NISTIR 7190

Distributed Biometric Access Control Testbed

Stephen J. Treado
Steven C. Cook
Michael Galler

NIST
National Institute of Standards and Technology
Technology Administration, U.S. Department of Commerce

NISTIR 7190

Distributed Biometric Access Control Testbed

Stephen J. Treado
Steven C. Cook
Michael Galler
Mechanical Systems and Controls Group
Building Environment Division

U.S DEPARTMENT OF COMMERCE
National Institute of Standard and Technology
Building and Fire Research Laboratory
Gaithersburg, MD 20899-8600

November 26, 2004

U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary
TECHNOLOGY ADMINISTRATION
Michelle O'Neill, Acting Under Secretary for Technology
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
William A. Jeffrey, Director

Abstract:

This report describes the development and implementation of a testbed for demonstrating a distributed, multimodal biometric authentication system for access control applications in buildings. The testbed includes a number of different biometric readers, along with a smart card reader, which were integrated with the Building and Fire Research Laboratory's Virtual Cybernetic Building Testbed (VCBT). The VCBT allows the real-time simulation of a complete building automation and control system. Typical access control scenarios were emulated using the virtual testbed, to develop methods for implementing biometric access control, and to demonstrate and evaluate the performance of the biometric access control system.

1. Introduction

Biometric authentication and identification techniques are increasingly being relied upon for managing access control, both physical access and virtual access. The underpinnings of biometric authentication are their ability to strongly bind identity to actors, using characteristics that are unique to individuals, and that can be reliably sensed and compared to reference characteristics. Vendors of biometric equipment, building owners and operators, and organizations responsible for security, both public and private, are actively pursuing the use of biometric techniques for access control. There are many open questions regarding the most effective methods for implementing biometric authentication for access control, including the use of biometric systems, the integration of biometric access control with the building automation system, and the interoperability of biometric systems in multimodal applications. These open questions mainly have to deal with the management and operation of the biometric systems, the transfer and storage of information, and the methods of communication between system elements.

In order to investigate these issues, the NIST Building and Fire Research Laboratory has expanded its Virtual Cybernetic Building Testbed (VCBT) to include an access control system incorporating distributed biometric authentication. The VCBT was developed to provide a means for developing, improving and demonstrating advanced building control strategies and control system integration [1]. The purpose of the biometric access control testbed is to develop and demonstrate the operation of a distributed, multimodal biometric access control system, including its integration with a building automation system. The objective of the accompanying research project is to utilize the BACnet and BioAPI standards to implement the biometric access control system. This report describes the results of the testbed demonstrations, and the implications for biometric system design and operation.

2. Background

Biometric authentication has been a very active field, including both applications and research [2,3]. Most of the emphasis in biometric research has been concentrated on developing more reliable, fast and accurate identification methods [4]. The performance of biometric readers and matching algorithms has seen continued improvement, although perfect accuracy remains an elusive goal. Although biometric authentication is used extensively for access control, there has been, however, less emphasis on the most effective methods for implementing biometrics for this application. There are numerous systems and network related issues associated with effectively integrating biometric authentication into building access control. These involve communication issues, information management and access control strategies.

For example, biometric authentication is the basis for establishing or verifying identity, which is only part of an access control decision. The determination of whether to allow access to an individual requesting it is based on a combination of the following: Is this *person* allowed access through this *access point* to this *access zone* at this *time*? In order to reach a satisfactory answer to the above question, the *identity*, the *access rights*, the *access times* and the *access rules* for that individual must all be considered. When dealing with a large building with many access points and zones, or even an extended campus or non-contiguous collection of building sites, the management and flow of the relevant information becomes a major issue [5]. Different biometric readers may be deployed at different locations, each with unique biometric data records. Access rights and rules may vary with location, time and circumstances (i.e., threat level or incident). Keeping track of the locations of individuals and their access rights, as well as managing access point and zone status, is a complex undertaking. This is the function of the access control system.

Examples of biometric characteristics that have been used for identity determination and verification include:

- Fingerprint
- Hand geometry
- Iris scan
- Facial recognition
- Retinal scan
- Voice recognition
- Handwriting
- Gait
- Typing pattern

The process of identifying an individual by sensing a biometric characteristic can be either an active or passive operation, from the point of view of the individual. Active biometric sampling requires the individual to proactively interact with a biometric reader, such as placing a finger on a fingerprint reader, or position their face or eye in close proximity to a camera, while remaining still. In contrast, passive biometric sampling involves monitoring that does not require cooperation from the individual being sampled, and may be done without their knowledge. Examples of passive biometric sampling include cameras for recording faces or gait, or voice recognition. The challenges of biometric identification using passive sampling methods are obviously greater, since 1), the sampling conditions are variable and uncontrolled, 2), the individual being monitored is not cooperating in providing the sample, and 3), in most cases there is no identity claim, so a one-to-many identification operation is required.

