems: AI	0.00481	9%
5	Y-3 Systems: Security	0.00481	9%
6	S-4 Software: Data store	0.00481	9%
7	H-2 Hardware: Actuators	0.00412	8%
8	Y-5 Systems: Resiliency	0.00343	7%
9	S-3 Software: Data collect	0.00343	7%
10	H-3 Hardware: Processing	0.00343	7%

Figure 25-6: Example Top 10 Single Technology Ranking

© Strategy of Things, 2025. All rights reserved.

Indicated in Desk Research or Interviews

If more than 1 mention include and adjust the survey value

For more than 1 mention, the average value is added to the scaled survey response:
1.25* 6.2% + 5.6% = 13.3% and then renormalized = 9.2%

		Desk (Use case)	Desk (Industry)	Interviews	Total	Include	Survey	Adjusted	Normalized
Hardware	IoT Sensors	1			1		11.1%	11.1%	7.7%
	Actuators	1			1		7.4%	7.4%	5.1%
	Processing		1		1		4.9%	4.9%	3.4%
	Edge Devices	1			1		6.2%	6.2%	4.3%
Software	Sensor Firmware						7.4%	7.4%	5.1%
	Edge Firmware/OS						6.2%	6.2%	4.3%
	Data Collection/Ingestior	1	1		2	✓	6.2%	13.3%	9.2%
	Data Storage	1	1		2	✓	3.7%	10.3%	7.1%
Networking	Gateways								0.0%
	Connectivity	1			1				0.0%
Applications	Device Management	1	1	1	3	✓		5.6%	3.9%
	Network Management								0.0%
	Data Management	1	1		2	✓		5.6%	3.9%
	Data Analytics	1	1		2	✓		5.6%	3.9%
	Data Visualization								0.0%
	User Interaction/Usabilit	1			1				0.0%
Systems	Middleware/Integration			1	1		2.5%	2.5%	1.7%
	Alerts and Notifications	1	1		2	✓	2.5%	8.7%	6.0%
	Security Management						8.6%	8.6%	6.0%
	Artificial Intelligence						3.7%	3.7%	2.6%
	System Resiliency		1		1		4.9%	4.9%	3.4%
Standards	Security			1	1		3.7%	3.7%	2.6%
	Data	1			1		3.7%	3.7%	2.6%
	Privacy	1			1		7.4%	7.4%	5.1%
	Interoperability		1	1	2	✓	9.9%	18.0%	12.4%
							100%	**145%**	**100%**
						Average value	5.6%		
Column		1	2	3	4	5	6	7	8	9	Normalized to total 100%

Figure 25-7: Data Integration Method

© Strategy of Things, 2025. All rights reserved.

25.2.3. Agriculture

The section covers:

- Industry desk research for use cases
- Other industry desk research
- Interviews
- Summary rankings.

25.2.3.1. Industry desk research for use cases

Figure 13-1 provides a set of representative use cases for agriculture and this section discusses the technical assessments for each use case group. Issues identified in the desk research were mapped to the taxonomy in Figure 11-4 using the table structure described in Figure 25-5.

Figure 25-8 below shows the single technology component classifications of each of the use cases from desk research.

© Strategy of Things, 2025. All rights reserved.

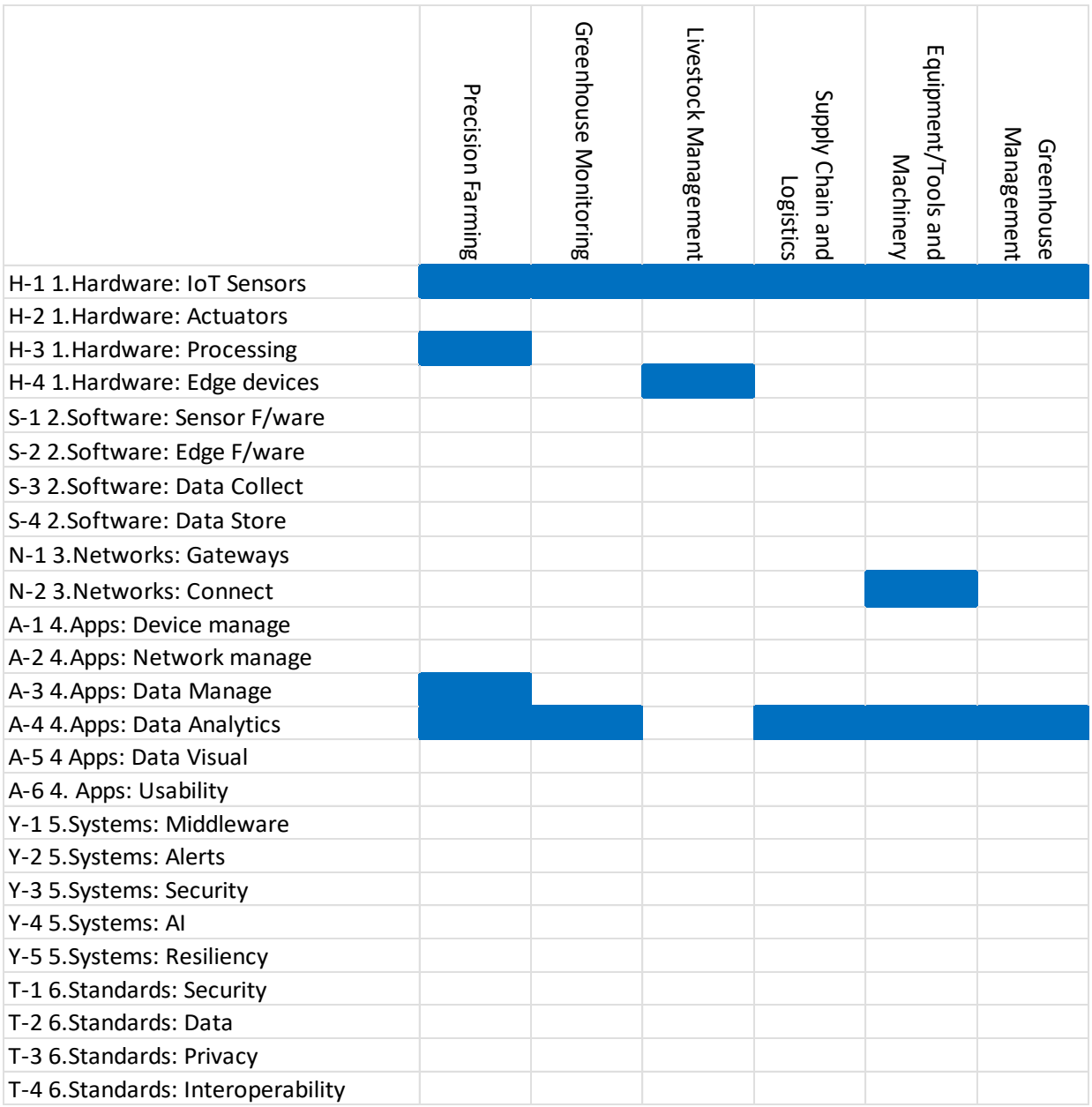


Figure 25-8: Agriculture: Use Cases: Single Technology Classifications

25.2.3.2. Other industry desk research

In addition to the above use cases, desk research identified an additional five single technology components that could delay the use and benefits of IoT services in agriculture. These are listed in detail below in Figure 25-10.

© Strategy of Things, 2025. All rights reserved.

ID	Single technology	Comment
1	N-1 - 3.Networks: Gateways	Disrupted cloud connectivity.[1728]
2	N-2 - 3.Networks: Connect	Poor or lack of internet connectivity in rural America.[1729]
3	A-3 - 4.Apps: Data Manage	Data sharing – governance, transparency, access.[1730]
4	Y-3 - 5.Systems: Security	Data security.[1731]
5	T-4 - 6.Standards: Interoperability	Interoperability of different standards.[1732]

Figure 25-9: Agriculture: Other Desk Research: Single Technology Classifications

Figure 25-10 below summarizes these results.

[1728] "Three Major Obstacles for IoT s in Agriculture", CGIAR, Platform for Big Data in Agriculture. Link

[1729] "Three Major Obstacles for IoT s in Agriculture", CGIAR, Platform for Big Data in Agriculture. Link

[1730] "IoT Challenges Associated With the Agriculture Industry", TechTarget, IoT Agenda, K. Popova, October 2018. Link

[1731] "IoT Challenges Associated With the Agriculture Industry", TechTarget, IoT Agenda, K. Popova, October 2018. Link

[1732] "America's Farmers Are Becoming Prisoners to Agriculture's Technological Revolution", Vice, Motherboard, R. Wanstreet, March 2018. Link

© Strategy of Things, 2025. All rights reserved.

H-1 1.Hardware: IoT Sensors	
H-2 1.Hardware: Actuators	
H-3 1.Hardware: Processing	
H-4 1.Hardware: Edge devices	
S-1 2.Software: Sensor F/ware	
S-2 2.Software: Edge F/ware	
S-3 2.Software: Data Collect	
S-4 2.Software: Data Store	
N-1 3.Networks: Gateways	
N-2 3.Networks: Connect	
A-1 4.Apps: Device manage	
A-2 4.Apps: Network manage	
A-3 4.Apps: Data Manage	
A-4 4.Apps: Data Analytics	
A-5 4 Apps: Data Visual	
A-6 4. Apps: Usability	
Y-1 5.Systems: Middleware	
Y-2 5.Systems: Alerts	
Y-3 5.Systems: Security	
Y-4 5.Systems: AI	
Y-5 5.Systems: Resiliency	
T-1 6.Standards: Security	
T-2 6.Standards: Data	
T-3 6.Standards: Privacy	
T-4 6.Standards: Interoperability	

Figure 25-10: Agriculture: Other Desk Research: Single Technology Classifications

25.2.3.3. Interviews

Interviews were conducted with six organizations to gather IoT adoption trends and issues. Figure 25-11 below lists the interviewees.

ID	Company Name	Type of Company
1	Sigfox	IoT Connectivity Provider
2	FarmX	IoT Sensor and Solution Provider
3	Fybr	IoT Solution Provider
4	Aker Technologies	IoT Sensor and Data Provider

© Strategy of Things, 2025. All rights reserved.

ID	Company Name	Type of Company
5	Agrov.fr	Indoor Farming Solution Provider
6	BLX.io	IoT Sensor and Solution Provider

Figure 25-11: Agriculture: Stakeholder Interviews

In addition, roundtable discussions were undertaken with the groups shown in Figure 25-12 below to gather input on IoT adoption and barriers in Agriculture:

ID	Group Name	Type of Group
1	The American Equipment Manufacturers	Manufacturing Association
2	Wisconsin IoT Council	IoT Association

Figure 25-12: Agriculture: Round Table Discussions

The interviews identified eleven areas that could delay the use and benefits of IoT services. Close to verbatim excerpts from the interviews along with a technical allocation for each set of comments are shown below in Figure 25-14.

ID	Single technology	Verbatim interviewee comment
1	H-1 - 1.Hardware: IoT Sensors	Devices themselves, components, are astounding how many options there are for sensors and microcontrollers. A lot of good options.
2	H-2 1.Hardware: Actuators	National Science Foundation collaboration on robotics, AI, pilots for broadband studies, last two years, national robotics have had so many agriculture grant applications.
3	H-4 - 1.Hardware: Edge devices	Edge computing - mitigates lack of connectivity or affordable connectivity by having real time response without going to the cloud.

© Strategy of Things, 2025. All rights reserved.

ID	Single technology	Verbatim interviewee comment
4	N-2 - 3.Networks: Connect	We do not have a map that tells us where there is and isn't broadband availability on farm fields. There is no government map that does…. it's a huge hole when they talk about broadband in rural areas.
5	A-1 - 4.Apps: Device manage	Maintainability and service/repair of equipment - developers need to think about how farmers will repair and service this equipment.
6	A-2 - 4.Apps: Network manage	Farmers are not early adopters..like to tinker and experiment... Like to repair and understand how equipment works.
7	A-4 - 4.Apps: Data Analytics	Getting information in the right format from IoT for farmers to take action.
8	A-6 - 4. Apps: Usability	Farm level imaging, soil conditions, etc. but getting the info to the right format to the farmer to take action was the main challenge.
9	Y-2 - 5.Systems: Alerts	Greenhouse Monitoring - For farmers investing a bit more…greenhouse growing for high value crops.
10	Y-4 5.Systems: AI	Maintainability and service/repair of equipment - developers need to think about how farmers will repair and service this equipment.
11	T-4 - 6.Standards: Interoperability	Talked to a bunch of extensions and universities. Farm level imaging, soil conditions, etc. but getting the info to the right format to the farmer to take action was the main challenge. didn't get a good sense of the integration of the info stream.

© Strategy of Things, 2025. All rights reserved.

Figure 25-13: Agriculture: Stakeholder Interviews: Single Technology Classifications

Figure 25-14 below summarizes these IoT single technology classifications.

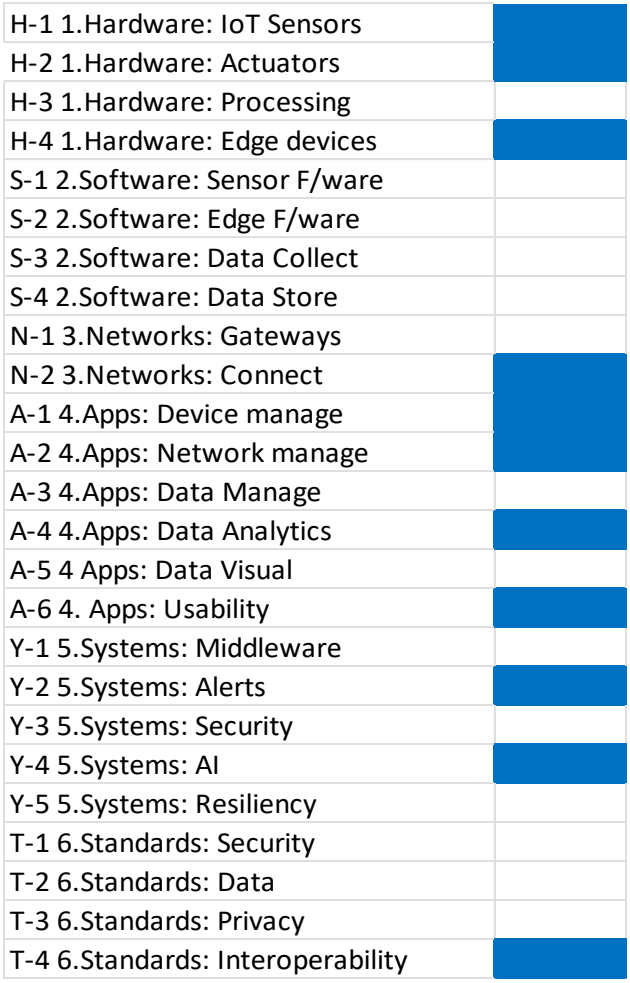


Figure 25-14: Agriculture: Stakeholder Interviews: Single Technology Classifications

25.2.3.4. Ranking technology infrastructure gaps

Figure 25-15 overleaf shows the integration of use cases, survey, interview and desk research to produce a ranking of the single technologies required to operationalize the most important use cases.

© Strategy of Things, 2025. All rights reserved.

			Desk (Use case)	Desk (Industry)	Interviews	Total	Include	Survey	Adjusted	Normalized
H-1	**Hardware**	IoT Sensors	1		1	2	✓	9.1%	17.1%	13.5%
H-2		Actuators			1	1		7.8%	7.8%	6.1%
H-3		Processing						6.5%	6.5%	5.1%
H-4		Edge Devices			1	1		10.4%	10.4%	8.2%
S-1	**Software**	Sensor Firmware						2.6%	2.6%	2.0%
S-2		Edge Firmware/OS						1.3%	1.3%	1.0%
S-3		Data Collection/Ingestion						6.5%	6.5%	5.1%
S-4		Data Storage						9.1%	9.1%	7.1%
N-1	**Networking**	Gateways		1		1				0.0%
N-2		Connectivity		1	1	2	✓		5.8%	4.5%
A-1	**Applications**	Device Management			1	1				0.0%
A-2		Network Management			1	1				0.0%
A-3		Data Management		1		1				0.0%
A-4		Data Analytics	1		1	2	✓		5.8%	4.5%
A-5		Data Visualization								0.0%
A-6		User Interaction/Usability			1	1				0.0%
Y-1	**Systems**	Middleware/Integration						1.3%	1.3%	1.0%
Y-2		Alerts and Notifications			1	1		2.6%	2.6%	2.0%
Y-3		Security Management		1		1		9.1%	9.1%	7.1%
Y-4		Artificial Intelligence			1	1		9.1%	9.1%	7.1%
Y-5		System Resiliency						6.5%	6.5%	5.1%
T-1	**Standards**	Security						2.6%	2.6%	2.0%
T-2		Data						3.9%	3.9%	3.1%
T-3		Privacy						3.9%	3.9%	3.1%
T-4		Interoperability		1	1	2	✓	7.8%	15.5%	12.2%
								100%	**127%**	**100%**

Figure 25-15: Agriculture: Interview, Desk Research and Survey Technical Results

© Strategy of Things, 2025. All rights reserved.

Figure 25-16 below shows the survey results of the role of the private and public sectors in undertaking research and development to operationalize the use cases.

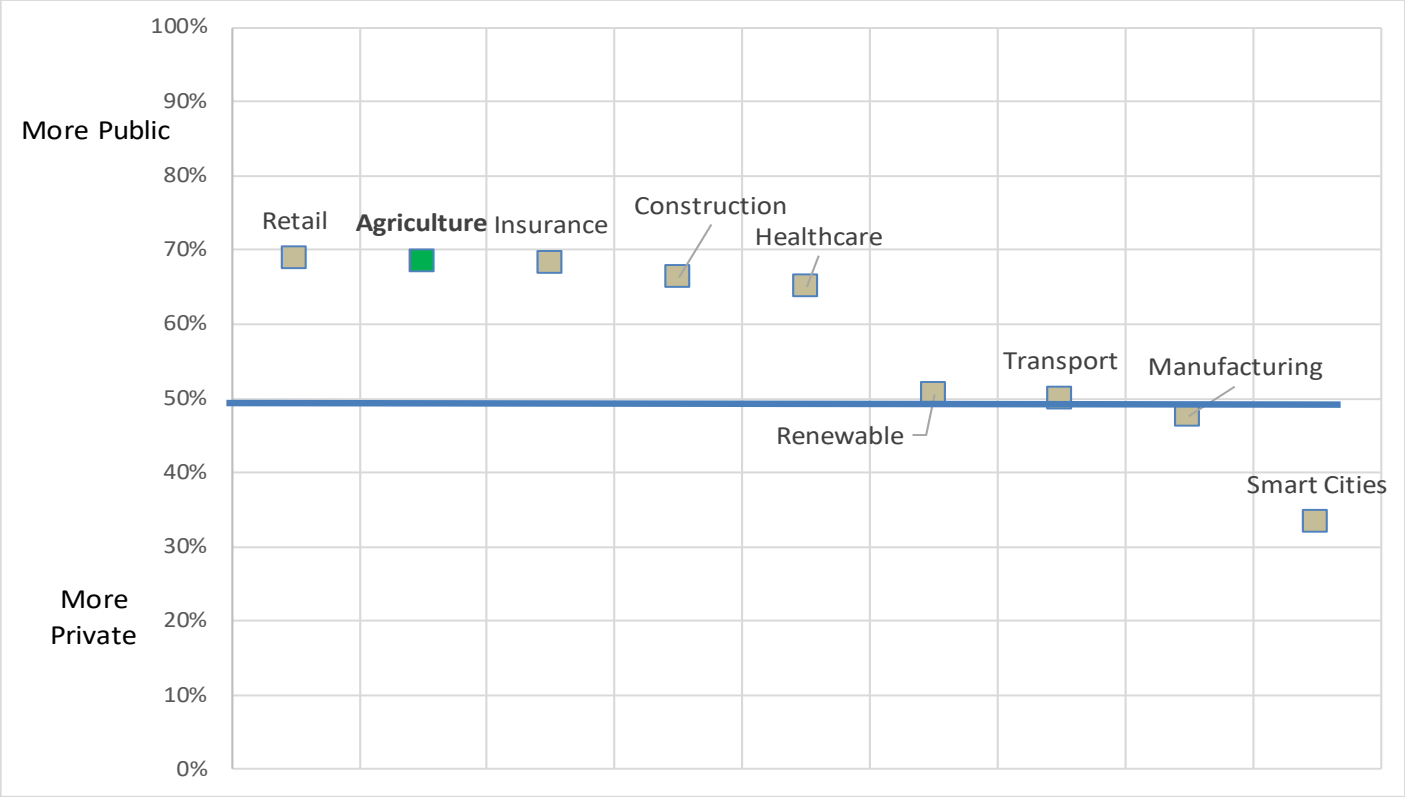


Figure 25-16: Agriculture: Role of the Public Sector in R&D

Figure 25-17 below shows the relative weightings for agriculture of the top 10 single technologies. This figure is based on an IoT value share of 10%[1733] for agriculture and a public contribution of 68% multiplied by the adjusted weighting shown in Figure 25-15.

Rank	Technology	Weighting	Percentage
1	H-1 Hardware: IoT Sensors	0.00906	18%
2	T-4 Standards: Interoperability	0.00820	16%
3	H-4 Hardware: Edge devices	0.00549	11%
4	Y-4 Systems: AI	0.00481	9%
5	Y-3 Systems: Security	0.00481	9%
6	S-4 Software: Data store	0.00481	9%
7	H-2 Hardware: Actuators	0.00412	8%
8	Y-5 Systems: Resiliency	0.00343	7%
9	S-3 Software: Data collect	0.00343	7%
10	H-3 Hardware: Processing	0.00343	7%

[1733] See Figure 25-3.

© Strategy of Things, 2025. All rights reserved.

Figure 25-17: Agriculture: Ranking and Single Technology Weightings

25.2.4. Manufacturing

The section covers:

- Industry desk research for use cases
- Other industry desk research
- Interviews
- Summary rankings

25.2.4.1. Industry desk research for use cases

Figure 14-1 provided a set of representative use cases for manufacturing and this section discusses the technical assessments for each use case group. Issues identified in the desk research were mapped to the taxonomy in Figure 11-4 using the table structure described in Figure 25-5.

Figure 25-18 below shows the single technology component classifications of each of the use cases from desk research.

© Strategy of Things, 2025. All rights reserved.

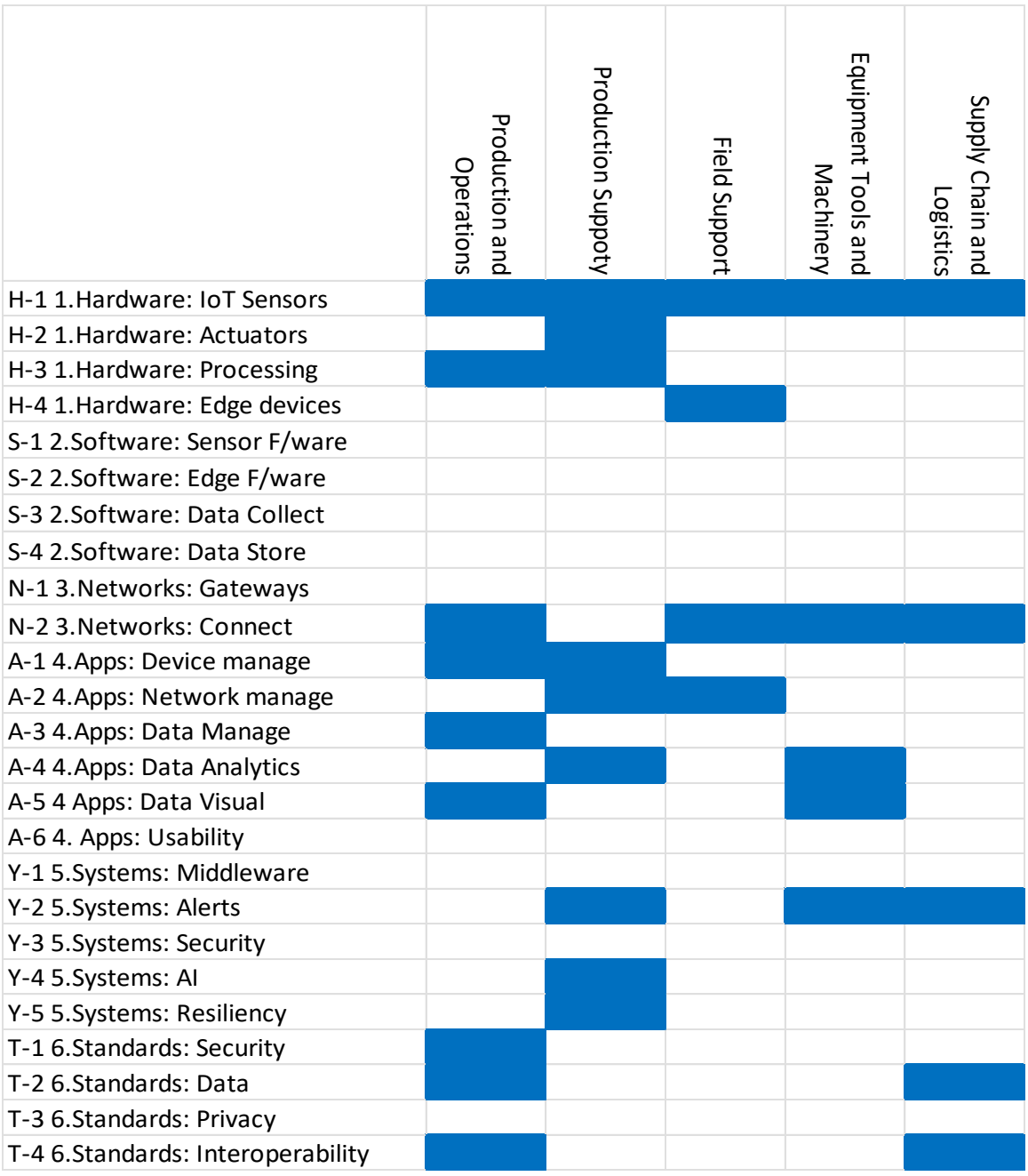


Figure 25-18: Manufacturing: Desk Research: Use Case Single Technology Classifications

25.2.4.2. Other industry desk research

In addition to the above use cases, desk research identified eleven additional single technology component issues that could delay the use and benefits of IoT services. These are discussed below in Figure 25-19.