Routine building access control usually is based on active biometric sampling, and one-to-one identity verification. Individuals are enrolled on each biometric device, and their biometric sample is stored as a template on the system, along with the relevant user information, such as name, department, etc.

For many reasons, multimodal biometric applications, defined as the use of more than one biometric feature for an identity verification, are receiving more interest. One application of multimodal biometrics is sampling more than one biometric characteristic at a single location and time in order to improve the identification performance. A great deal of effort is currently underway to investigate the best procedures for combining multimodal biometric samples to reduce the chances of making an error in identity determination, thereby reducing both false accepts and false rejects.

Another application of multimodal biometrics is combining a series of biometric authentication collected at different locations and at different times. Thus, a user might have their hand shape checked at the front gate, have a fingerprint checked at the main door, and then have an iris scan in order to enter the computer room. Rather than treating each of these biometric authentications as an independent event, each successive authentication can be combined with the previous ones in order to improve accuracy, and reduce false results. Thus, multimodal biometric authentications can be distributed throughout location and time, requiring methods for maintaining and transferring the relevant information, and procedures for reaching access decisions. Since this task falls outside the control of any single biometric device, it must be assumed by the access control system as well.

Multimodal biometric authentication involves the combining of more than one biometric characteristic in order to make an identity determination. There are different methods that can be used to combine multiple biometrics, but they can be grouped in the following categories:

1. Decision Based- a fusion of the identity decisions from each biometric
2. Score Based- a fusion of the matching scores produced by each biometric
3. Pattern Based- a fusion of the biometric characteristic samples themselves into a single sample

While it is not within the scope of this investigation to develop and evaluate multimodal biometric fusion algorithms, it is within the scope to develop methods for implementing distributed multimodal biometric access control. To that end, methods for enabling the collection, transfer and storage of the necessary biometric information by the access control system were developed and demonstrated using the biometric testbed. These methods were generalized to accommodate different system designs and implementations, as would be required for various access control applications. The BioAPI standard [6] was used to handle the interactions between the users and the biometric devices, and the biometric identity verifications, while the BACnet access control data structures and communication protocols [7] were used for the access control operations.

3. Design of the Biometric Testbed

3.1 Overview

The biometric testbed was added as an enhancement to the VCBT. The VCBT consists of several building HVAC controllers, a fire alarm system, and a lighting controller, all on a local area network (LAN), along with a computer system with the capability of simulating the operation of an actual building. Thus, from the controllers' point of view, all sensors and actuators are installed in a real building. The "virtual building" environment is provided by computer models of building operation, including HVAC systems, thermal interactions with the environment, and special scenarios, such as fires or other emergencies. Communication among the controllers is accomplished using the BACnet protocol.

The access control capability was added to the virtual building testbed in the form of an access controller application running on a server connected to the LAN. The access control system included three virtual access zones, each associated with a virtual access point, at which identity was checked using an actual biometric device. A smart card reader was also incorporated at one access point. Figure 1 shows a schematic representation of the physical layout of the biometric access control testbed. The smart card reader, the fingerprint reader and the iris scanner all connected directly to a computer workstation, while the hand shape reader connected directly to the LAN. Users were enrolled individually on each biometric device, using a BioAPI application. More details on the biometric and card readers are given below.

Figure 2 shows the three virtual access points and zones that correspond to the physical card reader and biometric readers. The test bed was exercised by having real subjects attempt to move through the virtual building zones by providing their biometric samples at the appropriate biometric reader. Each biometric device conducted its own identity verification, and provided the result to the access controller using the LAN. The access controller then applied its own rules, taking into consideration the access rights of the individual, along with any multimodal fusion logic, to make the final access decision, which was then transmitted to the virtual access point. If the user was granted access, he would move into the next access zone.