© Strategy of Things, 2025. All rights reserved.

ID	Single technology	Comment
1	H-1 1.Hardware: IoT Sensors	Enabling real-time insights, process improvements, predictive maintenance, etc.
2	H-2 1.Hardware: Actuators	Play a role in process automation
3	H-4 1.Hardware: Edge devices	Decentralize processes by restricting analysis and business decisions to the appropriate physical location
4	N-2 3.Networks: Connect	Driven by Industry 4.0
5	A-1 4.Apps: Device manage	Risk from increased cyber-attack surface areas and limited cybersecurity workforces
6	A-2 4.Apps: Network manage	The longer a manufacturing facility has been in operation, the more likely it is to have legacy systems that may not integrate with IoT technology.
7	A-4 4.Apps: Data Analytics	Comprehensive data allows managers to identify and optimize based on large-scale trends. This system-wide optimization is operationalized by access to this previously inaccessible data.[1734]
8	A-6 4. Apps: Usability	Ensure compatibility and ease of use for complex devices
9	Y-2 5.Systems: Alerts	Maintain safety in complex and often dangerous environments
10	Y-4 5.Systems: AI	Opportunity to transform manufacturing

[1734] "4 Examples of How the IoT is Transforming the Electronics Supply Chain", IoT Times, June 2018. Link

© Strategy of Things, 2025. All rights reserved.

ID	Single technology	Comment
11	T-4 6.Standards: Interoperability	The lack of standards in IoT, most notably for hardware, remains a challenge for implementation. Tools and best practices for software development such as unit testing are still largely absent from IoT hardware design.

Figure 25-19: Manufacturing: Other Industry Desk Research: Single Technology Classifications

Figure 25-20 below summarizes these technologies.

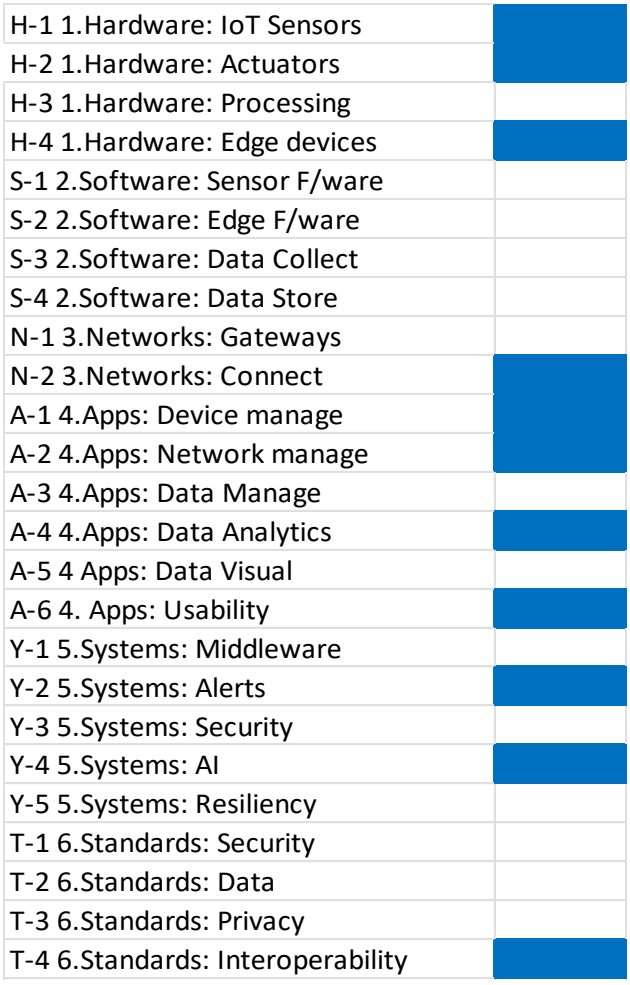


Figure 25-20: Manufacturing: Other Desk Research: Single Technology Classifications

25.2.4.3. Interviews

Interviews were conducted with four organizations to gather IoT adoption trends and issues. Figure 25-21 below lists the organizations.

© Strategy of Things, 2025. All rights reserved.

	Company Name	Type of Company
1	IIOT World	IoT Solution Provider
2	PICMG	Consortium for IoT Standards
3	Senior Growth Advisor	IoT Solution Provider
4	VP of IoT and analytics	Software Development

Figure 25-21: Manufacturing: Stakeholder Interviews

The interviews identified fifteen areas that could delay the use and benefits of IoT services. Close to verbatim excerpts from the interviews in Figure 25-22 along with a technical allocation for each set of comments.

ID	Single technology	Interviewee comment
1	H-1: IoT Sensors H-4 1.Hardware: Edge devices	Example of making decisions on emotion are when they trust the operator Operators editing machine will be based on data not emotion. Example of making decisions on emotion are when they trust the operator and gut feeling and rely on that over sensors…they are still checking the machines Exponential growth on pervasive sensing analytics
2	S-2: Edge Firmware/OS	…with IoT, need to multiply the sensors but move the intel to the sensors Operator side of things... they need training... they don't understand that they have a problem that PICMG has a solution for. This is because…they are used to running a factory with SCADA system... you want to move to iot... need to deploy 10 to 100 more sensor points than scada... in order to realize the value fully... to scale up scada system, that can be... with iot, need to multiply the sensors but move the intel to the sensors Software-what is the cause behind the changes shown on a sensor…edge devices have logic built in to show the cause of the specific problem… more results than just data…formula is part of the hardware such as the edge device

© Strategy of Things, 2025. All rights reserved.

ID	Single technology	Interviewee comment
3	N-2: Connectivity	Lack of wireless connectivity in industrial settings Remote asset management for field services (for OEM and equipment builders)
4	A-1: Device Management	Management such as firmware updates, configuration changes down to assets and devices
5	A-2: Network Management	Networking- needs to be able to handle a lot more sensors... Data collection timing intervals need to be improved…need for gateways to have different sources of data protocols. Wireless heart.4G,5G, LTE, LoRAWAN, BLE
6	A-3: Visualization	May need to do some programming to get that data out.
7	A-4: Data Analytics	Applications- Analytics is the most important in the next 5-10 years, needs to be a clean process with data validation Field Devices- low cost, low power, advanced analytic software
8	A-6: User Interaction/Usability	Exponential growth on remote monitoring and control – COVID has made remote monitoring a norm…. Controls remotely will be really popular. At the moment the control is not there for remote monitoring…control for making changes is still done on site, sensors were wired…probably >5% controllers are remote...
9	Y-1 5.Systems: Middleware	Technology is not just s/w, but it is the combination of h/w and s/w
10	Y-2: Alerts and Notifications	Manufacturing -this area is growing a bit… Mostly production line management (is the asset running?) connecting the unconnected to provide data to improve their business processes...
11	Y-3 5.Systems: Security	Cybersecurity concerns lacking memory safety since languages like C++ is outdated

© Strategy of Things, 2025. All rights reserved.

ID	Single technology	Interviewee comment
12	Y-4: Artificial Intelligence	As AI becomes important, we must develop entirely new intellectual property guidelines Systems- for AI and ML they have an AI system implementation…. OpticsAnalytics using AI and ML to make informed decisions
13	T-2: Data	standardization was one of the problems operators were facing with IoT rollouts" Morgan Stanley did a report – standardization was one of the problems operators were facing with IoT rollouts Smaller companies don't have the wherewithal and are loathe to share data. There needs to be some kind of rules or agreement otherwise there is no cooperation Evolution of Sensor Network protocol- the current do not address the pervasive sensing
14	T-3: Privacy	Small manufacturers don't like to share For AI and IoT to work. Need sharing of data Privacy is very important in healthcare because it affects each one of us IoT will be pervasive so need to talk to large companies as well as small ones.
15	T-4: Interoperability	Sensor domain is struggling to get a broad variety of sensors to be plug and play PICMG sees at sensor level there is no interoperability at the sensor and the edge levels Sensor domain is where PICMG is playing in this broader ecosystem Sensor domain is struggling to get a broad variety of sensors to be plug and play "Govt is leading but not in the US... example - European Space agency... they want to have some level of interoperability" Problem - PICMG sees at sensor level there is no interoperability at the sensor and the edge level

Figure 25-22: Manufacturing: Stakeholder Interviews: Qualitative Single Technologies

Figure 25-23 below tabulates the single technologies identified in the interviews.

© Strategy of Things, 2025. All rights reserved.

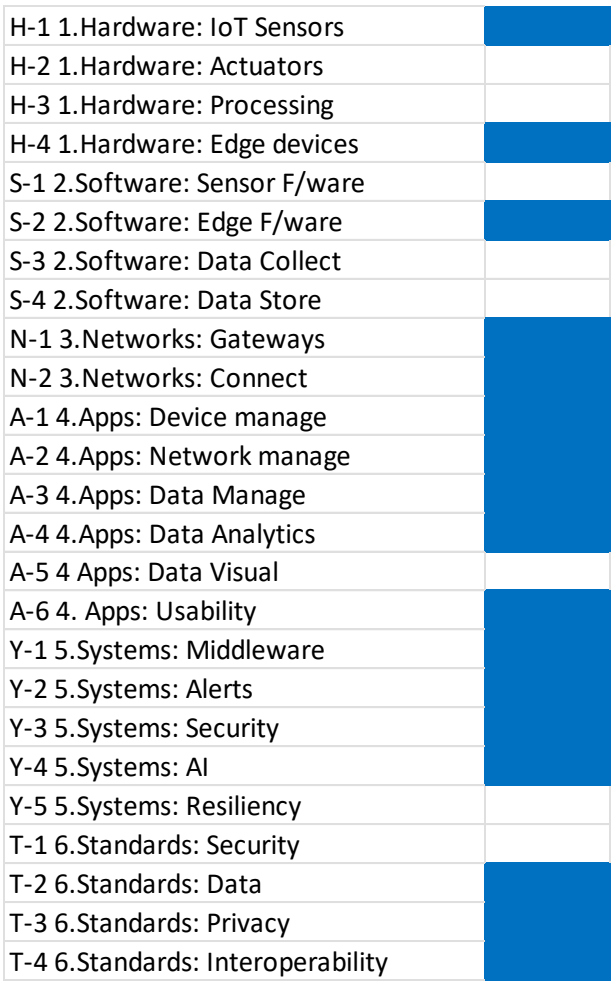


Figure 25-23: Manufacturing: Stakeholder Interviews: Qualitative Single Technologies Classifications

25.2.4.4. Ranked technology infrastructure gaps

Figure 25-24 overleaf shows the integration of use cases, survey, interview and desk research to produce a ranking of the single technologies required to operationalize the most important use cases.

© Strategy of Things, 2025. All rights reserved.

			Desk (Use case)	Desk (Industry)	Interviews	Total	Include	Survey	Adjusted	Normalized
H-1	**Hardware**	IoT Sensors	1		1	2	✓	14.4%	23.9%	13.3%
H-2		Actuators						4.8%	4.8%	2.7%
H-3		Processing	1			1		5.8%	5.8%	3.2%
H-4		Edge Devices	1			1		4.8%	4.8%	2.7%
S-1	**Software**	Sensor Firmware	1			1		4.8%	4.8%	2.7%
S-2		Edge Firmware/OS			1	1		2.9%	2.9%	1.6%
S-3		Data Collection/Ingestion						6.7%	6.7%	3.8%
S-4		Data Storage						4.8%	4.8%	2.7%
N-1	**Networking**	Gateways	1			1				0.0%
N-2		Connectivity	1		1	2	✓		5.8%	3.3%
A-1	**Applications**	Device Management	1		1	2	✓		5.8%	3.3%
A-2		Network Management	1	1	1	3	✓		5.8%	3.3%
A-3		Data Management	1	1	1	3	✓		5.8%	3.3%
A-4		Data Analytics	1	1	1	3	✓		5.8%	3.3%
A-5		Data Visualization	1			1				0.0%
A-6		User Interaction/Usability		1	1	2	✓		5.8%	3.3%
Y-1	**Systems**	Middleware/Integration	1			1		5.8%	5.8%	3.2%
Y-2		Alerts and Notifications	1	1	1	3	✓	1.9%	8.2%	4.6%
Y-3		Security Management	1			1		9.6%	9.6%	5.4%
Y-4		Artificial Intelligence	1	1	1	3	✓	6.7%	14.2%	7.9%
Y-5		System Resiliency	1			1		4.8%	4.8%	2.7%
T-1	**Standards**	Security	1			1		7.7%	7.7%	4.3%
T-2		Data	1	1	1	3	✓	4.8%	11.8%	6.6%
T-3		Privacy	1	1	1	3	✓	2.9%	9.4%	5.3%
T-4		Interoperability	1	1	1	3	✓	6.7%	14.2%	7.9%
								100%	**179%**	**100%**
							Average value	5.8%		

Figure 25-24: Manufacturing: Use Case, Interview, Desk Research, Survey Technical Results

© Strategy of Things, 2025. All rights reserved.

Figure 25-25 below shows the survey results of the role of the private and public sectors in undertaking research and development to operationalize the use cases

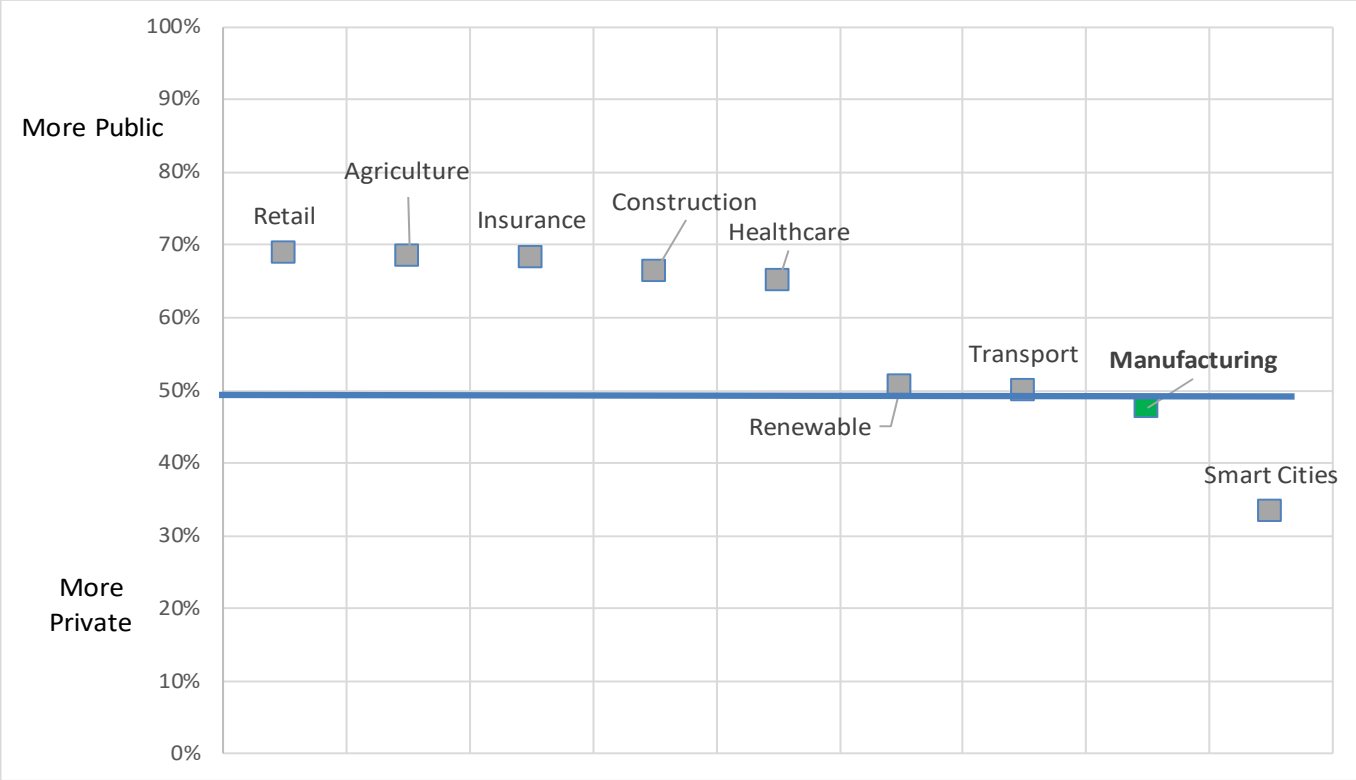


Figure 25-25: Manufacturing: Role of the Public Sector in R&D

Figure 25-26 below shows the relative weightings for manufacturing of the top 10 single technologies. This figure is based on an IoT value share of 16%[1735] for manufacturing and a public sector contribution of 48% multiplied by the normalized weighting shown in Figure 25-24.

[1735] See Figure 25-3.

© Strategy of Things, 2025. All rights reserved.

Rank	Technology	Weighting	Percentage
1	H-1 Hardware: IoT Sensors	0.00995	21%
2	T-4 Standards: Interoperability	0.00594	13%
3	Y-4 Systems: AI	0.00594	13%
4	T-2 Standards: Data	0.00494	11%
5	Y-3 Systems: Security	0.00401	9%
6	T-3 Standards: Privacy	0.00394	8%
7	Y-2 Systems: Alerts	0.00343	7%
8	T-1 Standards: Security	0.00321	7%
9	S-3 Software: Data collect	0.00281	6%
10	A-6 Apps: Usability	0.00243	5%

Figure 25-26: Manufacturing: Ranking and Single Technology Weightings

25.2.5. Construction

The section covers:

- Industry desk research for use cases
- Other industry desk research
- Interviews
- Summary rankings

25.2.5.1. Industry desk research for use cases

Figure 15-3 provided a set of representative use cases for construction and this section discusses the technical assessments for each use case group. Issues identified in the desk research were mapped to the taxonomy in Figure 11-4 using the table structure described in Figure 25-5.

Figure 25-27 below shows the single technology component classifications of each of the use cases from desk research.

© Strategy of Things, 2025. All rights reserved.

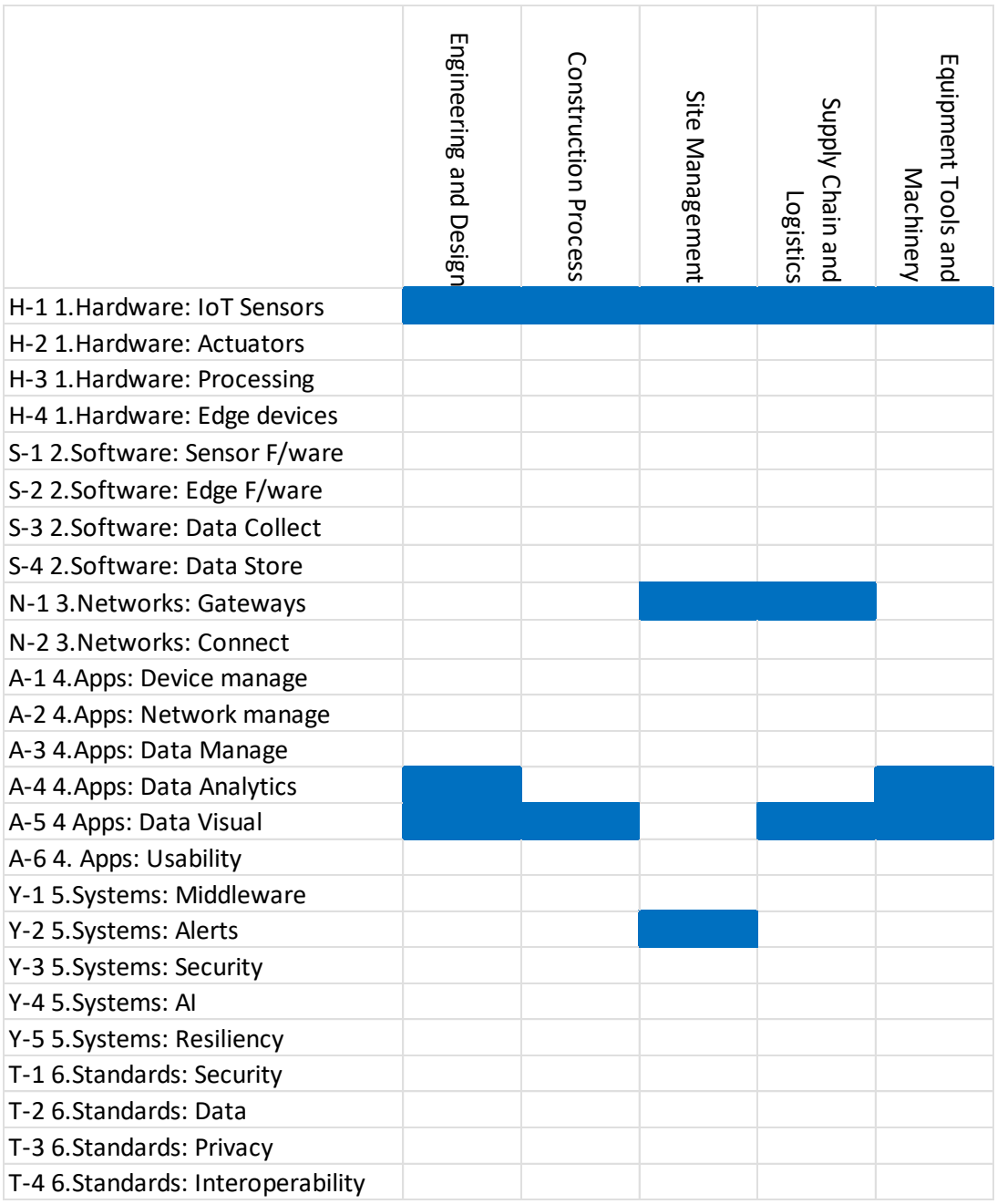


Figure 25-27: Construction Use Case: Single Technology Classifications

25.2.5.2. Other industry desk research

In addition to the above use cases, desk research identified five other single technology component issues that could delay the use and benefits of IoT services. These are discussed in detail below in Figure 25-28.

© Strategy of Things, 2025. All rights reserved.

	Single technology	Description
1	H-1 Hardware: IoT Sensors	Devices require updates and become vulnerable to attack as information on security issues becomes widely known.
2	Y-4 Systems: AI	The scale of data produced will require the use of AI tools and automation. IoT admins and network experts will have to set new rules so that unusual traffic patterns can be detected.
	Y-4 Systems: AI	Modern cloud services make use of threat intelligence for predicting security issues. Other such techniques include AI-powered monitoring and analytics tools.
3	T-1 Standards: Security	Many IoT companies sell devices that provide consumers with default credentials. Brute-force attacks can compromise the devices.
4	T-1 Standards: Security	The rapid rise in the development of IoT products will make cyber-attack permutations unpredictable.
5	T-1 Standards: Security	Data transmitted over the public internet can lead to data leaks. Not all the devices through which data are being transmitted or received are secure. Once the data are available hackers can sell it compromising data privacy and security

Figure 25-28: Construction: Other Desk Research: Single Technology Classifications

Figure 25-29 below summarizes these results.

© Strategy of Things, 2025. All rights reserved.

H-1 1.Hardware: IoT Sensors	
H-2 1.Hardware: Actuators	
H-3 1.Hardware: Processing	
H-4 1.Hardware: Edge devices	
S-1 2.Software: Sensor F/ware	
S-2 2.Software: Edge F/ware	
S-3 2.Software: Data Collect	
S-4 2.Software: Data Store	
N-1 3.Networks: Gateways	
N-2 3.Networks: Connect	
A-1 4.Apps: Device manage	
A-2 4.Apps: Network manage	
A-3 4.Apps: Data Manage	
A-4 4.Apps: Data Analytics	
A-5 4 Apps: Data Visual	
A-6 4. Apps: Usability	
Y-1 5.Systems: Middleware	
Y-2 5.Systems: Alerts	
Y-3 5.Systems: Security	
Y-4 5.Systems: AI	
Y-5 5.Systems: Resiliency	
T-1 6.Standards: Security	
T-2 6.Standards: Data	
T-3 6.Standards: Privacy	
T-4 6.Standards: Interoperability	

Figure 25-29: Construction: Other Desk Research: Single Technology Classifications

25.2.5.3. Interviews

Interviews were conducted with four organizations to gather IoT adoption trends and issues. Figure 25-30 below lists the interviewees.

© Strategy of Things, 2025. All rights reserved.

	Company Name	Type of Company
1	Association of Equipment Manufacturers (AEM)	Trade association
2	Strategic Building Innovation	Consulting group
3	AIOTA	Consulting group
4	Dodge Data & Analytics	Consulting group

Figure 25-30: Construction: Stakeholder Interviews

The interviews identified six areas that could delay the use and benefits of IoT services. Close to verbatim excerpts from the interviews in Figure 25-32 along with a technical allocation for each set of comments.

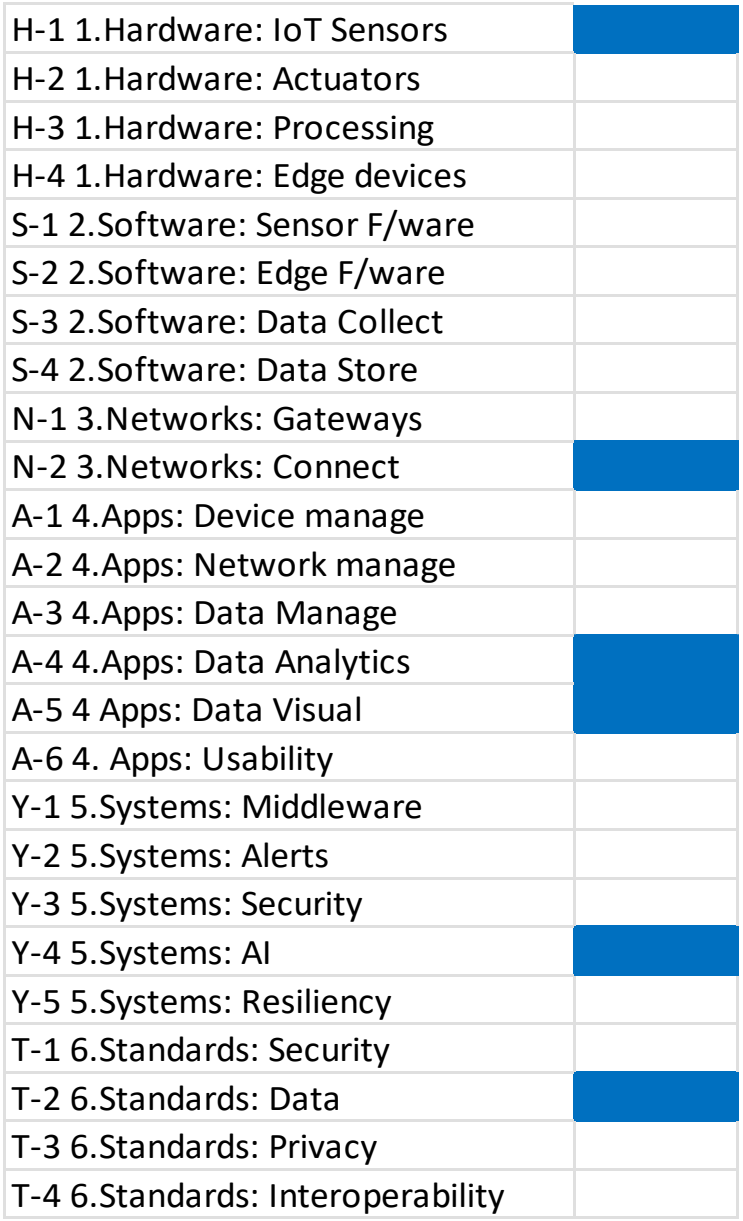
ID	Single technology	Interviewee comment
1	H-1 1.Hardware: IoT Sensors	“Construction can be so "heavy" in terms of innovation meaning that we are barely getting things sensorized, there are some pilots sponsored and marketed but industry is just starting to realize the full capacity of IoT.”
2	N-2 3.Networks: Connect	“Moving towards autonomy, data usage and connection density is an issue…. 5G sounds great but there are still areas without coverage causing a big challenge.”
3	A-4 4.Apps: Data Analytics	“Earth Brain, spinoff of Komatsu in Japan does analytics on their equipment, as well as the the equipment moves.”
4	A-5 4 Apps: Data Visual	“Industry has problems on projects all day long and they just need fewer problems on their projects. Anything that is tangible value in solving those problems, people will buy.”
5	Y-4 5.Systems: AI	“Versatile AI – hang sensors from tower cranes to capture all the activity on site and they're able to do large scale benchmarking.”

© Strategy of Things, 2025. All rights reserved.

ID	Single technology	Interviewee comment
6	T-2 6.Standards: Data	"One of the reasons IoT doesn't have as much "big lever" value is that there is no common data set, elements and processes like with BIM".

Figure 25-31: Construction: Stakeholder Interviews: Single Technology Classifications

Figure 25-32 below summarizes these results.



© Strategy of Things, 2025. All rights reserved.

Figure 25-32: Construction: Stakeholder Interviews: Single Technology Classifications

25.2.5.4. Ranking technology infrastructure gaps

Figure 25-33 overleaf shows the integration of use cases, survey, interview and desk research to produce a ranking of the single technologies required to operationalize the most important use cases.

© Strategy of Things, 2025. All rights reserved.

			Desk (Use case)	Desk (Industry)	Interviews	Total	Include	Survey	Adjusted	Normalized
H-1	**Hardware**	IoT Sensors	1	1	1	3	✓	9.9%	17.9%	14.3%
H-2		Actuators						6.9%	6.9%	5.5%
H-3		Processing						7.9%	7.9%	6.3%
H-4		Edge Devices						8.9%	8.9%	7.1%
S-1	**Software**	Sensor Firmware						4.0%	4.0%	3.2%
S-2		Edge Firmware/OS						4.0%	4.0%	3.2%
S-3		Data Collection/Ingestion						10.9%	10.9%	8.7%
S-4		Data Storage						5.9%	5.9%	4.7%
N-1	**Networking**	Gateways	1			1				0.0%
N-2		Connectivity			1	1				0.0%
A-1	**Applications**	Device Management								0.0%
A-2		Network Management								0.0%
A-3		Data Management								0.0%
A-4		Data Analytics	1		1	2	✓		5.6%	4.4%
A-5		Data Visualization	1		1	2	✓		5.6%	4.4%
A-6		User Interaction/Usability								0.0%
Y-1	**Systems**	Middleware/Integration						3.0%	3.0%	2.4%
Y-2		Alerts and Notifications						3.0%	3.0%	2.4%
Y-3		Security Management						3.0%	3.0%	2.4%
Y-4		Artificial Intelligence		1	1	2	✓	3.0%	9.3%	7.4%
Y-5		System Resiliency						9.9%	9.9%	7.9%
T-1	**Standards**	Security		1		1		1.0%	1.0%	0.8%
T-2		Data			1	1		5.0%	5.0%	3.9%
T-3		Privacy						3.0%	3.0%	2.4%
T-4		Interoperability						10.9%	10.9%	8.7%
								100%	**125%**	**100%**

Figure 25-33: Construction: Use Case, Interview, Desk Research, Survey Technical Results

© Strategy of Things, 2025. All rights reserved.

Figure 25-34 below shows the survey results of the role of the private and public sectors in undertaking research and development to operationalize the use cases.

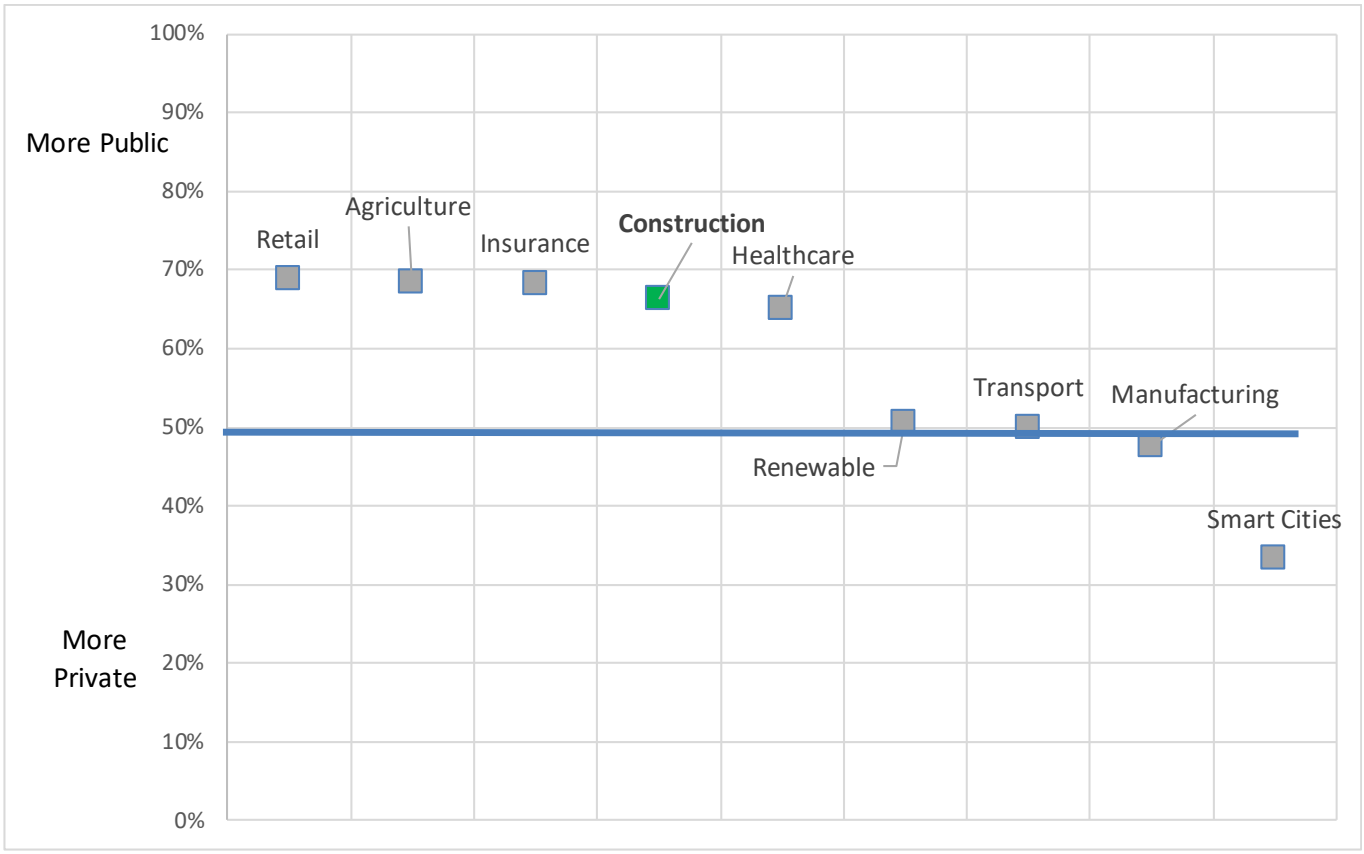


Figure 25-34: Construction: Role of the Public Sector

Figure 25-26 below shows the relative weightings for construction of the top 10 single technologies. This figure is based on an IoT value share of 8%[1736] for construction and a public sector contribution of 66% multiplied by the normalized weighting shown in Figure 25-33

[1736] See Figure 25-3.

© Strategy of Things, 2025. All rights reserved.

Rank	Technology	Weighting	Percentage
1	H-1 Hardware: IoT Sensors	0.00712	19%
2	T-4 Standards: Interoperability	0.00432	12%
3	S-3 Software: Data collect	0.00432	12%
4	Y-5 Systems: Resiliency	0.00393	11%
5	Y-4 Systems: AI	0.00368	10%
6	H-4 Hardware: Edge devices	0.00353	9%
7	H-3 Hardware: Processing	0.00314	8%
8	H-2 Hardware: Actuators	0.00275	7%
9	S-4 Software: Data store	0.00236	6%
10	A-5 Apps: Visualization	0.00221	6%

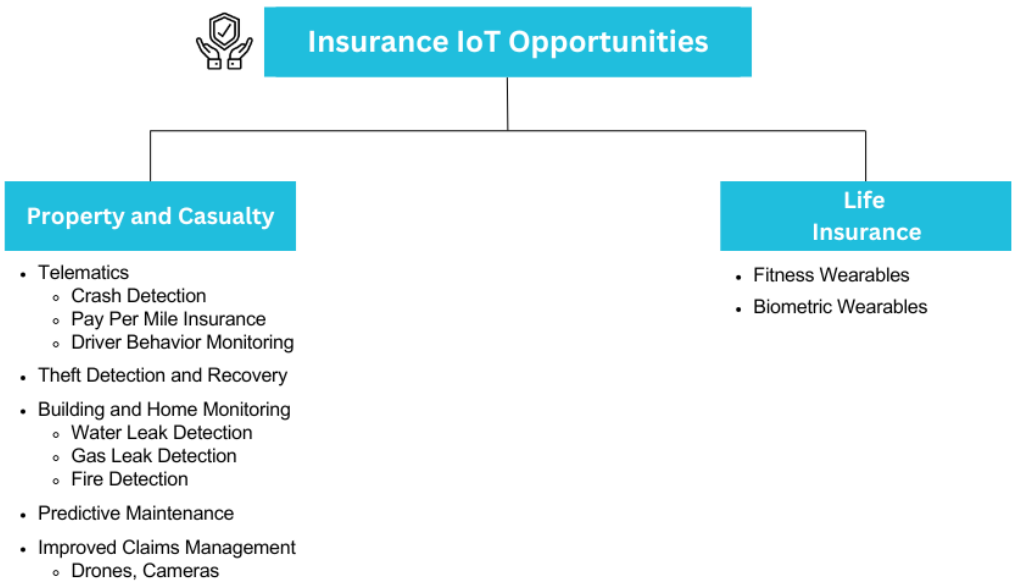
Figure 25-35: Construction: Ranking and Single Technology Weightings

25.2.6. Insurance

The section covers:

- Industry desk research for use cases
- Other industry desk research
- Interviews
- Summary rankings

25.2.6.1. Industry desk research for use cases



© Strategy of Things, 2025. All rights reserved.

Figure 16-1 provided a set of representative use cases for insurance. This section shows the associated technical assessments to either close a gap or operationalize a use case. These assessments were mapped using the taxonomy shown in Figure 11-4.

Figure 25-36 below shows example extracts from the use case analysis and the associated single technology classification.

ID	Single technology	Use Case Extracts
1	H-1 1.Hardware: IoT Sensors	By plugging a small telematics device into their car's onboard diagnostic port (OBD-II port), consumers can gain information about when the car is due for repair or how to be a safer driver.
2	N-2 3.Networks: Connect	One of the most significant benefit of the telematics technology is the ease with which it enables stolen vehicles to be detected and recovered
3	A-1 4.Apps: Device manage	Data regarding the state of various parts, detection of a failure, warning signs like speed warnings or proximity levels, will be provided.
4	A-4 4.Apps: Data Analytics	Car owners are able to monitor car temperature, brake condition, tire condition and general car condition.
5	A-5 4 Apps: Data Visual	The insurance industry has made significant improvements by using IOT in order to capture cargo shipment data which is documented for insurance purposes, although real-time visibility to cargo risk remains limited and the claims data that the industry needs to understand loss trends often lags months behind.
6	Y-2 5.Systems: Alerts	In case, an accident occurs, IoT devices will report the incident to the insurer. This report will be forwarded to the nearest service provider.
7	Y-4 5.Systems: AI	AI and IoT will help shape the insurance industry in the coming years as most of the leading insurance agencies are blending their data analytics algorithms with probably the most recent AI innovation so as to enhance the precision of risk calculations.
8	T-4 6.Standards: Interoperability	With the help of analytical tools and AI applied to aggregated data, insurers determine which clinical processes may have the better impact on patient’s wellness.

© Strategy of Things, 2025. All rights reserved.

Figure 25-36: Insurance: Use Case: Single Technology Classifications

Figure 25-37 below tabulates these results using the table structure described in Figure 25-5.

	Property & Casualty	Life/Annuity
H-1 1.Hardware: IoT Sensors	■	
H-2 1.Hardware: Actuators		
H-3 1.Hardware: Processing		
H-4 1.Hardware: Edge devices		
S-1 2.Software: Sensor F/ware		
S-2 2.Software: Edge F/ware		
S-3 2.Software: Data Collect		
S-4 2.Software: Data Store		
N-1 3.Networks: Gateways		
N-2 3.Networks: Connect	■	■
A-1 4.Apps: Device manage	■	■
A-2 4.Apps: Network manage		
A-3 4.Apps: Data Manage		
A-4 4.Apps: Data Analytics	■	■
A-5 4 Apps: Data Visual	■	
A-6 4. Apps: Usability		
Y-1 5.Systems: Middleware		
Y-2 5.Systems: Alerts	■	■
Y-3 5.Systems: Security		
Y-4 5.Systems: AI		■
Y-5 5.Systems: Resiliency		
T-1 6.Standards: Security		
T-2 6.Standards: Data		
T-3 6.Standards: Privacy		
T-4 6.Standards: Interoperability		■

© Strategy of Things, 2025. All rights reserved.

Figure 25-37: Insurance: Use Cases: Single Technology Classifications

25.2.6.2. Other industry desk research

Our desk research identified four additional areas that could delay the use and benefits of IoT services. These are discussed in detail along with the associated IoT Area and single technology component in Figure 25-39 below.

ID	Single Technology	Description
1	H-1 - 1.Hardware: IoT Sensors	By connecting with sensors and IoT gadgets, policies may change in real-time by adapting increasingly around an enrollee's conduct and risk profile.[1737]
2	H-2 - 1.Hardware: Actuators	Robotics has seen many recent accomplishments and this development will keep on changing how people collaborate with their surroundings. Additive manufacturing, otherwise called 3-D printing, will drastically reshape manufacturing and the insurance products in the commercial markets soon. By 2025, 3-D-printed structures will be normal and transporters should survey how this advancement changes risk evaluations.[1738]
3	A-4 – 4.Data Analytics	AI and IoT will help shape the insurance industry in the coming years as most of the leading insurance agencies are blending their data analytics algorithms with the most recent AI innovation to enhance the precision of risk calculations. The explanation behind this is that insurance agencies need huge amounts of information to enhance their appreciation of customer hazard.[1739]
4	Y-4 - 5. Systems: AI	AI processing relies upon the size and nature of accessible data. The more data AI has about clients, the better fit between cost and risk.[1740]

[1737] "The Role of AI and IoT in Future of Insurance Industry", Analytics Insight, P. Dialani, December 2018. Link

[1738] ibid.

[1739] ibid.

[1740] ibid.

© Strategy of Things, 2025. All rights reserved.

Figure 25-38: Insurance: Other Desk Research: Single Technology Classifications

Figure 25-39 tabulates these results.

H-1 1.Hardware: IoT Sensors	
H-2 1.Hardware: Actuators	
H-3 1.Hardware: Processing	
H-4 1.Hardware: Edge devices	
S-1 2.Software: Sensor F/ware	
S-2 2.Software: Edge F/ware	
S-3 2.Software: Data Collect	
S-4 2.Software: Data Store	
N-1 3.Networks: Gateways	
N-2 3.Networks: Connect	
A-1 4.Apps: Device manage	
A-2 4.Apps: Network manage	
A-3 4.Apps: Data Manage	
A-4 4.Apps: Data Analytics	
A-5 4 Apps: Data Visual	
A-6 4. Apps: Usability	
Y-1 5.Systems: Middleware	
Y-2 5.Systems: Alerts	
Y-3 5.Systems: Security	
Y-4 5.Systems: AI	
Y-5 5.Systems: Resiliency	
T-1 6.Standards: Security	
T-2 6.Standards: Data	
T-3 6.Standards: Privacy	
T-4 6.Standards: Interoperability	

Figure 25-39: Insurance: Other Desk Research: Single Technology Classifications

25.2.6.3. Interviews

Interviews were conducted with three organizations to gather IoT adoption trends and issues. Figure 25-40 below lists the interviewees.

© Strategy of Things, 2025. All rights reserved.

	Company Name	Type of Company
1	Gartner	Research organization
2	HSB	Offers insurance for equipment breakdown, cyber risk & employment practices liability
3	Ciceri	Insurer

Figure 25-40: Insurance: Stakeholder Interviews

The interviews identified six areas that could delay the use and benefits of IoT services. Close to verbatim excerpts from the interviews along with a technical allocation for each set of comments is shown below in Figure 25-41.

ID	Single technology	Interviewee comment
1	H-1 1.Hardware: IoT Sensors	For vehicle telematics there is the connected vehicle, there's an aftermarket device attached/plugged into the vehicle and then there are mobile apps on operator's cell phone, all of which can offload data
2	N-2 3.Networks: Connect	Cellular SIM- into remote areas, there's a challenge out there, because some devices will allow you to connect with the strongest signal, whereas other devices, the SIM card only operates through one provider.
3	A-3 4.Apps: Data Manage	In the past year, we have hired several analysts across the company, from an underwriting, inspection and iot perspective, to analyze all this data and make good use of the data that we are collecting and cleansing the data
4	A-4 4.Apps: Data Analytics	Companies do not usually have top technology talent and have not invested to have the proper infrastructure in place (people and technology challenges), they can write risk very well, but to analyze patters in the data, they could struggle

© Strategy of Things, 2025. All rights reserved.

ID	Single technology	Interviewee comment
5	T-2 6.Standards: Data	Make it easy for the data to flow back and forth, help facilitate the standard transfer, storage and availability of the data Sensors, cell phone and an aftermarket devices in a vehicle all behave differently. The normalization, or harmonization of data from different sets is a huge challenge for the industry.
6	T-3 6.Standards: Privacy	Who owns the data? Car manufacturer? Software creator? Company? Manufactures are trying to own the data coming out of their automobiles everyone wants to monetize their data and not share it

Figure 25-41: Insurance: Stakeholder Interviews: Single Technology Classifications

Figure 25-42 tabulates these results.

© Strategy of Things, 2025. All rights reserved.

H-1 1.Hardware: IoT Sensors	
H-2 1.Hardware: Actuators	
H-3 1.Hardware: Processing	
H-4 1.Hardware: Edge devices	
S-1 2.Software: Sensor F/ware	
S-2 2.Software: Edge F/ware	
S-3 2.Software: Data Collect	
S-4 2.Software: Data Store	
N-1 3.Networks: Gateways	
N-2 3.Networks: Connect	
A-1 4.Apps: Device manage	
A-2 4.Apps: Network manage	
A-3 4.Apps: Data Manage	
A-4 4.Apps: Data Analytics	
A-5 4 Apps: Data Visual	
A-6 4. Apps: Usability	
Y-1 5.Systems: Middleware	
Y-2 5.Systems: Alerts	
Y-3 5.Systems: Security	
Y-4 5.Systems: AI	
Y-5 5.Systems: Resiliency	
T-1 6.Standards: Security	
T-2 6.Standards: Data	
T-3 6.Standards: Privacy	
T-4 6.Standards: Interoperability	

Figure 25-42: Insurance: Stakeholder Interviews: Single Technology Classifications

25.2.6.4. Ranking technology infrastructure gaps

Figure 25-43 overleaf shows the integration of use cases, survey, interview and desk research to produce a ranking of the single technologies required to operationalize the most important use cases.

© Strategy of Things, 2025. All rights reserved.

			Desk (Use case	esk (Industry	Interviews	Total	Include	Survey	Adjusted	Normalized
H-1	**Hardware**	IoT Sensors	1	1	1	3	✓	6.9%	14.2%	12.0%
H-2		Actuators		1		1		10.3%	10.3%	8.7%
H-3		Processing						3.4%	3.4%	2.9%
H-4		Edge Devices						3.4%	3.4%	2.9%
S-1	**Software**	Sensor Firmware						3.4%	3.4%	2.9%
S-2		Edge Firmware/OS						3.4%	3.4%	2.9%
S-3		Data Collection/Ingestion						3.4%	3.4%	2.9%
S-4		Data Storage						3.4%	3.4%	2.9%
N-1	**Networking**	Gateways								0.0%
N-2		Connectivity	1		1	2	✓		5.6%	4.7%
A-1	**Applications**	Device Management	1			1				0.0%
A-2		Network Management								0.0%
A-3		Data Management			1	1				0.0%
A-4		Data Analytics	1	1	1	3	✓		5.6%	4.7%
A-5		Data Visualization	1			1				0.0%
A-6		User Interaction/Usability								0.0%
Y-1	**Systems**	Middleware/Integration						3.4%	3.4%	2.9%
Y-2		Alerts and Notifications	1			1		3.4%	3.4%	2.9%
Y-3		Security Management						10.3%	10.3%	8.7%
Y-4		Artificial Intelligence		1		1		6.9%	6.9%	5.8%
Y-5		System Resiliency						3.4%	3.4%	2.9%
T-1	**Standards**	Security						6.9%	6.9%	5.8%
T-2		Data			1	1		3.4%	3.4%	2.9%
T-3		Privacy			1	1		13.8%	13.8%	11.6%
T-4		Interoperability						10.3%	10.3%	8.7%
								100%	**119%**	**100%**

Figure 25-43: Insurance: Interview, Desk Research & Survey Integrated Results

© Strategy of Things, 2025. All rights reserved.

Figure 25-44 below shows the survey results of the role of the private and public sectors in undertaking research and development to operationalize the use cases.

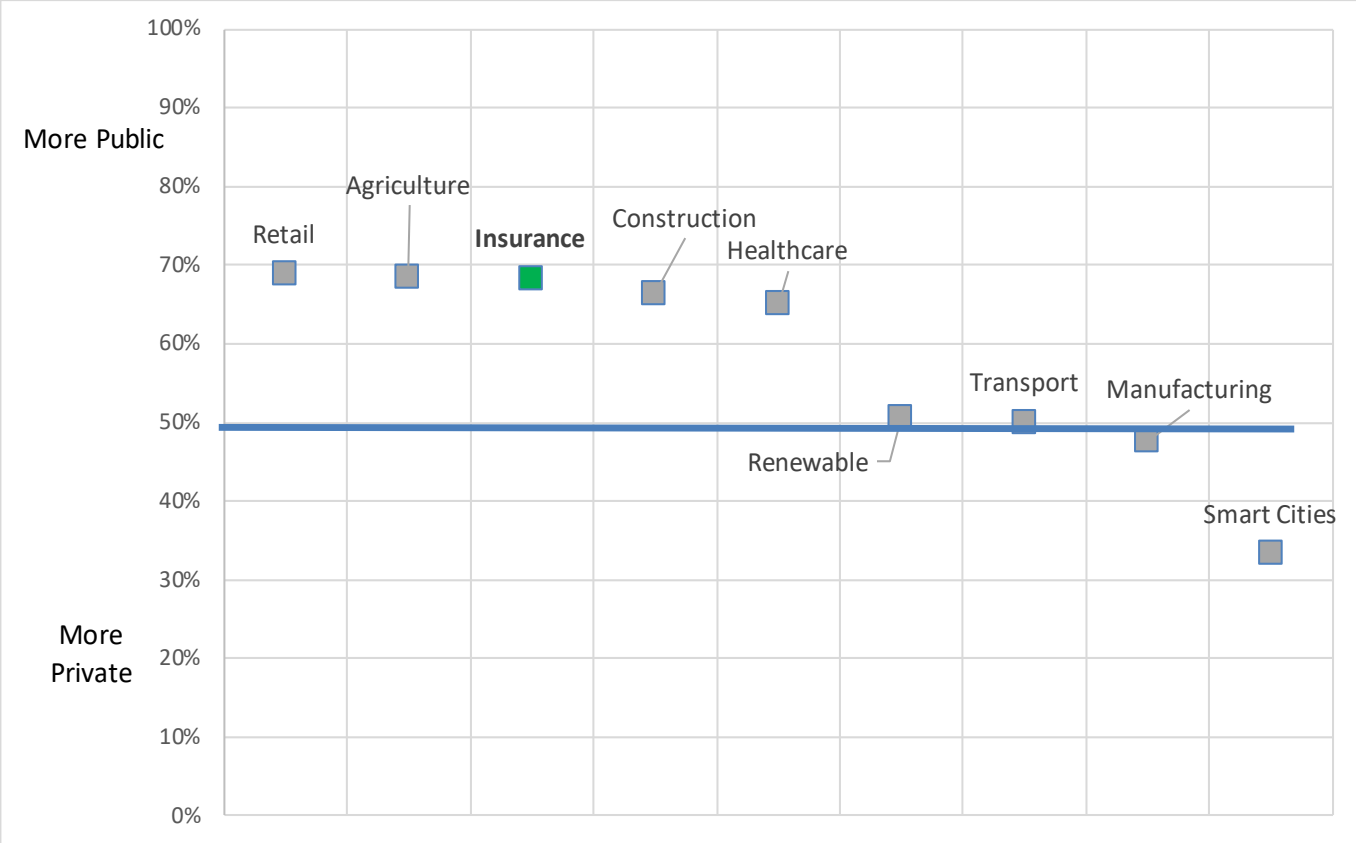


Figure 25-44: Insurance: Role of the Public Sector in R&D

Figure 25-45 below shows the relative weightings for insurance of the top 10 single technologies. This figure is based on an IoT value share of 3%[1741] for insurance and a public sector contribution of 68% multiplied by the normalized weighting shown in Figure 25-43.

[1741] See Figure 25-3

© Strategy of Things, 2025. All rights reserved.

Rank	Technology	Weighting	Percentage
1	H-1 Hardware: IoT Sensors	0.00265	16%
2	T-3 Standards: Privacy	0.00257	16%
3	T-4 Standards: Interoperability	0.00193	12%
4	Y-3 Systems: Security	0.00193	12%
5	H-2 Hardware: Actuators	0.00193	12%
6	T-1 Standards: Security	0.00128	8%
7	Y-4 Systems: AI	0.00128	8%
8	A-4 Apps: Data analytics	0.00104	6%
9	N-2 Network: Connectivity	0.00104	6%
10	T-2 Standards: Data	0.00064	4%

Figure 25-45: Insurance: Ranking and Single Technology Weightings

25.2.7. Smart Cities

The section covers:

- Industry desk research for use cases
- Other industry desk research
- Interviews
- Summary rankings

25.2.7.1. Industry desk research for use cases

Figure 17-2 provided a set of representative use cases for smart cities. This section provides the technical assessments for each use case group. Issues identified in the desk research were mapped to the taxonomy in Figure 11-4 using the table structure described in Figure 25-5.

Figure 25-46 below shows the single technology component classifications of each of the use cases from desk research.

© Strategy of Things, 2025. All rights reserved.

	City operations	Public safety	Environment & Sustainability	Mobility and Transportation	Smart Buildings & Campuses
H-1 1.Hardware: IoT Sensors	■				■
H-2 1.Hardware: Actuators					
H-3 1.Hardware: Processing					
H-4 1.Hardware: Edge devices					
S-1 2.Software: Sensor F/ware					
S-2 2.Software: Edge F/ware					
S-3 2.Software: Data Collect					
S-4 2.Software: Data Store					
N-1 3.Networks: Gateways					
N-2 3.Networks: Connect	■				
A-1 4.Apps: Device manage	■				■
A-2 4.Apps: Network manage					
A-3 4.Apps: Data Manage					
A-4 4.Apps: Data Analytics	■				■
A-5 4 Apps: Data Visual	■				
A-6 4. Apps: Usability	■				
Y-1 5.Systems: Middleware					
Y-2 5.Systems: Alerts	■				■
Y-3 5.Systems: Security					
Y-4 5.Systems: AI	■				
Y-5 5.Systems: Resiliency					
T-1 6.Standards: Security					
T-2 6.Standards: Data					
T-3 6.Standards: Privacy					
T-4 6.Standards: Interoperability					

Figure 25-46: Smart Cities: Use Cases: Single Technology Classifications

25.2.7.2. Other industry desk research

In addition to the above use cases, desk research identified an additional four gaps that could delay the use and benefits of IoT services. These are listed in detail below in Figure 25-47.

© Strategy of Things, 2025. All rights reserved.

ID	Single technology	Comment
1	S-3 2.Software: Data Collect	Data from various sources such as people, their phones, devices, sensors, cameras, RFID chips, smart meters and other relevant points. These data are used to make better decisions when controlling different city infrastructures.
2	T-1 6.Standards: Security	Smart city practitioners adopt standards early to promote the interoperability and security of solutions
3	T-2 6.Standards: Data	Provide metrics for smart cities and guidance on implementation
4	T-3 6.Standards: Privacy	Privacy guidelines provide recommendations and guidance on the management of privacy and on the use of supporting standards

Figure 25-47: Smart Cities: Other Desk Research: Single Technology Classifications

Figure 25-48 below summarizes these results.

© Strategy of Things, 2025. All rights reserved.

H-1 1.Hardware: IoT Sensors	
H-2 1.Hardware: Actuators	
H-3 1.Hardware: Processing	
H-4 1.Hardware: Edge devices	
S-1 2.Software: Sensor F/ware	
S-2 2.Software: Edge F/ware	
S-3 2.Software: Data Collect	
S-4 2.Software: Data Store	
N-1 3.Networks: Gateways	
N-2 3.Networks: Connect	
A-1 4.Apps: Device manage	
A-2 4.Apps: Network manage	
A-3 4.Apps: Data Manage	
A-4 4.Apps: Data Analytics	
A-5 4 Apps: Data Visual	
A-6 4. Apps: Usability	
Y-1 5.Systems: Middleware	
Y-2 5.Systems: Alerts	
Y-3 5.Systems: Security	
Y-4 5.Systems: AI	
Y-5 5.Systems: Resiliency	
T-1 6.Standards: Security	
T-2 6.Standards: Data	
T-3 6.Standards: Privacy	
T-4 6.Standards: Interoperability	

Figure 25-48: Smart Cities: Other Desk Research: Single Technology Classifications

25.2.7.3. Interviews

Interviews were conducted with one organization to gather IoT adoption trends and issues. Figure 25-49 below lists the interviewee.

	Company Name	Type of Company
1	AIOTA	Advocacy group

Figure 25-49: Smart Cities: Stakeholder Interviews

The interviews identified four areas that could delay the use and benefits of IoT services. Close to verbatim excerpts from the interviews along with a technical allocation for each set of comments are shown below in Figure 25-14.

© Strategy of Things, 2025. All rights reserved.

ID	Single technology	Verbatim interviewee comment
1	S3. 2.Software: Data Collect	Most projects are one-offs. They start with addressing the connectivity and then use that to drive intelligence, like how do I connect bus to intersection, etc. In Saudi Arabia NEOM project, start with data. Created a cognitive, digital twin engine and how that connects into all parts of the city. And how you make sure that you have this complicated environment where all the agencies are sharing data and that data has context so it's not just having it a database or in a data warehouse or data lake. And it's not just figuring out the data engineering, the data schema and how you Extract, Transform, Load (ETL), but it's also the ontology for the data and the context for it.
2	T1 6. Standards: Security T3. 6.Standards: Privacy	Example of NIST cybersecurity framework. They were instrumental in figuring out and saying these are the regulations, because cybersecurity is too important to leave it to an individual entity. It comes back to data and data are too important a thing to leave to an individual or entity. And that's something that the government needs to set standards are to a certain level.
3	T2. 6.Standards: Data	Siloed data - State of data in cities is that it is siloed. In addition, you have private entities that operate in a city that doesn't share data. Example – multi modal mobility. data from ridesharing is not shared with cities but they use city data.
4	T-3 6.Standards: Privacy	Is an issue that is solvable. We definitely need a GDPR. And there are people working on data governance data policy framework. Everything that I'm talking about is all metadata. Note to reader: GDPR is European Union's General Data Protection Regulation.

Figure 25-50: Smart Cities: Stakeholder Interviews: Single Technology Classifications

Figure 25-51 below summarizes these results.

© Strategy of Things, 2025. All rights reserved.

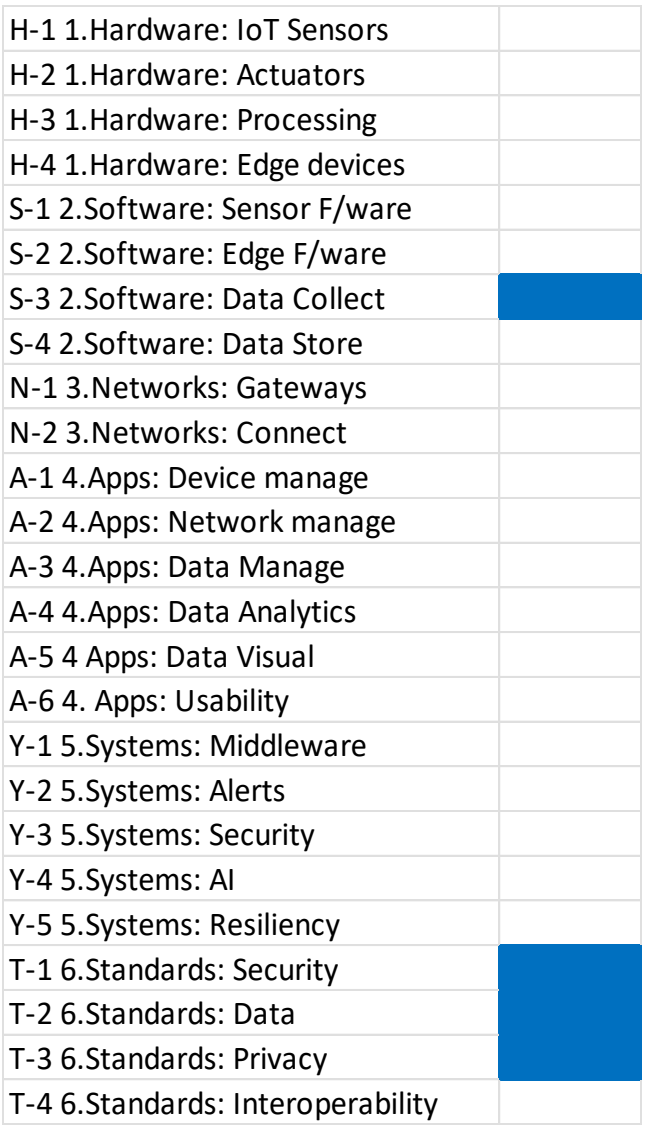


Figure 25-51: Smart Cities: Stakeholder Interviews: Single Technology Classifications

25.2.7.4. Ranking technology infrastructure gaps

Figure 25-52 overleaf shows the integration of use cases, survey, interview and desk research to produce a ranking of the single technologies required to operationalize the most important use cases.

.

© Strategy of Things, 2025. All rights reserved.

			Desk (Use case)	Desk (Industry)	Interviews	Total	Include	Survey	Adjusted	Normalized
H-1	**Hardware**	IoT Sensors	1			1		10.6%	10.6%	9.3%
H-2		Actuators						1.5%	1.5%	1.3%
H-3		Processing						6.1%	6.1%	5.3%
H-4		Edge Devices						3.0%	3.0%	2.7%
S-1	**Software**	Sensor Firmware						1.5%	1.5%	1.3%
S-2		Edge Firmware/OS						3.0%	3.0%	2.7%
S-3		Data Collection/Ingestion		1		1		4.5%	4.5%	4.0%
S-4		Data Storage						1.5%	1.5%	1.3%
N-1	**Networking**	Gateways								0.0%
N-2		Connectivity								0.0%
A-1	**Applications**	Device Management	1			1				0.0%
A-2		Network Management								0.0%
A-3		Data Management								0.0%
A-4		Data Analytics	1		1	2	✓		5.6%	4.9%
A-5		Data Visualization								0.0%
A-6		User Interaction/Usability								0.0%
Y-1	**Systems**	Middleware/Integration						3.0%	3.0%	2.7%
Y-2		Alerts and Notifications	1			1		3.0%	3.0%	2.7%
Y-3		Security Management						7.6%	7.6%	6.6%
Y-4		Artificial Intelligence			1	1		10.6%	10.6%	9.3%
Y-5		System Resiliency						4.5%	4.5%	4.0%
T-1	**Standards**	Security		1		1		9.1%	9.1%	8.0%
T-2		Data		1	1	2	✓	12.1%	20.7%	18.2%
T-3		Privacy		1		1		7.6%	7.6%	6.6%
T-4		Interoperability						10.6%	10.6%	9.3%
								100%	**114%**	**100%**

Figure 25-52: Smart Cities: Interview, Desk Research & Survey Integrated Results

© Strategy of Things, 2025. All rights reserved.

Figure 25-53 below shows the survey results of the role of the private and public sectors in undertaking research and development to operationalize the use cases.

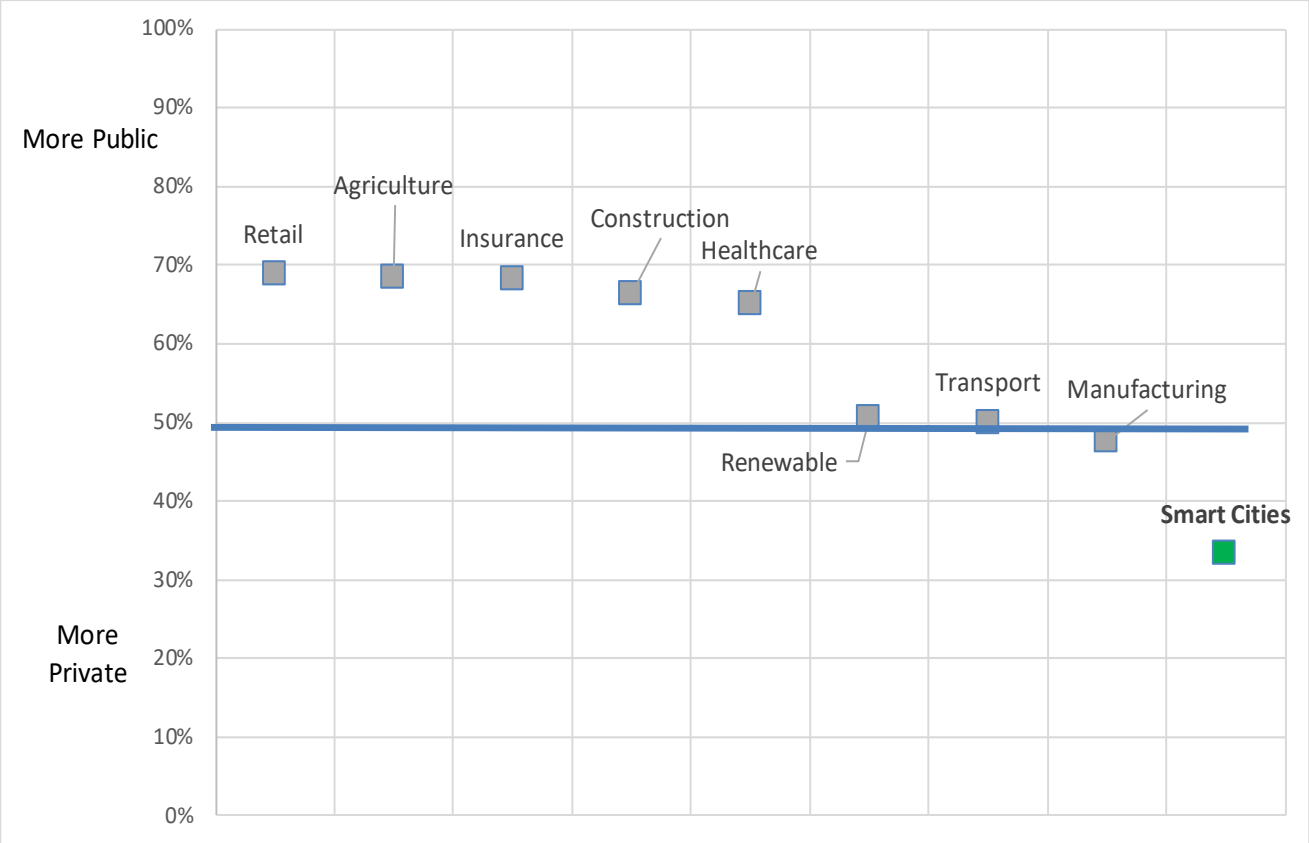


Figure 25-53: Smart Cities: Role of the Public Sector

Figure 25-54 below shows the relative weightings for smart cities of the top 10 single technologies. This figure is based on an IoT value share of 10%[1742] for smart cities and a public sector contribution of 33% multiplied by the normalized weighting shown in Figure 25-52.

[1742] See Figure 25-3

© Strategy of Things, 2025. All rights reserved.

Rank	Technology	Weighting	Percentage
1	T-2 Standards: Data	0.00582	22%
2	T-4 Standards: Interoperability	0.00298	11%
3	Y-4 Systems: AI	0.00298	11%
4	H-1 Hardware: IoT Sensors	0.00298	11%
5	T-1 Standards: Security	0.00255	10%
6	T-3 Standards: Privacy	0.00213	8%
7	Y-3 Systems: Security	0.00213	8%
8	H-3 Hardware: Processing	0.00170	7%
9	A-4 Apps: Data analytics	0.00157	6%
10	Y-5 Systems: Resiliency	0.00128	5%

Figure 25-54: Smart Cities: Ranking and Single Technology Weightings

25.2.8. Transport

The section covers:

- Industry desk research for use cases
- Other industry desk research
- Interviews
- Summary rankings

25.2.8.1. Industry desk research for use cases

Figure 18-4 provided a set of the representative use cases for transport. This section provides the technical assessments for each use case group. Issues identified in the desk research were mapped to the taxonomy in Figure 11-4 using the table structure described in Figure 25-5.

Figure 25-55 below shows the single technology component classifications of each of the use cases from desk research.

© Strategy of Things, 2025. All rights reserved.

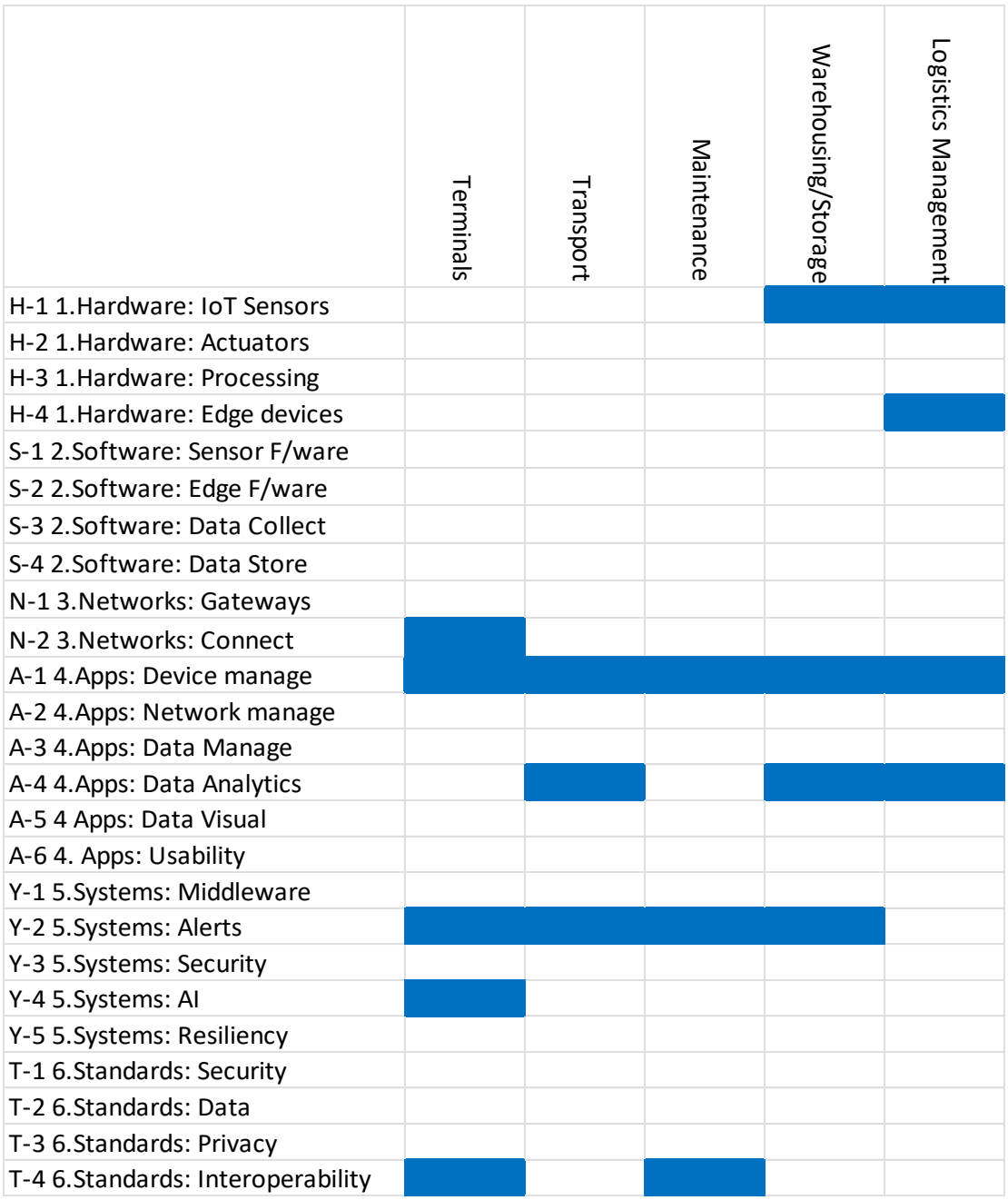


Figure 25-55: Transport and Logistics: Use Cases: Single Technology Classifications

25.2.8.2. Other industry desk research

In addition to the above use cases, desk research identified additional single technology component issues in standards that could delay the use and benefits of IoT services. These are listed in detail below in Figure 25-56.

© Strategy of Things, 2025. All rights reserved.

ID	Single technology	Comment
1	T-1 6.Standards: Security T-2 6.Standards: Data T-3 6.Standards: Privacy T-4 6.Standards: Interoperability	The Federal Transit Administration's Standards Development Program plans to "devise or expand existing transit standards due to innovation and technological advances, determine the need for new transit standards in areas where standards are lacking or where there are gaps within existing standards and work with the transit industry to develop and implement safety and other standards and best practices.[1743]"

Figure 25-56: Transport and Logistics: Other Desk Research: Single Technology Classifications

Figure 25-57 below summarizes these results.

[1743] "Standards Development Program", Federal Transit Administration. Link

© Strategy of Things, 2025. All rights reserved.

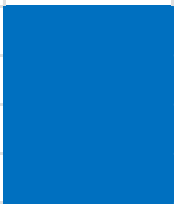
H-1 1.Hardware: IoT Sensors	
H-2 1.Hardware: Actuators	
H-3 1.Hardware: Processing	
H-4 1.Hardware: Edge devices	
S-1 2.Software: Sensor F/ware	
S-2 2.Software: Edge F/ware	
S-3 2.Software: Data Collect	
S-4 2.Software: Data Store	
N-1 3.Networks: Gateways	
N-2 3.Networks: Connect	
A-1 4.Apps: Device manage	
A-2 4.Apps: Network manage	
A-3 4.Apps: Data Manage	
A-4 4.Apps: Data Analytics	
A-5 4 Apps: Data Visual	
A-6 4. Apps: Usability	
Y-1 5.Systems: Middleware	
Y-2 5.Systems: Alerts	
Y-3 5.Systems: Security	
Y-4 5.Systems: AI	
Y-5 5.Systems: Resiliency	
T-1 6.Standards: Security	
T-2 6.Standards: Data	
T-3 6.Standards: Privacy	
T-4 6.Standards: Interoperability	

Figure 25-57: Transport and Logistics: Other Desk Research: Single Technology Classifications

25.2.8.3. Interviews

Interviews were conducted with two organizations to gather IoT adoption trends and issues. Figure 25-58 below lists the interviewees.

© Strategy of Things, 2025. All rights reserved.

	Company Name	Type of Company
1	ITS America	Research and deployment of intelligent transportation technologies
2	USDT	Public sector

Figure 25-58: Transport and Logistics: Stakeholder Interviews

The interviews identified four areas that could delay the use and benefits of IoT services. Close to verbatim excerpts from the interviews along with a technical allocation for each set of comments are shown below in Figure 25-59.

ID	Single technology	Verbatim interviewee comment
1	N-2 3.Networks: Connect	"infrastructure, the connective infrastructure, which is roads and bridges, but increasingly is fiber and broadband, you know, high speed, equitable access to broadband high-speed broadband. "
2	A-2 4.Apps: Network manage	"Rural areas have broadband gaps, public areas have issues with signal or building interference and network congestion"
3	Y-3 5.Systems: Security	"Public sector feels the push to embrace the technology but they do not have the capacity to ensure their residents, users, customers data will be secure, appropriate cybersecurity measures in place…."
4	T-1, 6.Standards: Security T-3 6.Standards: Privacy	"Privacy and security are huge issues and may be the main outstanding issues, not just actual privacy issues it is perceived issues, until public is onboard and accept…"

Figure 25-59: Transport and Logistics: Stakeholder Interviews: Single Technology Classifications

Figure 25-60 below summarizes these results.

© Strategy of Things, 2025. All rights reserved.

H-1 1.Hardware: IoT Sensors	
H-2 1.Hardware: Actuators	
H-3 1.Hardware: Processing	
H-4 1.Hardware: Edge devices	
S-1 2.Software: Sensor F/ware	
S-2 2.Software: Edge F/ware	
S-3 2.Software: Data Collect	
S-4 2.Software: Data Store	
N-1 3.Networks: Gateways	
N-2 3.Networks: Connect	
A-1 4.Apps: Device manage	
A-2 4.Apps: Network manage	
A-3 4.Apps: Data Manage	
A-4 4.Apps: Data Analytics	
A-5 4 Apps: Data Visual	
A-6 4. Apps: Usability	
Y-1 5.Systems: Middleware	
Y-2 5.Systems: Alerts	
Y-3 5.Systems: Security	
Y-4 5.Systems: AI	
Y-5 5.Systems: Resiliency	
T-1 6.Standards: Security	
T-2 6.Standards: Data	
T-3 6.Standards: Privacy	
T-4 6.Standards: Interoperability	

Figure 25-60: Transport and Logistics: Stakeholder Interviews: Single Technology Classifications

25.2.8.4. Ranking technology infrastructure gaps

Figure 25-61 overleaf shows the integration of use cases, survey, interview and desk research to produce a ranking of the single technologies required to operationalize the most important use cases.

© Strategy of Things, 2025. All rights reserved.

			Desk (Use case)	Desk (Industry)	Interviews	Total	Include	Survey	Adjusted	Normalized
H-1	**Hardware**	IoT Sensors	1			1		8.6%	8.6%	7.1%
H-2		Actuators						3.4%	3.4%	2.8%
H-3		Processing						1.7%	1.7%	1.4%
H-4		Edge Devices						6.9%	6.9%	5.7%
S-1	**Software**	Sensor Firmware						3.4%	3.4%	2.8%
S-2		Edge Firmware/OS						3.4%	3.4%	2.8%
S-3		Data Collection/Ingestion						12.1%	12.1%	10.0%
S-4		Data Storage						5.2%	5.2%	4.3%
N-1	**Networking**	Gateways								0.0%
N-2		Connectivity			1	1				0.0%
A-1	**Applications**	Device Management	1			1				0.0%
A-2		Network Management			1	1				0.0%
A-3		Data Management								0.0%
A-4		Data Analytics	1			1				0.0%
A-5		Data Visualization								0.0%
A-6		User Interaction/Usability								0.0%
Y-1	**Systems**	Middleware/Integration						3.4%	3.4%	2.8%
Y-2		Alerts and Notifications	1			1		3.4%	3.4%	2.8%
Y-3		Security Management			1	1		10.3%	10.3%	8.5%
Y-4		Artificial Intelligence						8.6%	8.6%	7.1%
Y-5		System Resiliency						8.6%	8.6%	7.1%
T-1	**Standards**	Security		1	1	2	✓	5.2%	12.4%	10.2%
T-2		Data		1		1		6.9%	6.9%	5.7%
T-3		Privacy		1	1	2	✓	3.4%	10.2%	8.4%
T-4		Interoperability	1	1		2	✓	5.2%	12.4%	10.2%
								100%	**121%**	**100%**

Figure 25-61: Transport and Logistics: Interview, Desk Research and Survey Technical Results

© Strategy of Things, 2025. All rights reserved.

Figure 25-62 below shows the survey results of the role of the private and public sectors in undertaking research and development to operationalize the use cases.

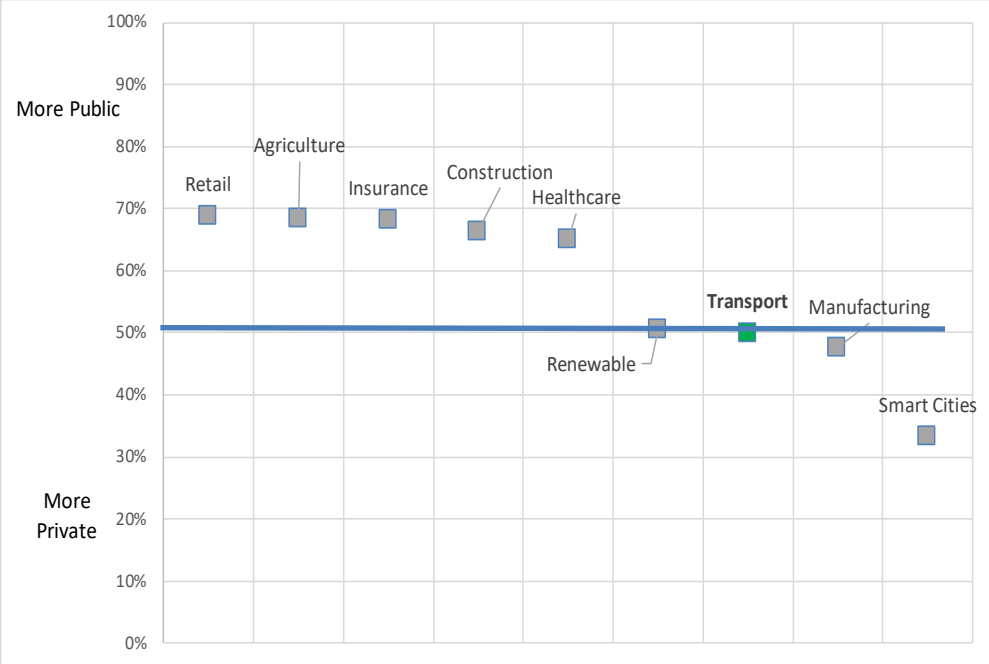


Figure 25-62: Transport and Logistics: Role of the Public Sector in R&D

Figure 25-63 below shows the relative weightings for transportation of the top 10 single technologies. This figure is based on an IoT value share of 5%[1744] for transport and a public sector contribution of 50% multiplied by the adjusted weighting shown in Figure 25-63.

Rank	Technology	Weighting	Percentage
1	T-4 Standards: Interoperability	0.00266	13%
2	T-1 Standards: Security	0.00266	13%
3	S-3 Software: Data collect	0.00259	12%
4	Y-3 Systems: Security	0.00222	11%
5	T-3 Standards: Privacy	0.00220	11%
6	Y-5 Systems: Resiliency	0.00185	9%
7	Y-4 Systems: AI	0.00185	9%
8	H-1 Hardware: IoT Sensors	0.00185	9%
9	T-2 Standards: Data	0.00148	7%
10	H-4 Hardware: Edge devices	0.00148	7%

[1744] See Figure 25-3

© Strategy of Things, 2025. All rights reserved.

Figure 25-63: Transport and Logistics: Ranking and Single Technology Weightings

25.2.9. Healthcare

The section covers:

- Industry desk research for use cases
- Other industry desk research
- Interviews
- Summary rankings

25.2.9.1. Industry desk research for use cases

Figure 19-4 provided a set of the representative use cases for healthcare. This section provides the technical assessments for each use case group. Issues identified in the desk research were mapped to the taxonomy in Figure 11-4 using the table structure described in Figure 25-5.

Figure 25-64 below shows the single technology component classifications of each of the use cases from desk research.

© Strategy of Things, 2025. All rights reserved.

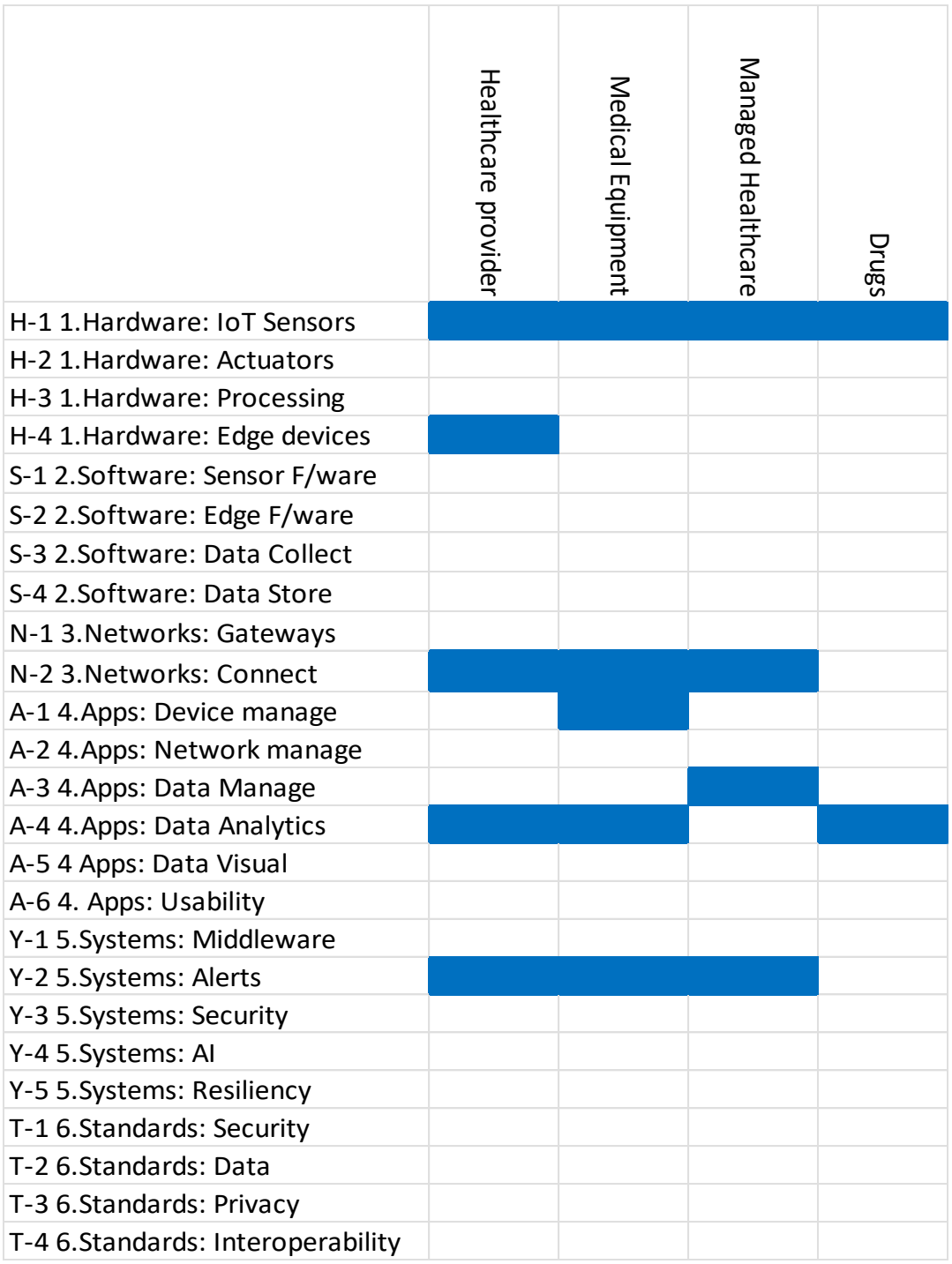


Figure 25-64: Healthcare: Use Cases: Single Technology Classifications

25.2.9.2. Other industry desk research

In addition to the above use cases, desk research identified an additional nine single technology component issues that could delay the use and benefits of IoT services. These are listed in detail below in Figure 25-65.

© Strategy of Things, 2025. All rights reserved.

ID	Single technology	Comment
1	H-3 1.Hardware: Processing	This refers to the way healthcare systems manage information. It involves the implementation of technology to streamline and improve the delivery of care
2	S-3 2.Software: Data Collect	Gathering patient data from various sources across providers and organizations. It allows healthcare providers to enter patient information into a database where it can be securely stored, analyzed and shared.
3	S-4 2.Software: Data Store	Involves securely storing patient data in a manner that ensures its accessibility and integrity. The three options available for data storage in healthcare are on-premises, cloud or hybrid
4	A-1 4.Apps: Device manage	The use of technology to manage and secure devices used in healthcare. It includes the implementation of policies and procedures to safeguard health information on mobile devices
5	A-3 4.Apps: Data Manage	It involves not only organizing medical data but also integrating it and enabling its analysis to make patient care more efficient
6	A-4 4.Apps: Data Analytics	Helps healthcare organizations to evaluate and develop practitioners, detect anomalies in scans, predict outbreaks in illness and lower costs for healthcare organizations
7	Y-2 5.Systems: Alerts	Can refer to notifications about public health emergencies, disease outbreaks as well as updates related to patient care
8	Y-5 5.Systems: Resiliency	The ability of the healthcare system to adjust its functioning before, during, or following changes and disturbances so that it can sustain required operations, even after a major mishap or in the presence of continuous stress
9	T-4 6.Standards: Interoperability	The ability of different information systems, devices and applications to access, exchange, integrate and cooperatively use data in a coordinated manner, within and across organizational, regional and national boundaries

© Strategy of Things, 2025. All rights reserved.

Figure 25-65: Healthcare: Other Desk Research: Single Technology Classifications

Figure 25-66 below summarizes these results.

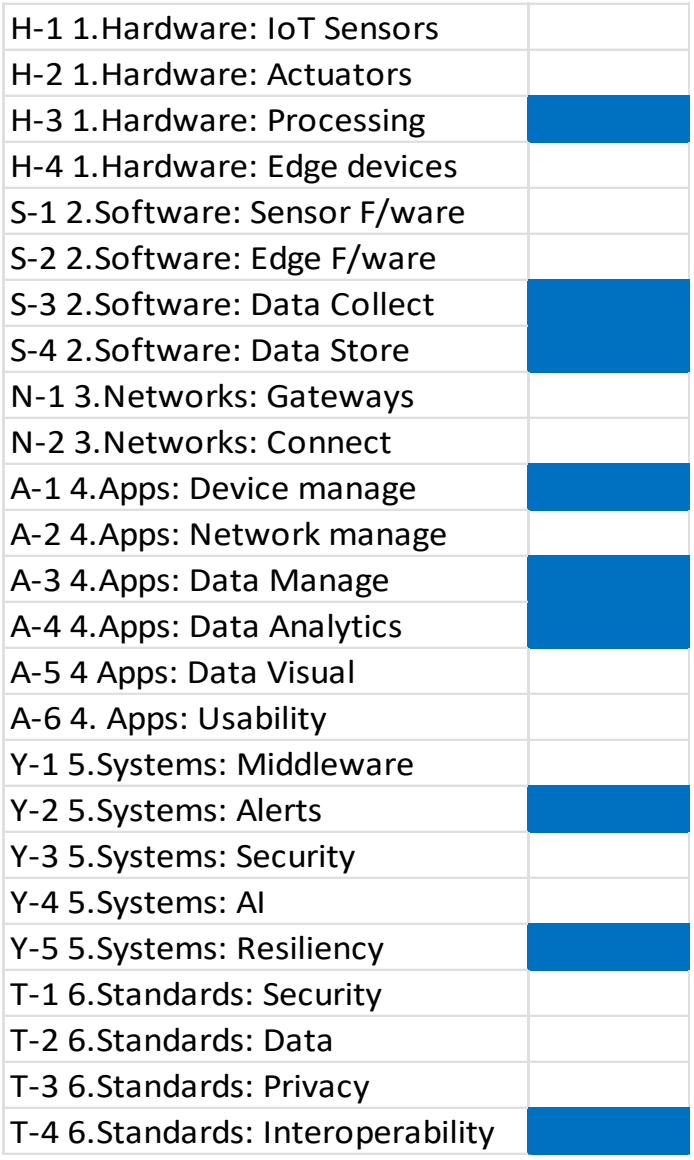


Figure 25-66: Healthcare: Other Desk Research: Single Technology Classifications

25.2.9.3. Interviews

Interviews were conducted with one organization to gather IoT adoption trends and issues. Figure 25-68 below lists the interviewee.

© Strategy of Things, 2025. All rights reserved.

	Company Name	Type of Company
1	Accenture	Management Consulting

Figure 25-67: Healthcare: Stakeholder Interviews

The interviews identified seven areas that could delay the use and benefits of IoT services. Close to verbatim excerpts from the interviews along with a technical allocation for each set of comments are shown below in Figure 25-68.

ID	Single technology	Verbatim interviewee comment
1	H-1 1.Hardware: IoT Sensors	Fast growth - healthcare is one of the fast growing areas, mainly due to remote monitoring, telemedicine... Lots of instrumentation on patients.
2	H-4 Hardware: Edge devices	Healthcare- small handheld products, they do not want batteries, they want the product sealed in the medical environment, hermetically sealed…using RF long distance wireless charging… works with partners who build their own RF harvesters…. But also work with companies that build complete RF environment from transmitter to receiver… complete solution to allow long distance wireless charging.
3	S-3 2.Software: Data Collect	Not sure if people know what IoT means, it used to be connected to the internet, now there are so many healthcare devices reading information and this is just consumer facing… on the clinician side how we capture data from machines providing care, all machines are connected to Internet, does this make it IoT?
4	A-1 Apps: Device Management	True value is using IoT to increase the operational efficiency in health service machinery … asset tracking.
5	Y-2: Systems: Alerts	Equipment monitoring and maintenance.

© Strategy of Things, 2025. All rights reserved.

ID	Single technology	Verbatim interviewee comment
6	T-1 6.Standards: Security	All these devices such as Phillips, GE etc have their own standard protocol, Hospitals spend a lot of security, but we do not know how many custom protocols are being run on the network…huge risk, using custom protocols to connect to internal networks….they are hackable.
7	T-2: Standards: Data	Many medical manufactures refuse to share data and protocols, lack of standard protocols pushes slow uptake.

Figure 25-68: Healthcare: Stakeholder Interviews: Single Technology Classifications

Figure 25-69 below summarizes these results.

© Strategy of Things, 2025. All rights reserved.

H-1 1.Hardware: IoT Sensors	
H-2 1.Hardware: Actuators	
H-3 1.Hardware: Processing	
H-4 1.Hardware: Edge devices	
S-1 2.Software: Sensor F/ware	
S-2 2.Software: Edge F/ware	
S-3 2.Software: Data Collect	
S-4 2.Software: Data Store	
N-1 3.Networks: Gateways	
N-2 3.Networks: Connect	
A-1 4.Apps: Device manage	
A-2 4.Apps: Network manage	
A-3 4.Apps: Data Manage	
A-4 4.Apps: Data Analytics	
A-5 4 Apps: Data Visual	
A-6 4. Apps: Usability	
Y-1 5.Systems: Middleware	
Y-2 5.Systems: Alerts	
Y-3 5.Systems: Security	
Y-4 5.Systems: AI	
Y-5 5.Systems: Resiliency	
T-1 6.Standards: Security	
T-2 6.Standards: Data	
T-3 6.Standards: Privacy	
T-4 6.Standards: Interoperability	

Figure 25-69: Healthcare: Stakeholder Interviews: Single Technology Classifications

25.2.9.4. Ranking technology infrastructure gaps

Figure 25-70 overleaf shows the integration of use cases, survey, interview and desk research to produce a ranking of the single technologies required to operationalize the most important use cases.

© Strategy of Things, 2025. All rights reserved.

			Desk (Use case)	Desk (Industry)	Interviews	Total	Include	Survey	Adjusted	Normalized
H-1	**Hardware**	IoT Sensors	1		1	2	✓	11.1%	19.5%	14.7%
H-2		Actuators						7.4%	7.4%	5.6%
H-3		Processing		1		1		4.9%	4.9%	3.7%
H-4		Edge Devices			1	1		6.2%	6.2%	4.6%
S-1	**Software**	Sensor Firmware						7.4%	7.4%	5.6%
S-2		Edge Firmware/OS						6.2%	6.2%	4.6%
S-3		Data Collection/Ingestion		1	1	2	✓	6.2%	13.3%	10.0%
S-4		Data Storage		1		1		3.7%	3.7%	2.8%
N-1	**Networking**	Gateways								0.0%
N-2		Connectivity	1			1				0.0%
A-1	**Applications**	Device Management		1	1	2	✓		5.6%	4.2%
A-2		Network Management								0.0%
A-3		Data Management		1		1				0.0%
A-4		Data Analytics	1	1		2	✓		5.6%	4.2%
A-5		Data Visualization								0.0%
A-6		User Interaction/Usability								0.0%
Y-1	**Systems**	Middleware/Integration						2.5%	2.5%	1.9%
Y-2		Alerts and Notifications	1	1	1	3	✓	2.5%	8.7%	6.6%
Y-3		Security Management						8.6%	8.6%	6.5%
Y-4		Artificial Intelligence						3.7%	3.7%	2.8%
Y-5		System Resiliency		1		1		4.9%	4.9%	3.7%
T-1	**Standards**	Security			1	1		3.7%	3.7%	2.8%
T-2		Data			1	1		3.7%	3.7%	2.8%
T-3		Privacy						7.4%	7.4%	5.6%
T-4		Interoperability		1		1		9.9%	9.9%	7.4%
								100%	**133%**	**100%**

Figure 25-70: Healthcare: Interview, Desk Research and Survey Technical Results

© Strategy of Things, 2025. All rights reserved.

Figure 25-71 below shows the survey results of the role of the private and public sectors in undertaking research and development to operationalize the use cases.

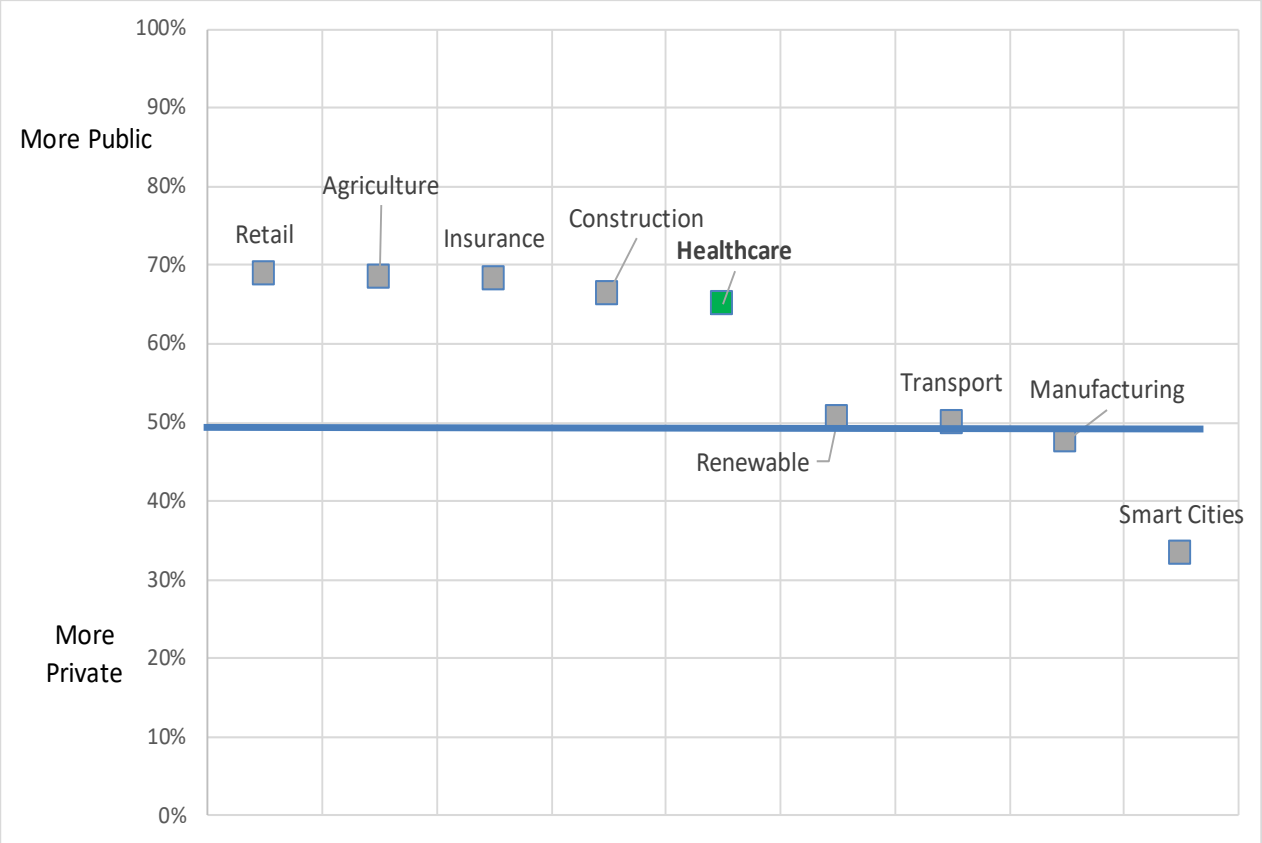


Figure 25-71: Healthcare: Role of the Public Sector in R&D

Figure 25-72 below shows the relative weightings for healthcare for the top 10 technologies. This figure is based on an IoT value share of 39%[1745] for healthcare and a public sector contribution of 65% multiplied by the adjusted weighting shown in Figure 25-70.

[1745] See Figure 25-3

© Strategy of Things, 2025. All rights reserved.

Rank	Technology	Weighting	Percentage
1	H-1 Hardware: IoT Sensors	0.03747	21%
2	S-3 Software: Data collect	0.02562	14%
3	T-4 Standards: Interoperability	0.01896	10%
4	Y-2 Systems: Alerts	0.01673	9%
5	Y-3 Systems: Security	0.01659	9%
6	T-3 Standards: Privacy	0.01422	8%
7	S-1 Software: Sensor F/ware	0.01422	8%
8	H-2 Hardware: Actuators	0.01422	8%
9	S-2 Software: Edge F/ware	0.01185	7%
10	H-4 Hardware: Edge devices	0.01185	7%

Figure 25-72: Healthcare: Most Important Single Technology Weightings

25.2.10. Retail

The section covers:

- Industry desk research for use cases
- Other industry desk research
- Interviews
- Summary rankings

25.2.10.1. Industry desk research for use cases

Figure 20-1 provided a set of representative use cases for retail. This section shows the associated technical assessments to either close a gap or operationalize a use case. These assessments were mapped using the taxonomy shown in Figure 11-4.

Figure 25-73 below shows example extracts from the use case analysis and the associated single technology classification.

ID	Single technology	Use Case Extracts
1	H-1 1.Hardware: IoT Sensors	Real time stock management and fulfilment via RFID, shelf sensors, warehouse robotics
2	H-4 1.Hardware: Edge devices	Fleet management via GPS and other vehicle sensors
3	N-2 3.Networks: Connect	IoT is not possible without fast and reliable broadband connectivity

© Strategy of Things, 2025. All rights reserved.

ID	Single technology	Use Case Extracts
4	A-2 4.Apps: Network manage	Maximize intra-factory communication and performance
5	A-3 4.Apps: Data Manage	Foot traffic monitoring, food safety monitoring, theft control, shopping cart tracking, camera systems
6	A-4 4.Apps: Data Analytics	Manage production data, analyze that data to drive better insights and augment human performance
7	A-5 4 Apps: Data Visual	Digital Signage and Kiosks, touch friendly screens, USB charging, wayfinding, located in malls, cities, airports, transit
8	Y-4 5.Systems: AI	AI for market intelligence, customer service chat bots, rapid prototyping, store design/reformatting

Figure 25-73: Retail: Use Case: Single Technology Classifications

Figure 25-74 below tabulates these results using the table structure described in Figure 25-5.

© Strategy of Things, 2025. All rights reserved.

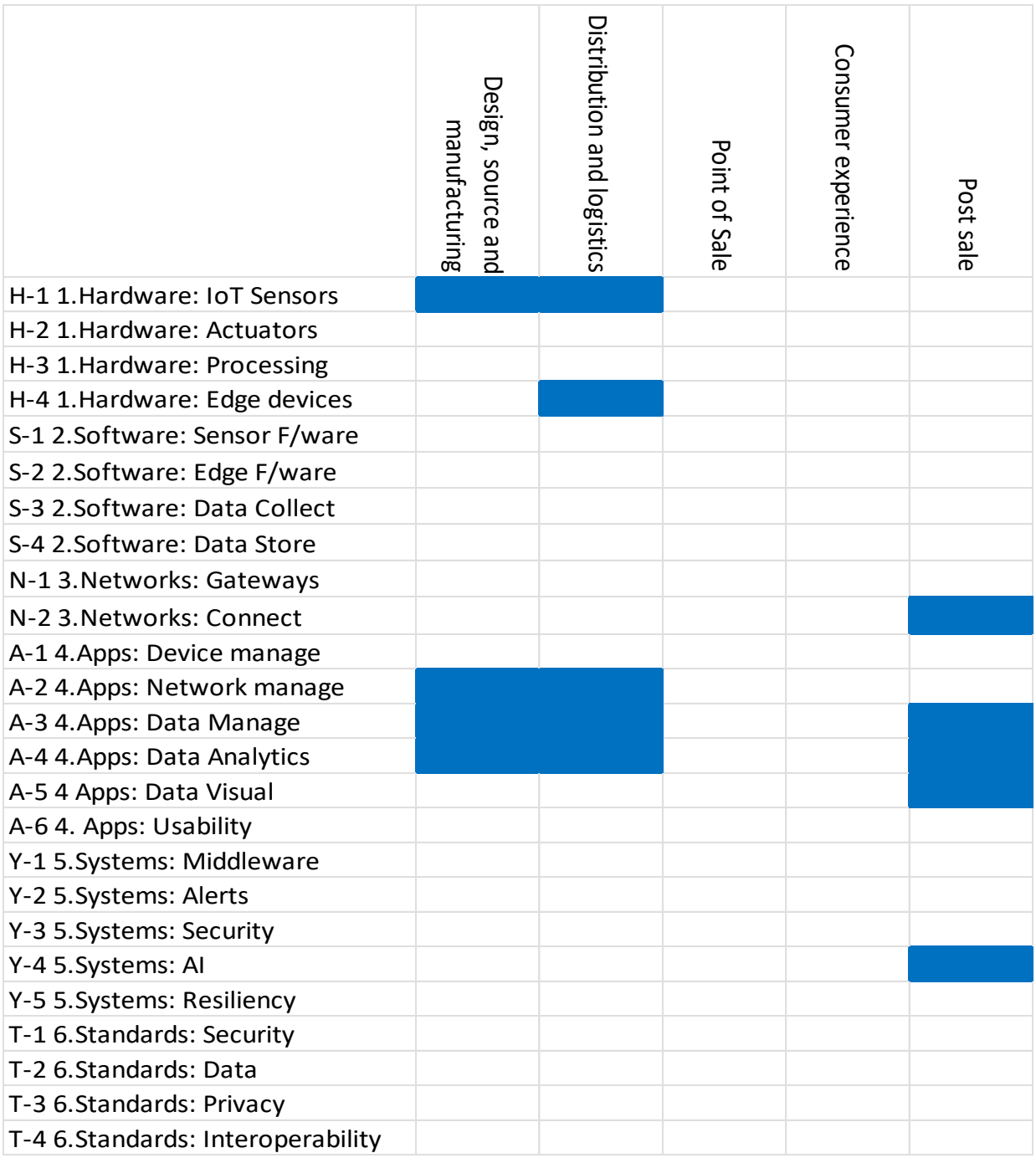


Figure 25-74: Retail: Use Cases: Single Technology Classifications

25.2.10.2. Other industry desk research

In addition to the above use cases, desk research identified two additional single technology component issues that could delay the use and benefits of IoT services. These are listed in detail below in Figure 25-75.

© Strategy of Things, 2025. All rights reserved.

ID	Single technology	Comment
1	A3 Apps Data Management	Collection of various types of data at every stage of product lifecycle. Operational intelligence systems access, aggregate and visualize data. Life Cycle Analysis. Accessible on any web connected device
2	T3 Standards Privacy	Collect data with consumer consent and store with security.

Figure 25-75: Retail: Other Desk Research: Single Technology Classifications

Figure 25-76 below tabulates these results.

© Strategy of Things, 2025. All rights reserved.

H-1 1.Hardware: IoT Sensors	
H-2 1.Hardware: Actuators	
H-3 1.Hardware: Processing	
H-4 1.Hardware: Edge devices	
S-1 2.Software: Sensor F/ware	
S-2 2.Software: Edge F/ware	
S-3 2.Software: Data Collect	
S-4 2.Software: Data Store	
N-1 3.Networks: Gateways	
N-2 3.Networks: Connect	
A-1 4.Apps: Device manage	
A-2 4.Apps: Network manage	
A-3 4.Apps: Data Manage	
A-4 4.Apps: Data Analytics	
A-5 4 Apps: Data Visual	
A-6 4. Apps: Usability	
Y-1 5.Systems: Middleware	
Y-2 5.Systems: Alerts	
Y-3 5.Systems: Security	
Y-4 5.Systems: AI	
Y-5 5.Systems: Resiliency	
T-1 6.Standards: Security	
T-2 6.Standards: Data	
T-3 6.Standards: Privacy	
T-4 6.Standards: Interoperability	

Figure 25-76: Retail: Other Desk Research: Single Technology Classifications

25.2.10.3. Interviews

Interviews were conducted with an organization to gather IoT adoption trends and issues. Figure 25-77 below lists the interviewee.

	Company Name	Type of Company
1	RSR C	Retail consulting

© Strategy of Things, 2025. All rights reserved.

Figure 25-77: Retail: Stakeholder Interviews

The interviews identified six areas that could delay the use and benefits of IoT services. Close to verbatim excerpts from the interviews along with a technical allocation for each set of comments are shown below in Figure 25-78.

ID	Single technology	Verbatim interviewee comment
1	A-3 4.Apps: Data Manage	"RFID throws off lots of signals. Most of them aren't important. Some of them are very important. And which ones do you want to keep and which ones you want to toss."
2	A-4 4.Apps: Data Analytics	"they talk about once you're collecting all this information that all these various points along the travel, you'll be able to do smarter and more intelligent things."
3	Y-2 5.Systems: Alerts	"So you can always see that in sales, sales analysis, but they don't know where their inventory is in real time."
4	Y-3 5.Systems: Security	"The secure data security issue is a really big one"
5	Y-4: Systems: AI	"…from the technology perspective, the big innovation in the last several years, five or six years has been AI."
6	T-4 6.Standards: Interoperability	"And if you let commercial enterprises develop so called standards, you'll have a variety of standards to choose from."

Figure 25-78: Retail: Stakeholder Interviews: Single Technology Classifications

Figure 25-79 below tabulates these results.

© Strategy of Things, 2025. All rights reserved.

H-1 1.Hardware: IoT Sensors	
H-2 1.Hardware: Actuators	
H-3 1.Hardware: Processing	
H-4 1.Hardware: Edge devices	
S-1 2.Software: Sensor F/ware	
S-2 2.Software: Edge F/ware	
S-3 2.Software: Data Collect	
S-4 2.Software: Data Store	
N-1 3.Networks: Gateways	
N-2 3.Networks: Connect	
A-1 4.Apps: Device manage	
A-2 4.Apps: Network manage	
A-3 4.Apps: Data Manage	
A-4 4.Apps: Data Analytics	
A-5 4 Apps: Data Visual	
A-6 4. Apps: Usability	
Y-1 5.Systems: Middleware	
Y-2 5.Systems: Alerts	
Y-3 5.Systems: Security	
Y-4 5.Systems: AI	
Y-5 5.Systems: Resiliency	
T-1 6.Standards: Security	
T-2 6.Standards: Data	
T-3 6.Standards: Privacy	
T-4 6.Standards: Interoperability	

Figure 25-79: Retail: Stakeholder Interviews: Single Technology Classifications

25.2.10.4. Ranking technology infrastructure gaps

Figure 25-80 overleaf shows the integration of use cases, survey, interview and desk research to produce a ranking of the single technologies required to operationalize the most important use cases.

© Strategy of Things, 2025. All rights reserved.

			Desk (Use case)	Desk (Industry)	Interviews	Total	Include	Survey	Adjusted	Normalized
H-1	**Hardware**	IoT Sensors	1			1		9.5%	9.5%	8.5%
H-2		Actuators						5.4%	5.4%	4.9%
H-3		Processing						10.8%	10.8%	9.7%
H-4		Edge Devices						8.1%	8.1%	7.3%
S-1	**Software**	Sensor Firmware						6.8%	6.8%	6.1%
S-2		Edge Firmware/OS						2.7%	2.7%	2.4%
S-3		Data Collection/Ingestion						5.4%	5.4%	4.9%
S-4		Data Storage						4.1%	4.1%	3.6%
N-1	**Networking**	Gateways								0.0%
N-2		Connectivity								0.0%
A-1	**Applications**	Device Management								0.0%
A-2		Network Management	1			1				0.0%
A-3		Data Management	1	1	1	3	✓		5.6%	5.0%
A-4		Data Analytics	1		1	2	✓		5.6%	5.0%
A-5		Data Visualization								0.0%
A-6		User Interaction/Usability								0.0%
Y-1	**Systems**	Middleware/Integration						4.1%	4.1%	3.6%
Y-2		Alerts and Notifications			1	1		2.7%	2.7%	2.4%
Y-3		Security Management			1	1		8.1%	8.1%	7.3%
Y-4		Artificial Intelligence			1	1		4.1%	4.1%	3.6%
Y-5		System Resiliency						5.4%	5.4%	4.9%
T-1	**Standards**	Security						4.1%	4.1%	3.6%
T-2		Data						4.1%	4.1%	3.6%
T-3		Privacy		1		1		4.1%	4.1%	3.6%
T-4		Interoperability			1	1		10.8%	10.8%	9.7%
								100%	**111%**	**100%**

Figure 25-80: Retail: Interview, Desk Research and Survey Technical Results

© Strategy of Things, 2025. All rights reserved.

Figure 25-81 below shows the survey results of the role of the private and public sectors in undertaking research and development to operationalize the use cases.

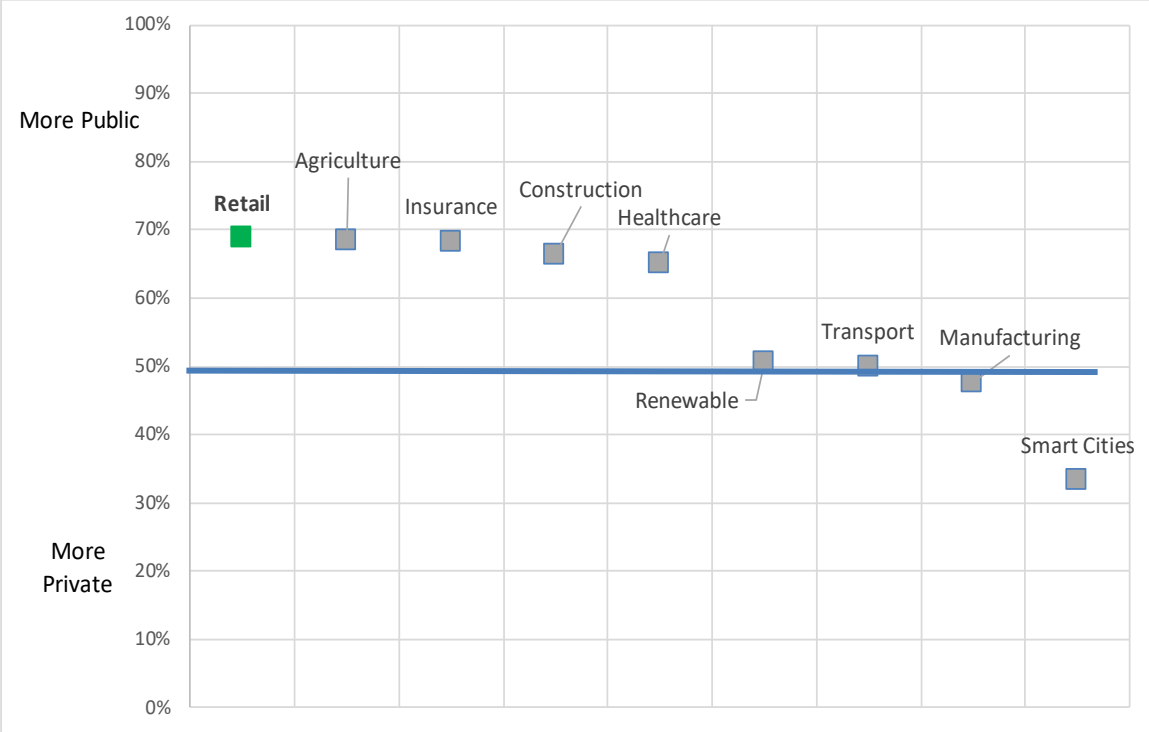


Figure 25-81: Retail: Role of the Public Sector in R&D

Figure 25-82 below shows the relative weightings for retail of the top 10 single technologies. This figure is based on an IoT value share of 8%[1746] for retail and a public contribution of 69% multiplied by the adjusted weighting shown in Figure 25-80.

Rank	Technology	Weighting	Percentage
1	T-4 Standards: Interoperability	0.00545	14%
2	H-3 Hardware: Processing	0.00545	14%
3	H-1 Hardware: IoT Sensors	0.00477	12%
4	Y-3 Systems: Security	0.00409	11%
5	H-4 Hardware: Edge devices	0.00409	11%
6	S-1 Software: Sensor F/ware	0.00341	9%
7	A-4 Apps: Data analytics	0.00281	7%
8	A-3 Apps: Data manage	0.00281	7%
9	Y-5 Systems: Resiliency	0.00273	7%
10	S-3 Software: Data collect	0.00273	7%

[1746] See Figure 25-3

© Strategy of Things, 2025. All rights reserved.

Figure 25-82: Retail: Most Important Single Technology Weightings

25.2.11. Renewable Energy

The section covers:

- Industry desk research for use cases
- Other industry desk research
- Interviews
- Summary rankings

25.2.11.1. Industry desk research for use cases

Figure 21-1 provided a set of the representative use cases for renewable energy. This section provides the technical assessments for each use case group. Issues identified in the desk research were mapped to the taxonomy in Figure 11-4 using the table structure described in Figure 25-5.

Figure 25-83 below shows the single technology component classifications of each of the use cases from desk research.

© Strategy of Things, 2025. All rights reserved.

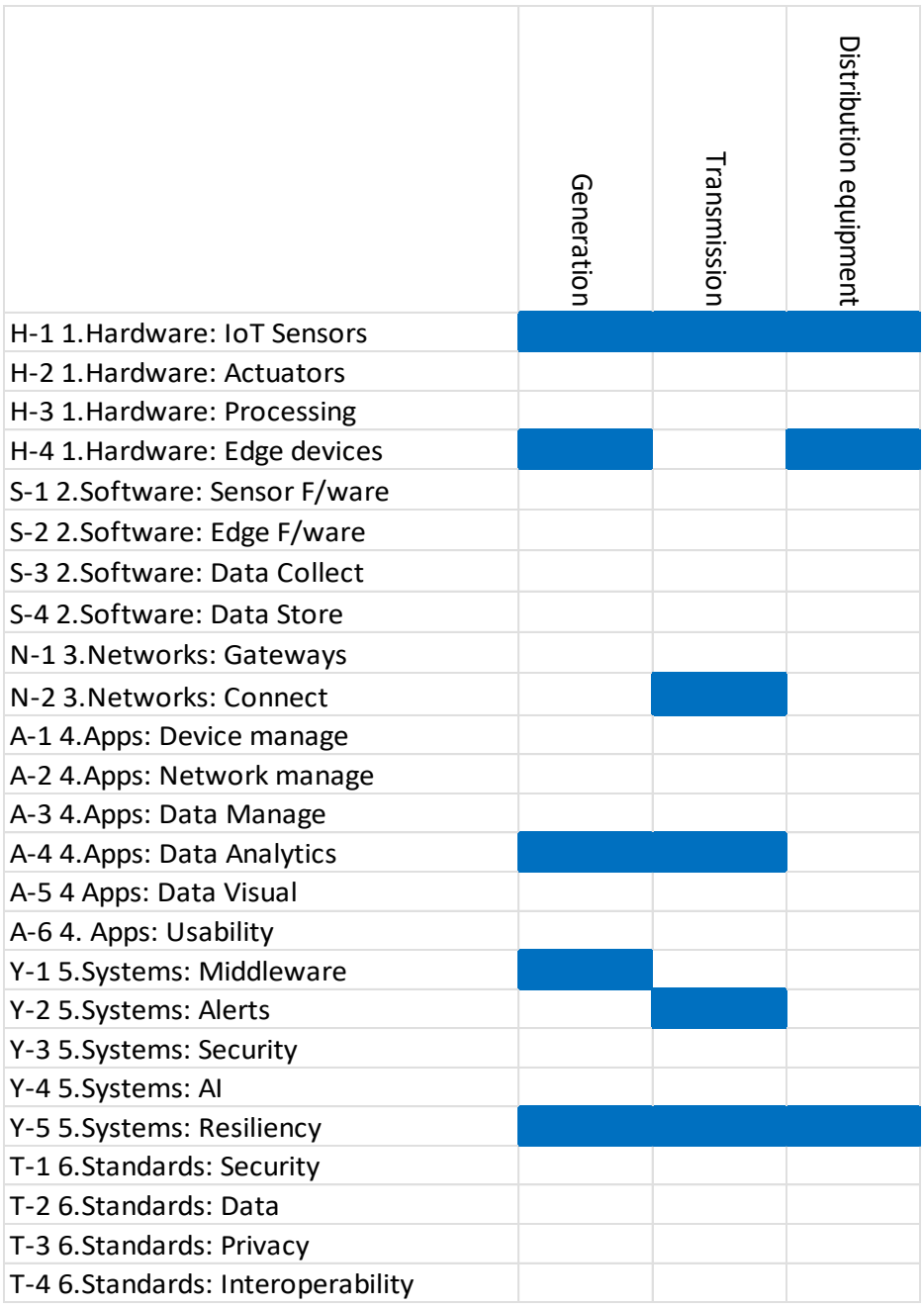


Figure 25-83: Renewable Energy: Use Cases: Single Technology Classifications

25.2.11.2. Other industry desk research

In addition to the above use cases, desk research identified an additional seven single technology component issues that could delay the use and benefits of IoT services. These are listed in detail below in Figure 25-84.

© Strategy of Things, 2025. All rights reserved.

ID	Single technology	Comment
1	H-1 1.Hardware: IoT Sensors	Manage renewable and non-renewable resource. The collection and transmission of massive amount of performance and environmental data remotely helping organizations make evidence-based decisions when outages occur
2	H-4 1.Hardware: Edge devices	Edge computing devices manage distributed energy resources such as electric vehicles, home batteries, solar panels and wind farms to enhance power grid resiliency and accelerate the energy transition. They help process data to be compressed, reduced and transmitted efficiently and support local decision-making
3	N-1 3.Networks: Gateways	Help in practical coordination of network infrastructure to bolster the state's energy resilience.
4	A-4 4.Apps: Data Analytics	Optimize and improve processes, making contributions to day-to-day operations, balance electricity supply and demand needs in real-time, optimize energy use and storage to reduce rates.
5	Y-3 5.Systems: Security	Respond and remain stable when unexpected events occur
6	Y-4 5.Systems: AI	Role in modeling, analysis and prediction of the performance
7	Y-5 5.Systems: Resiliency	Limiting the scope and impact of outages

Figure 25-84: Renewable Energy: Other Desk Research: Single Technology Classifications

Figure 25-85 below summarizes these results.

© Strategy of Things, 2025. All rights reserved.

H-1 1.Hardware: IoT Sensors	
H-2 1.Hardware: Actuators	
H-3 1.Hardware: Processing	
H-4 1.Hardware: Edge devices	
S-1 2.Software: Sensor F/ware	
S-2 2.Software: Edge F/ware	
S-3 2.Software: Data Collect	
S-4 2.Software: Data Store	
N-1 3.Networks: Gateways	
N-2 3.Networks: Connect	
A-1 4.Apps: Device manage	
A-2 4.Apps: Network manage	
A-3 4.Apps: Data Manage	
A-4 4.Apps: Data Analytics	
A-5 4 Apps: Data Visual	
A-6 4. Apps: Usability	
Y-1 5.Systems: Middleware	
Y-2 5.Systems: Alerts	
Y-3 5.Systems: Security	
Y-4 5.Systems: AI	
Y-5 5.Systems: Resiliency	
T-1 6.Standards: Security	
T-2 6.Standards: Data	
T-3 6.Standards: Privacy	
T-4 6.Standards: Interoperability	

Figure 25-85: Renewable Energy: Other Desk Research: Single Technology Classifications

25.2.11.3. Interviews

Interviews were conducted with four organizations to gather IoT adoption trends and issues. Figure 25-86 below lists the interviewees.

	Company Name	Type of Company
1	naak.io	Energy cloud services
2	e-peas	Energy harvesting
3	End phase energy	Energy management technology
4	Mayor of City of Fort Wayne	Public sector

© Strategy of Things, 2025. All rights reserved.

Figure 25-86: Renewable Energy: Stakeholder Interviews

The interviews identified five areas that could delay the use and benefits of IoT services. Close to verbatim excerpts from the interviews along with a technical allocation for each set of comments are shown below in Figure 25-87.

ID	Single technology	Verbatim interviewee comment
1	H-1 1.Hardware: IoT Sensors	"The industry is nascent, but some do have an appetite to constantly challenge and adopt state of the art…however this is not a commodity product yet, until it becomes like a lightbulb you still have to monitor it."
2	S-2 2.Software: Edge F/ware	"Address in real time. Respond at the embedded device level... Need a local brain at the edge to make the decision."
3	N-2 3.Networks: Connect	"Come up with more robust and reliable connectivity options besides Zigbee."
5	T-4 6.Standards: Interoperability	"… these machines are a mix of old and new, cannot just plug ethernet into them, need understanding the connectivity requirements of each machine."

Figure 25-87: Renewable Energy: Stakeholder Interviews: Single Technology Classifications

Figure 25-88 below summarizes these results.

© Strategy of Things, 2025. All rights reserved.

H-1 1.Hardware: IoT Sensors	
H-2 1.Hardware: Actuators	
H-3 1.Hardware: Processing	
H-4 1.Hardware: Edge devices	
S-1 2.Software: Sensor F/ware	
S-2 2.Software: Edge F/ware	
S-3 2.Software: Data Collect	
S-4 2.Software: Data Store	
N-1 3.Networks: Gateways	
N-2 3.Networks: Connect	
A-1 4.Apps: Device manage	
A-2 4.Apps: Network manage	
A-3 4.Apps: Data Manage	
A-4 4.Apps: Data Analytics	
A-5 4 Apps: Data Visual	
A-6 4. Apps: Usability	
Y-1 5.Systems: Middleware	
Y-2 5.Systems: Alerts	
Y-3 5.Systems: Security	
Y-4 5.Systems: AI	
Y-5 5.Systems: Resiliency	
T-1 6.Standards: Security	
T-2 6.Standards: Data	
T-3 6.Standards: Privacy	
T-4 6.Standards: Interoperability	

Figure 25-88: Renewable Energy: Stakeholder Interviews: Single Technology Classifications

25.2.11.4. Ranking technology infrastructure gaps

Figure 25-89 overleaf shows the integration of use cases, survey, interview and desk research to produce a ranking of the single technologies required to operationalize the most important use cases.

© Strategy of Things, 2025. All rights reserved.

			Desk (Use case)	Desk (Industry)	Interviews	Total	Include	Survey	Adjusted	Normalized
H-1	**Hardware**	IoT Sensors	1	1	1	3	✓	4.3%	11.1%	8.7%
H-2		Actuators						4.3%	4.3%	3.4%
H-3		Processing						8.7%	8.7%	6.8%
H-4		Edge Devices	1	1		2	✓	8.7%	16.6%	12.9%
S-1	**Software**	Sensor Firmware						4.3%	4.3%	3.4%
S-2		Edge Firmware/OS			1	1		4.3%	4.3%	3.4%
S-3		Data Collection/Ingestion						4.3%	4.3%	3.4%
S-4		Data Storage						4.3%	4.3%	3.4%
N-1	**Networking**	Gateways		1		1				0.0%
N-2		Connectivity			1	1				0.0%
A-1	**Applications**	Device Management								0.0%
A-2		Network Management								0.0%
A-3		Data Management								0.0%
A-4		Data Analytics	1	1		2	✓		5.7%	4.4%
A-5		Data Visualization								0.0%
A-6		User Interaction/Usability								0.0%
Y-1	**Systems**	Middleware/Integration						4.3%	4.3%	3.4%
Y-2		Alerts and Notifications						4.3%	4.3%	3.4%
Y-3		Security Management		1		1		8.7%	8.7%	6.8%
Y-4		Artificial Intelligence		1		1		8.7%	8.7%	6.8%
Y-5		System Resiliency	1	1		2	✓	8.7%	16.6%	12.9%
T-1	**Standards**	Security						4.3%	4.3%	3.4%
T-2		Data						4.3%	4.3%	3.4%
T-3		Privacy						4.3%	4.3%	3.4%
T-4		Interoperability			1	1		8.7%	8.7%	6.8%
								100%	**128%**	**100%**

Figure 25-89: Renewable Energy: Interview, Desk Research and Survey Technical Results

© Strategy of Things, 2025. All rights reserved.

Figure 25-90 below shows the survey results of the role of the private and public sectors in undertaking research and development to operationalize the use cases.

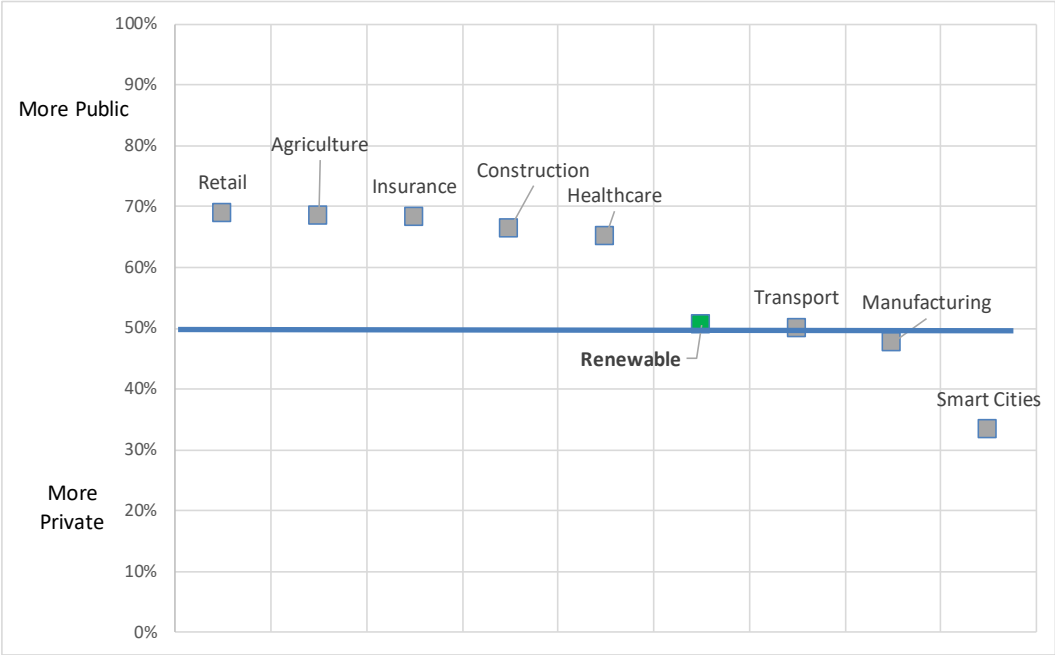


Figure 25-90: Renewable Energy: Role of the Public Sector in R&D

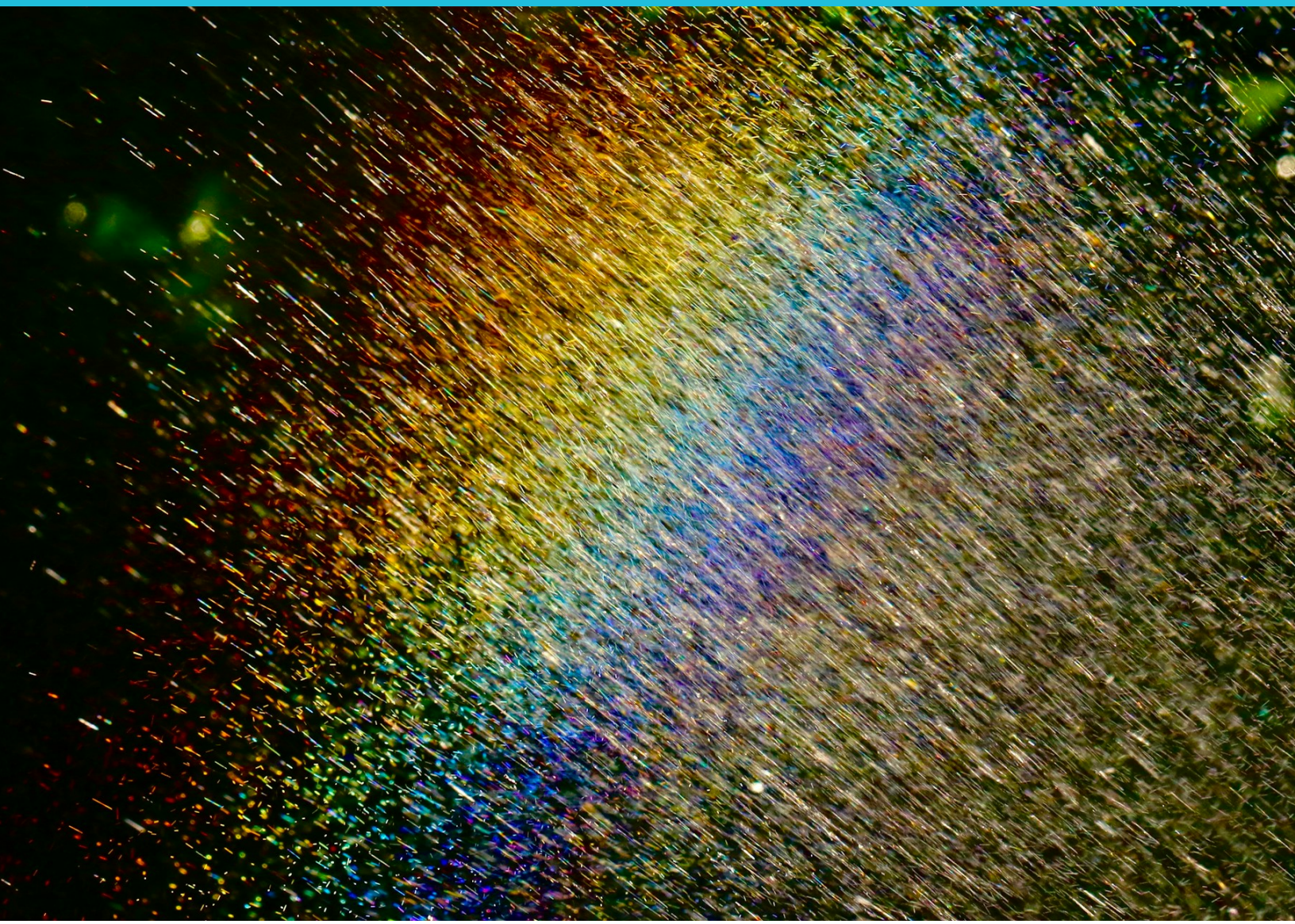
Figure 25-91 below shows the relative weightings for renewable energy of the top 10 single technologies. This figure is based on an IoT value share of 1%[1747] for renewable energy and a public contribution of 51% multiplied by the adjusted weighting shown in Figure 25-89.

Rank	Technology	Weighting	Percentage
1	H-1 Hardware: IoT Sensors	0.00906	18%
2	T-4 Standards: Interoperability	0.00820	16%
3	H-4 Hardware: Edge devices	0.00549	11%
4	Y-4 Systems: AI	0.00481	9%
5	Y-3 Systems: Security	0.00481	9%
6	S-4 Software: Data store	0.00481	9%
7	H-2 Hardware: Actuators	0.00412	8%
8	Y-5 Systems: Resiliency	0.00343	7%
9	S-3 Software: Data collect	0.00343	7%
10	H-3 Hardware: Processing	0.00343	7%

Figure 25-91: Renewable Energy: Ranking and Single Technology Weightings

[1747] See Figure 25-3

© Strategy of Things, 2025. All rights reserved.



Appendix: Qualitative and Economic Rankings

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

© Strategy of Things, 2025. All rights reserved.

26. Appendix: Qualitative and economic rankings

This appendix integrates information from all the analyses to produce two results.

- A ranking of the qualitative issues discussed in each industry section
- A ranking of the economic results for each industry adjusted by the role of the public sector.

26.1. Ranking of qualitative issues

The industry analysis provides a qualitative list of IoT related issues. These issues were grouped into broad categories and were then weighted by their economic impact and the role of the public sector. Figure 26-1 below shows the importance of each qualitative issue by industry using this weighting.[1748]

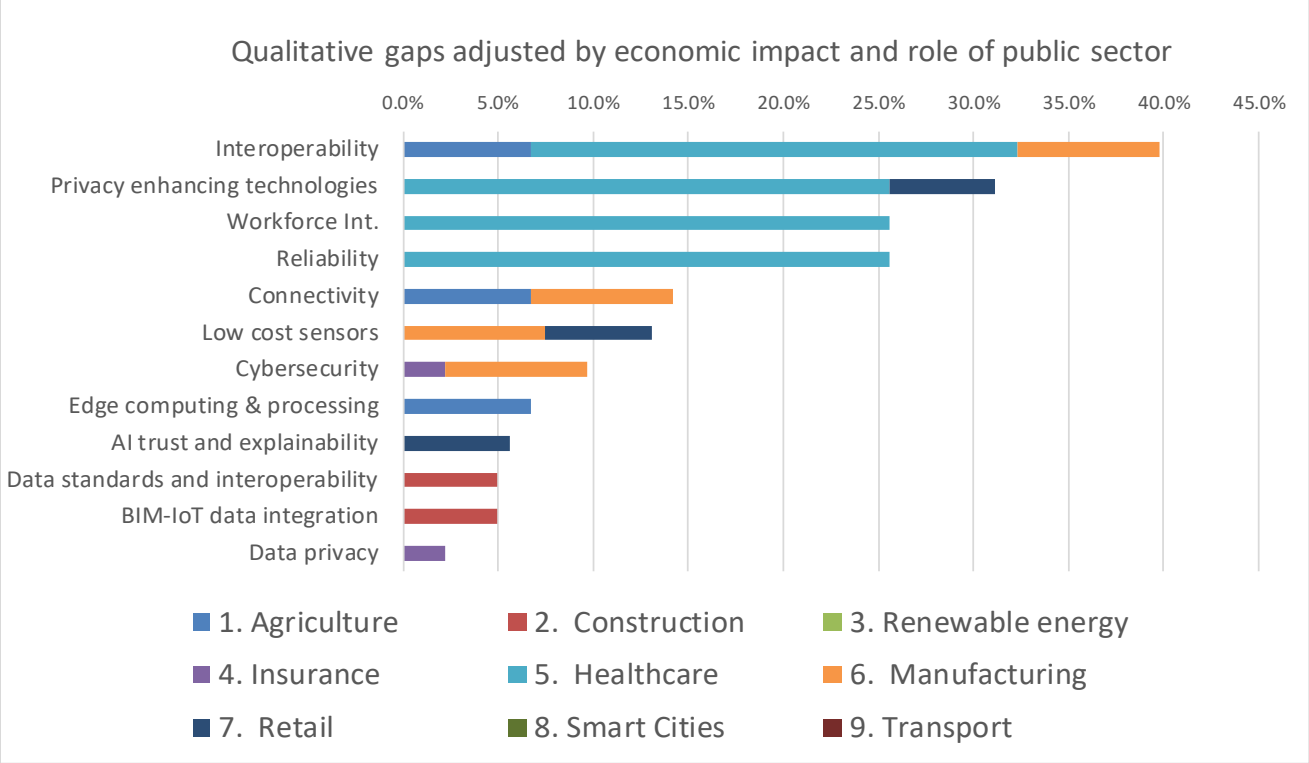


Figure 26-1: Qualitative Gap Importance by Industry

26.2. Ranking by economics and technology

[1748] For example, agriculture has an economic IoT share of 10% (See Section 25.1)and a public sector share of 68% (see Figure 25 16: Agriculture: Role of the Public Sector in R&D). This provides a value of 6.7% for each of the three gaps highlighted in the agriculture section.

© Strategy of Things, 2025. All rights reserved.

Figure 26-2 below shows the central estimates of the weightings for the top single technology components when all adjusted industry results are summed.

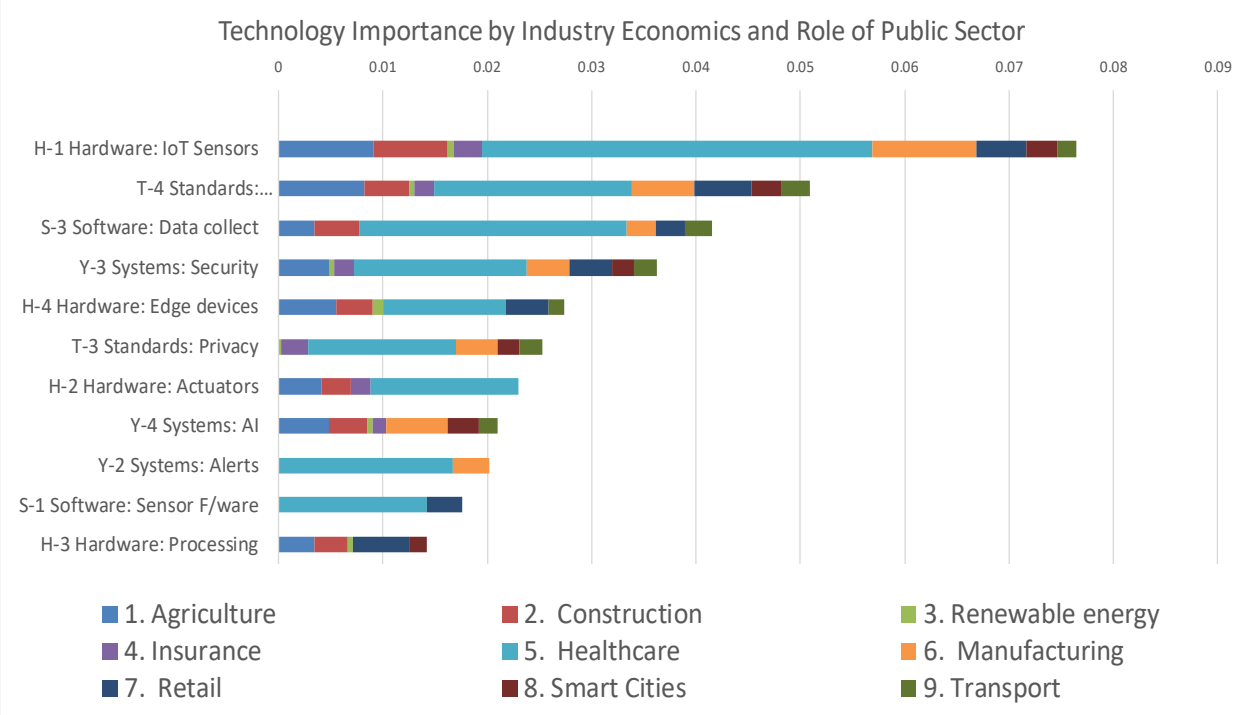


Figure 26-2: All Industries Single Technology Component Technical Rankings

26.3. Sensitivity analysis

In undertaking the economic ranking calculations, two arbitrary decisions were made to integrate the interviews and desk research with the survey results. These were:

1. The requirement for two mentions of a single technology components from the three sources for an adjustment to the survey results
2. When an adjustment was present, the survey result was scaled by 1.25 plus the average of the survey responses. This scaling and offset combination incorporated the interview and desk results even if there was a zero response in the survey[1749].

A Monte Carlo method was applied to these two assumptions along with the range estimates provided in Section 22. These three parameters were replaced with probability distributions with the following characteristics:

- The requirement for 2 mentions is replaced with a range of 1 to 3 mentions each with equal probability.

[1749] As a formula: If [two mentions] then [New Survey Value for that Single Technology Component = 1.25 * That Weighting + Average(All Weightings)]

© Strategy of Things, 2025. All rights reserved.

- The scalar ranges from 1.1 to 1.5 based on a flat probability distribution.
- The economic values are replaced with triangular probability distributions with a peak at the most likely value and zeros at either extreme.

Figure 26-3 overleaf shows the distributions.[1750] The figure shows:

- There is some overlap between T-4 and H-1. There is a likelihood that these are of equal importance and are classified as equal first.
- S-3 is sensitive to changes in the parameters as is introduced into the top 3 rankings and classified as equal third with Y-3.

This provides the following rankings for the single technology components:

- Equal first: H-1 Hardware: IoT Sensors, T-4 Standards: Interoperability
- Second: Y-3: Systems Security
- Third: S-3 Software: Data Collect

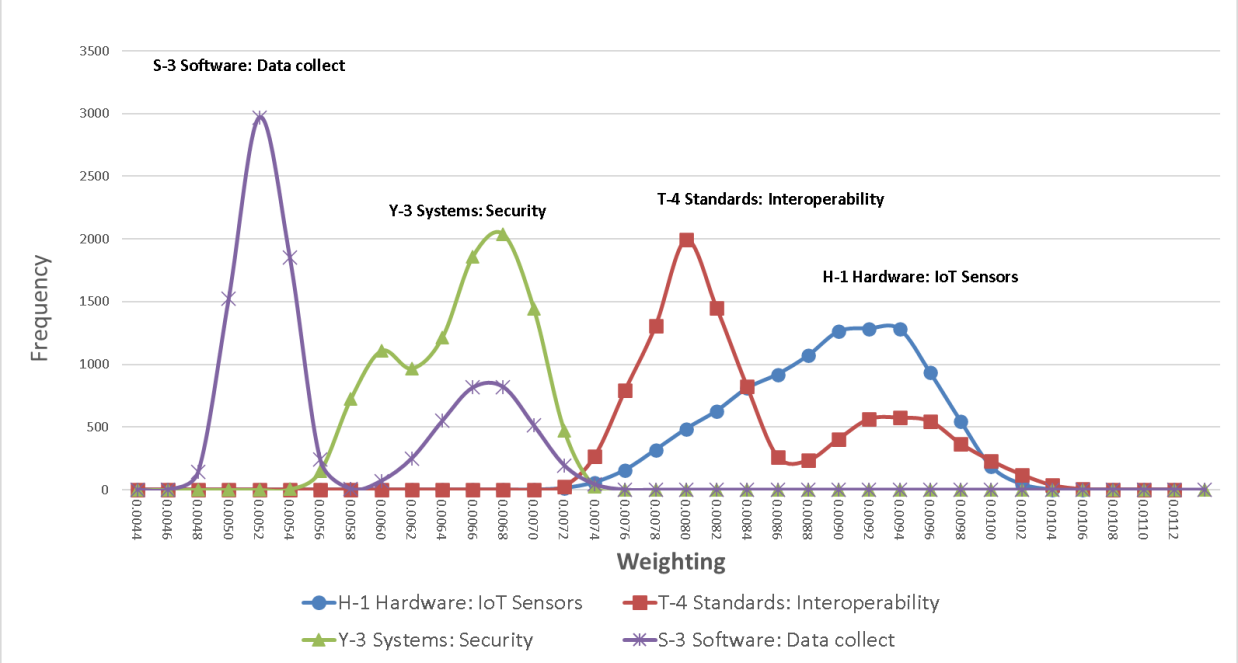


Figure 26-3: Subcategory Weighting Probability Distributions

26.4. Impact of $10 million investment in public R&D

[1750] The decision to weigh information from interviews and desk research with a step function introduces non linearities in the model. This produces bi-modal distributions for each of the technologies.

© Strategy of Things, 2025. All rights reserved.

The model results can be used to determine the economic surplus from a nominal $10 million investment[1751] in the most highly ranked IoT technologies. A figure is calculated using the following method:

- An investment of $10 million in public research for an IoT technology is allocated across industries based on the normalized calculated weightings for that technology. For each industry, these weightings have considered:
    - the importance of the technology
    - the value of IoT in the U.S. economy
    - the role of the public sector.

- This R&D investment in the single technology will lead to a revenue based on the historical ratio of R&D spend to revenue for that industry.
- This revenue will lead to a surplus based on the historical gross margin in that industry[1752].

The remainder of this appendix provides these calculations for the four selected single technologies and the gaps identified in the core and intelligence categories. These calculations should be seen as directional and used to illustrate the concept given the uncertainty associated with the inputs.

26.4.1. R&D to revenue

Figure 26-4 below provides detailed information on the ratio of R&D to revenue by selected industry.[1753] The model uses high, medium and low classifications to estimate the revenue obtained from investment in R&D. These values are at the 66th, 50th and 33rd percentiles, respectively.

[1751] The nominal $10 million is considered as the value of a combination of different government initiatives and support.

[1752] As a formula: Surplus = ($ 10 million * Weighting) / R&D to revenue ratio) * Gross Margin

[1753] "R&D Spending as a Percentage of Revenue by Industry [S&P500.]" Link

© Strategy of Things, 2025. All rights reserved.

Industry	R&D to revenue
Aerospace & Defense	0.5.%
Automobiles	1.6.%
Biotechnology	30.3.%
Capital Markets	0.5.%
Chemicals	2.4.%
Communications Equipment	16.7.%
Electrical Equipment	0.8.%
Electronic Equipment, Instruments & Compon	8.8.%
Energy Equipment & Services	0.6.%
Entertainment	9.9.%
Equity Real Estate Investment Trusts (REITs)	0.0.%
Food Products	0.1.%
Health Care Equipment & Supplies	7.4.%
Health Care Providers & Services	0.0.%
Health Care Technology	13.6.%
Hotels, Restaurants & Leisure	0.0.%
Household Durables	1.9.%
Household Products	0.4.%
Independent Power and Renewable Electricity	0.0.%
Industrial Conglomerates	2.3.%
Interactive Media & Services	18.8.%
Internet & Direct Marketing Retail	11.2.%
IT Services	1.5.%
Leisure Products	4.7.%
Life Sciences Tools & Services	7.4.%
Machinery	1.8.%
Metals & Mining	0.4.%
Pharmaceuticals	15.2.%
Semiconductors & Semiconductor Equipment	16.7.%
Software	19.0.%
Technology Hardware, Storage & Peripherals	8.5.%

Figure 26-4: Detailed R&D to Revenue by Industry

Rank	Assement	Value
66th percentile	High	8.3%
50th percentile	Medium	2.3%
33rd percentile	Low	0.8%

© Strategy of Things, 2025. All rights reserved.

Figure 26-5: High, Medium and Low R&D to Revenue Percentages

Figure 26-6 below applies these ratios to each of the analyzed industries.

Industry	R&D to revenue	Value
1.Agriculture	Low	0.8%
2.Construction	Low	0.8%
3.Renewable energy	Low	0.8%
4.Insurance	Low	0.8%
5.Healthcare	High	8.3%
6.Manufacturing	Medium	2.3%
7.Retail	Low	0.8%
8.Smart Cities	Medium	2.3%
9.Transport	Medium	2.3%

Figure 26-6: R&D to Revenue by Industry

26.4.2. Gross margins

Figure 26-7 below shows the mean gross margin on sales for the selected industries.

Industry	Gross Margin
1. Agriculture	14%
2. Construction	23%
3. Renewable energy	40%
4. Insurance	31%
5. Healthcare	52%
6. Manufacturing	35%
7. Retail	24%
8.Smart Cities	29%
9. Transport	21%

© Strategy of Things, 2025. All rights reserved.

Figure 26-7: Gross Margin by Industry[1754]

Gross margins were available for 94 economic activities. These activities were assigned to one of the nine industries and the standard deviation of those selected activities was calculated. Three standard deviations were used to produce the gross margin variance for the Monte Carlo analysis that provided a range estimate.

This produced the following central estimates and ranges for the surplus from a $10 million public sector investment.

[1754] "Margins by Sector (US)", NYU Stern School of Business, January 2023. Link

© Strategy of Things, 2025. All rights reserved.

26.4.3. Surplus estimates by single technology component

Figure 26-8 applies these ratios to a nominal $10 million investment spread across each industry based on the calculated weightings. For example, healthcare receives a majority of the $10 million investment as it received the highest weighting of all the industries, representing around 49% of the total.

This investment leads to an estimate of the surplus generated by the most important technology. This shows a long term associated surplus of $143 million.

Industry	H-1 Hardware: IoT Sensors Weighting	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
5. Healthcare	0.037467	$4.90	8.3%	$59	52%	$31
6. Manufacturing	0.009951	$1.30	2.3%	$57	35%	$20
1. Agriculture	0.009056	$1.18	0.8%	$152	14%	$21
2. Construction	0.007115	$0.93	0.8%	$119	23%	$27
7. Retail	0.004772	$0.62	0.8%	$80	24%	$19
8. Smart Cities	0.002978	$0.39	2.3%	$17	29%	$5
4. Insurance	0.002649	$0.35	0.8%	$44	31%	$14
10. Transport	0.001849	$0.24	2.3%	$11	21%	$2
3. Renewable energy	0.000623	$0.08	0.8%	$10	40%	$4
		$10.0		**$549**		**$143**

© Strategy of Things, 2025. All rights reserved.

Figure 26-8: Economic Surplus from a Nominal $10 million Investment in H-1 Hardware: IoT Sensors

Similarly, Figure 26-9 below shows the impact of allocating the investment in the equal first most important technology. This shows a long term associated surplus of $106 million.

Industry	T-4 Standards: Interoperability Weighting	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
5. Healthcare	0.018956	$2.48	8.3%	$30	52%	$16
1. Agriculture	0.008197	$1.07	0.8%	$137	14%	$19
6. Manufacturing	0.005940	$0.78	2.3%	$34	35%	$12
7. Retail	0.005454	$0.71	0.8%	$91	24%	$22
2. Construction	0.004318	$0.56	0.8%	$72	23%	$16
8. Smart Cities	0.002978	$0.39	2.3%	$17	29%	$5
10. Transport	0.002659	$0.35	2.3%	$15	21%	$3
4. Insurance	0.001926	$0.25	0.8%	$32	31%	$10
3. Renewable energy	0.000486	$0.06	0.8%	$8	40%	$3
		$10.0		**$438**		**$106**

Figure 26-9: Economic Surplus from a Nominal $10 million Investment in T-4 Standards: Interoperability

Figure 26-10 below shows the impact of the investment in the third most important technology. This shows a long term associated surplus of $72 million.

© Strategy of Things, 2025. All rights reserved.

Industry	S-3 Software: Data collect Weighting	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
5. Healthcare	0.025620	$3.35	8.3%	$40	52%	$21
2. Construction	0.004318	$0.56	0.8%	$72	23%	$16
1. Agriculture	0.003433	$0.45	0.8%	$58	14%	$8
6. Manufacturing	0.002807	$0.37	2.3%	$16	35%	$6
7. Retail	0.002727	$0.36	0.8%	$46	24%	$11
10. Transport	0.002589	$0.34	2.3%	$15	21%	$3
8. Smart Cities	0.001276	$0.17	2.3%	$7	29%	$2
4. Insurance	0.000642	$0.08	0.8%	$11	31%	$3
3. Renewable energy	0.000243	$0.03	0.8%	$4	40%	$2
		$10.0		**$269**		**$72**

Figure 26-10: Economic Surplus from a Nominal $10 million Investment in S-3 Software: Data collect

© Strategy of Things, 2025. All rights reserved.

Figure 26-11 below shows the impact of the investment in the remaining fourth most important technology. This shows a long term associated surplus of $150 million.

Industry	Y-3 Systems: Security Weighting	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
5. Healthcare	0.016586	$4.43	8.3%	$54	52%	$28
1. Agriculture	0.004807	$1.28	0.8%	$165	14%	$22
7. Retail	0.004091	$1.09	0.8%	$140	24%	$34
6. Manufacturing	0.004010	$1.07	2.3%	$47	35%	$16
10. Transport	0.002219	$0.59	2.3%	$26	21%	$5
8. Smart Cities	0.002127	$0.57	2.3%	$25	29%	$7
4. Insurance	0.001926	$0.51	0.8%	$66	31%	$20
2. Construction	0.001178	$0.31	0.8%	$40	23%	$9
3. Renewable energy	0.000486	$0.13	0.8%	$17	40%	$7
		$10.0		**$578**		**$150**

Figure 26-11: Economic Surplus from a Nominal $10 million Investment in Y-3 Systems: Security

26.4.4. Surplus estimates by identified core and intelligence gaps

The analysis provided a set of core and intelligent gaps. Each of these gaps maps to one or more of the 25 single technologies indicated in the IoT taxonomy. The model uses the following allocations for each of the gaps:

Core Gaps:

- Interoperability: Y-1 Systems Middleware + T-4 Standards: Interoperability
- Privacy: Standards: T-3 Standards Privacy + Y-3 Systems Security + T-1 Standards Security
- Security Standards: Y-3 Systems Security + T-1 Standards Security

© Strategy of Things, 2025. All rights reserved.

- Connectivity N-1: Network Gateways + N-2: Network Connectivity + A-2 Application Network Management

Intelligence Gaps:

- Data management: A-3 Application Data Management
- Artificial intelligence: A-4 Apps: Data analytics + Y-4 Systems Artificial Intelligence
- Intelligent devices: H-3 Hardware: Processing + H-4 Hardware: Edge Devices+ H-1 Hardware IoT Sensors

Figures Figure 26-12 to Figure 26-18 below show the impact of allocating a nominal public sector investment of $10 million to each of identified gaps in core and intelligence allocated across industries. In particular:

- The model produces estimates of associated surplus ranging from $149 million to $239 million for the identified gaps.
- In cases where there has been minimal mention in the survey or desk research of a particular technology, no funds are allocated for the particular technology. This is most pronounced in Core: Connectivity where funds are allocated across only four industries.
- Healthcare with its large roles in the economy and the public sector along with a high gross margin often receives a substantial allocation of the $10 million investment.
- Data Management investments are most pronounced in the manufacturing and retail sectors.
- With the exception of Data Management, Agriculture receives investments in each of the remaining gaps.

© Strategy of Things, 2025. All rights reserved.

Core: Interoperability								
Industry	Y-1 Systems: Middleware	T-4 Standards: Interoperability	Sum	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
1. Agriculture	0.0007	0.0082	0.0089	$1.38	0.8%	$177	14%	$24
2. Construction	0.0012	0.0043	0.0055	$0.85	0.8%	$109	23%	$25
3. Renewable energy	0.0002	0.0005	0.0007	$0.11	0.8%	$15	40%	$6
4. Insurance	0.0006	0.0019	0.0026	$0.40	0.8%	$51	31%	$16
5. Healthcare	0.0047	0.0190	0.0237	$3.68	8.3%	$44	52%	$23
6. Manufacturing	0.0024	0.0059	0.0083	$1.30	2.3%	$56	35%	$20
7. Retail	0.0020	0.0055	0.0075	$1.16	0.8%	$149	24%	$36
8. Smart Cities	0.0009	0.0030	0.0038	$0.59	2.3%	$26	29%	$7
10. Transport	0.0007	0.0027	0.0034	$0.53	2.3%	$23	21%	$5
				$10.0		**$650**		**$162**

Figure 26-12: Impact of a Nominal $10 million Public Sector Investment in Core: Interoperability

Core: Privacy									
Industry	T-3 Standards: Privacy	Y-3 Systems: Security	T-1 Standards: Security	Sum	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
1. Agriculture	0.0021	0.0048	0.0014	0.0082	$0.93	0.8%	$119	14%	$16
2. Construction	0.0012	0.0012	0.0004	0.0027	$0.31	0.8%	$40	23%	$9
3. Renewable energy	0.0002	0.0005	0.0002	0.0010	$0.11	0.8%	$14	40%	$6
4. Insurance	0.0026	0.0019	0.0013	0.0058	$0.65	0.8%	$83	31%	$26
5. Healthcare	0.0142	0.0166	0.0071	0.0379	$4.27	8.3%	$52	52%	$27
6. Manufacturing	0.0039	0.0040	0.0032	0.0112	$1.26	2.3%	$55	35%	$19
7. Retail	0.0020	0.0041	0.0020	0.0082	$0.92	0.8%	$118	24%	$29
8. Smart Cities	0.0021	0.0021	0.0026	0.0068	$0.77	2.3%	$33	29%	$10
10. Transport	0.0022	0.0022	0.0027	0.0071	$0.80	2.3%	$35	21%	$7
					$10.0		**$548**		**$149**

Figure 26-13: Impact of a Nominal $10 million Public Sector Investment in Core: Privacy

© Strategy of Things, 2025. All rights reserved.

Core: Security								
Industry	T-1 Standards: Security	Y-3 Systems: Security	Sum	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
1. Agriculture	0.0014	0.0048	0.0062	$1.06	0.8%	$136	14%	$18
2. Construction	0.0004	0.0012	0.0016	$0.27	0.8%	$35	23%	$8
3. Renewable energy	0.0002	0.0005	0.0007	$0.13	0.8%	$16	40%	$6
4. Insurance	0.0013	0.0019	0.0032	$0.55	0.8%	$71	31%	$22
5. Healthcare	0.0071	0.0166	0.0237	$4.06	8.3%	$49	52%	$26
6. Manufacturing	0.0032	0.0040	0.0072	$1.24	2.3%	$54	35%	$19
7. Retail	0.0020	0.0041	0.0061	$1.05	0.8%	$135	24%	$33
8. Smart Cities	0.0026	0.0021	0.0047	$0.80	2.3%	$35	29%	$10
10. Transport	0.0027	0.0022	0.0049	$0.84	2.3%	$36	21%	$8
				$10.0		**$566**		**$150**

Figure 26-14: Impact of a Nominal $10 million Public Sector Investment in Core: Security

Core: Connectivity									
Industry	A-2 Apps: Network Mngt	N-2 Network: Connectivity	N-1 Network: Gateways	Sum	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
1. Agriculture		0.0030		0.0030	$3.40	0.8%	$436	14%	$59
2. Construction					$0.00	0.8%	$0	23%	$0
3. Renewable energy					$0.00	0.8%	$0	40%	$0
4. Insurance		0.0010		0.0010	$1.17	0.8%	$149	31%	$46
5. Healthcare					$0.00	8.3%	$0	52%	$0
6. Manufacturing	0.0024	0.0024		0.0049	$5.43	2.3%	$236	35%	$84
7. Retail					$0.00	0.8%	$0	24%	$0
8. Smart Cities					$0.00	2.3%	$0	29%	$0
10. Transport					$0.00	2.3%	$0	21%	$0
					$10.0		**$822**		**$189**

Figure 26-15: Impact of a Nominal $10 million Public Sector Investment in Core: Connectivity

© Strategy of Things, 2025. All rights reserved.

Intelligence: Data Management							
Industry	A-3 Apps: Data manage	Sum	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
1. Agriculture			$0.00	0.8%	$0	14%	$0
2. Construction			$0.00	0.8%	$0	23%	$0
3. Renewable energy			$0.00	0.8%	$0	40%	$0
4. Insurance			$0.00	0.8%	$0	31%	$0
5. Healthcare			$0.00	8.3%	$0	52%	$0
6. Manufacturing	0.0024	0.0024	$4.64	2.3%	$202	35%	$71
7. Retail	0.0028	0.0028	$5.36	0.8%	$688	24%	$167
8. Smart Cities			$0.00	2.3%	$0	29%	$0
10. Transport			$0.00	2.3%	$0	21%	$0
			$10.0		**$889**		**$239**

Figure 26-16: Impact of a Nominal $10 million Public Sector Investment in Intelligence: Data Management

Intelligence: Artificial Intelligence								
Industry	A-4 Apps: Data analytics	Y-4 Systems: AI	Sum	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
1. Agriculture	0.0030	0.0048	0.0079	$1.44	0.8%	$185	14%	$25
2. Construction	0.0022	0.0037	0.0059	$1.08	0.8%	$139	23%	$32
3. Renewable energy	0.0003	0.0005	0.0008	$0.15	0.8%	$19	40%	$8
4. Insurance	0.0010	0.0013	0.0023	$0.43	0.8%	$55	31%	$17
5. Healthcare	0.0108	0.0071	0.0179	$3.29	8.3%	$40	52%	$21
6. Manufacturing	0.0024	0.0059	0.0084	$1.54	2.3%	$67	35%	$24
7. Retail	0.0028	0.0020	0.0049	$0.89	0.8%	$114	24%	$28
8. Smart Cities	0.0016	0.0030	0.0045	$0.84	2.3%	$36	29%	$11
10. Transport		0.0018	0.0018	$0.34	2.3%	$15	21%	$3
				$10.0		**$670**		**$167**

Figure 26-17: Impact of a Nominal $10 million Public Sector Investment in Intelligence: Artificial Intelligence

© Strategy of Things, 2025. All rights reserved.

Intelligence: Intelligent Devices									
Industry	H-3 Hardware: Processing	H-4 Hardware: Edge devices	H-1 Hardware: IoT Sensors	Sum	Public R&D investment ($m)	R&D to Revenue	Revenue ($m)	Gross margin	Surplus from Revenue ($m)
1. Agriculture	0.0034	0.0055	0.0091	0.0180	$1.34	0.8%	$171	14%	$23
2. Construction	0.0031	0.0035	0.0071	0.0138	$1.03	0.8%	$131	23%	$30
3. Renewable energy	0.0005	0.0009	0.0006	0.0020	$0.15	0.8%	$19	40%	$8
4. Insurance	0.0006	0.0006	0.0026	0.0039	$0.29	0.8%	$38	31%	$12
5. Healthcare	0.0095	0.0118	0.0375	0.0588	$4.37	8.3%	$53	52%	$28
6. Manufacturing	0.0024	0.0020	0.0100	0.0144	$1.07	2.3%	$46	35%	$16
7. Retail	0.0055	0.0041	0.0048	0.0143	$1.06	0.8%	$137	24%	$33
8. Smart Cities	0.0017	0.0009	0.0030	0.0055	$0.41	2.3%	$18	29%	$5
10. Transport	0.0004	0.0015	0.0018	0.0037	$0.28	2.3%	$12	21%	$3
					$10.0		**$626**		**$158**

Figure 26-18: Impact of a Nominal $10 million Public Sector Investment in Intelligence: Intelligent Devices

© Strategy of Things, 2025. All rights reserved.

Appendix: Acronyms and Initialisms

Economic Research and Analysis of the National Need for Technology Infrastructure to Support the Internet of Things (IoT)

© Strategy of Things, 2025. All rights reserved.

27. Appendix: Acronyms and Initialisms

Acronym	Description
ADAPT	Open-source project/toolkit by AgGateway
BIM	Building Information Modeling
CAD	Computer-aided Design
CAGR	Compound Annual Growth Rate
CAN	Controller Area Network
CESMII	Clean Energy Smart Manufacturing Innovation Institute
CHIPS	CHIPS for America Act (Legislation)
COVID	COVID-19
DDOS	Distributed Denial of Service
EBIT	Earnings Before Interest and Taxes
GEO	Geosynchronous Earth Orbit
HVAC	Heating, Ventilation and Air Conditioning
LEED	Leadership in Energy and Environmental Design
LEO	Low Earth Orbit
LIDAR	Light Detection and Ranging
LoRaWAN	Long Range Wide Area Network
LPWAN	Low Power Wide Area Network
MAGNET	Manufacturing Advocacy and Growth Network (Company)
MEC	Multi-access Edge Computing
NEOM	NEOM Smart City Project in Saudi Arabia
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency or Internal Report
NUGU	Artificial Intellgiance service by SK Telecom
OATS	Open Ag Technology and Systems
PICMG	PCI Industrial Computer Manufacturers Group
REST	REpresentational State Transfer

© Strategy of Things, 2025. All rights reserved.

Acronym	Description
SCADA	Supervisory Control and Data Acquisition
SIM	Subscriber Identity Module
STEM	Science, Technology, Engineering and Mathematics
WIP	Work in Progress

© Strategy of Things, 2025. All rights reserved.

Initialism	Description
AFBF	American Farm Bureau Federation
AGV	Automated Guided Vehicles
AI	Artificial Intelligence
AIOTA	AIOTA Solutions (Company)
API	Application Programming Interface
AQ	Air Quality
AR	Augmented Reality
AWS	Amazon Web Services
AZ	Arizona
BIL	Bipartisan Infrastructure Law
BLE	Bluetooth Low Energy
BLS	Bureau of Labor Statistics
BLX	BLX.io (Company)
CA	California
CBRS	Citizens Band Radio Service
CCPA	California Consumer Protection Act
CM	China Mobile
CME	CME Group (Company)
CoAP	Constrained Application Protocol
CTIA	Cellular Telecommunications Industry Association
CTO	Chief Technology Officer
DC	District of Columbia
DCS	Distributed Control Systems
DDS	Data Distribution Service
DE	Delaware
DT	Deutsche Telekom
DX	Digital Transformation

© Strategy of Things, 2025. All rights reserved.

Initialism	Description
ERP	Enterprise Resource Planning
ESS	Energy Storage System
ETA	Estimated Time of Arrival
ETL	Extract, Transform, Load
EU	European Union
FCC	Federal Communications Commission
FI	FI-PPP (Future Internet Public Private Partnership)
FL	Florida
FNOL	First Notice of Loss
GA	Georgia
GC	General Contractor
GCFI	Gross Cash Farm Income
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation`
GPS	Global Positioning System
GSA	Government Services Administration
HB	HB 2395 (legislation)
HSB	HSB Canada (Company)
HPC	High Performance Computing
HTTP	Hypertext Transfer Protocol
IBM	International Business Machines (Company)
IEC	International Electrotechnical Organization
IIOT	Industrial Internet of Things
IL	Illinois
IMF	International Monetary Fund
IN	Indiana
IOT	Internet of Things

© Strategy of Things, 2025. All rights reserved.

Initialism	Description
IP	Internet Protocol
ISA	International Society of Automation
ISA99	International Society of Automation Committee
IT	Information Technology
JD	J.D. Power (Company)
KPMG	KPMG (Company)
LTE	Long-term Evolution
M2M	Machine to Machine
MA	Massachusetts
MD	Maryland
MEP	Manufacturing Extension Partnership
MES	Manufacturing Execution System
ML	Machine Learning
MQTT	Message Queuing Telemetry Transport
MR	Mixed Reality
MSA	Metropolitan Statistical Areas
NB	Narrowband
NGMN	Next Generation Mobile Networks
NH	New Hampshire
NJ	New Jersey
NR	New Radio
NTT	Nippon Telegraph and Telephone (Company)
NY	New York
OEM	Original Equipment Manufacturers
OMB	Office of Management and Budget
OPC	Open Platform Communications (OPC Foundation)
OPM	Open Manufacturing Platform

© Strategy of Things, 2025. All rights reserved.

Initialism	Description
OS	Operating System
OT	Operational Technology
OVH	OVHcloud (Company)
PA	Pennsylvania
PCI	Peripheral Component Interconnect
PII	Personally Identifiable Information
PLC	Programmable Logic Controllers
PMIS	Project Management Information Systems
PPP	FI-PPP (Future Internet Public Private Partnership)
QA	Quality Assurance
RF	Radio Frequency
ROI	Return on Investment
REST	Representational State Transfer
SB	Senate Bill (legislation)
SDN	Software Defined Networking
SKT	South Korea Telecom
SOA	Service-Oriented Architecture
SP800	Cybersecurity for IoT Program
SVP	Senior Vice President
TCP	Transmission Control Protocol
TV	Television
TX	Texas
UA	Unified Architecture
UK	United Kingdom
UN	United Nations
UTM	Unified Threat Management
V2G	Vehicle to Grid

© Strategy of Things, 2025. All rights reserved.

Initialism	Description
VA	Virginia
VP	Vice President
VPP	Virtual Power Plants
VR	Virtual Reality
VRT	Variable Rate Technology
WA	Washington
WFP	World Food Programme
WI	Wisconsin
WV	West Virginia
XMPP	Extensible Messaging and Presence Protocol

© Strategy of Things, 2025. All rights reserved.

For more information contact:

Benson Chan

Email: benson@strategyofthings.io

Renil Paramel

Email: renil@strategyofthings.io

Christopher Reberger

Email: christopher@strategyofthings.io

Strategy of Things

www.strategyofthings.io

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the authors, except in the case of brief quotations embodied in research reports, industry articles and certain other noncommercial uses permitted by copyright law. For permission requests, write to the publisher, addressed "Attention: Permissions Coordinator," at the address below.

Strategy of Things LLC

1305 Franklin Street, Suite 507

Oakland, CA 94612

marketing@strategyofthings.io