3.2 Smart Card Reader and Fingerprint Reader

Smart cards are frequently used in access control systems, usually without any biometric functionality. In that mode, the smart card can be read as part of an identity claim, either stand alone or followed by a biometric authentication. However, for the biometric testbed, the smart cards were used with dual functionality, both as an identity token and to store a fingerprint template. All valid users were enrolled with their user information and a fingerprint scan, which was converted into a template and stored on the smart card with the user data. The data encoded on the smart card included the following:

- Username
- Department
- Password
- Access Level
- Fingerprint Template

In order to claim an identity, the user must provide the smart card, along with the proper password, and provide a matching fingerprint. This approach provides three layers of security, and relieves the access control system of the burden of managing the biometric template, since it is carried on the smart card. Of course, proper precautions must be taken to keep the information on the card secure; this can be accomplished using techniques such as encryption and challenge/response. Specific security procedures are beyond the scope of this project, but they are being addressed elsewhere [8]. Figure 3 shows the smart card data fields.

In the virtual building, Access Point 1 requires the user to insert a valid smart card, provide the correct password and provide a fingerprint match. If these are successfully accomplished, Access Point 1 will send an access request for the user to enter Access Zone 1 to the access controller. The access controller will apply the access rights and rules, and respond with an access granted or denied. Figure 4 shows the basic operation of the biometric and access control applications.

3.2 Hand Shape Reader and Iris Camera

The input devices for access points 2 and 3 are a hand shape reader and an iris camera. Users are enrolled on these devices using the same user names as on their smart card. The biometric templates for the hand shape device are stored on the device, while the templates for the iris camera are stored on the biometric workstation. BioAPI allows for these to be moved and stored by the applications as desired. Thus, they could be collected in a database for backup or other purposes.

Users can request entry through access points 2 or 3 by providing their user name and biometric sample. If their identity is verified by the local device (i.e., the respective biometric device), an access request is sent to the access controller, which again applies the access rights and rules to reach an access decision. This process is repeated for subsequent access points. Figure 5 summarizes the logical flow of the biometric testbed.

3.3 Access Controller

The access controller performs several functions. Its most important function is to be the final arbiter on granting access. It does so on the basis of its application of access rights for the individual requesting access, the access rules employed by the access control system, and the multimodal fusion rules, if they are being implemented. The access controller also is responsible for updating user data, user logs, access zone logs and activity logs. Finally, the access controller must provide a mechanism by which system administrators can enter and edit access rights and rules, and add or delete users.

As was the case with the smart cards, the appropriate security measures must be implemented to ensure that only authorized administrators can modify the attributes of the access controller. This can be accomplished using traditional network login authorization procedures, which can themselves incorporate biometric authentication [9]. These specific security procedures are beyond the scope of this project.

4. Access Control Operations and Data Structures

The biometric testbed described above is a particular implementation of a general biometric access control scheme. In the general case, different biometric devices can be incorporated into an access control system in unique configurations. Biometric algorithms and records can be stored, retrieved and utilized in a particular manner. Thus, in order to design and model an access system using biometric authentication, it is useful to delineate all of the essential components and elements, and the information management strategies needed to implement a fully functional system. Then, typical access control scenarios can be simulated to evaluate their performance.

A general biometric access control system must be able to provide the following functions:

- Valid user enrollment
- Administrator management of user data, access rights and rules
- Identity verification
- Access decision
- Control of access points
- Monitoring of sensors

These functions require the use of algorithms tailored to the biometric devices, as follows:

- Biometric template algorithms- convert biometric sample data to templates
- Biometric matching algorithms- compare biometric templates to verify identity
- Multimodal biometric fusion algorithms- apply multimodal methods for enhanced identification accuracy
- Access decision algorithms- make final decision on granting access based on identity, access rights and access rules

These algorithms operate on different data elements, which may be collected in separate databases, as listed below:

- User database
  - Name
  - Organization
  - Location
  - Access level
  - Pointer to biometric data
- Biometric template database
- Access rights database
- Access rules database

Access rights could include things such as time and date ranges when individuals are allowed or denied access to certain zones, or categories of employees allowed certain access privileges. Access rules would involve concepts such as the logical movement of individuals through access points, whereby they should pass through one zone before they attempt to enter another, and rules regarding a minimum or maximum number of zone occupants.

The components of the biometric authentication access control system include:

- Biometric readers
- Access controllers
    - Door locks
    - Signaling
    - Sensors
- Tokens and smart cards
    - User data
    - Biometric template
    - Matching algorithm
- Operators workstation
- Server
    - Processing
    - Database

The operation and status of the access control system is represented by logs, as follows:

- User log
    - Access history
    - Current zone
- Access zone log
    - Current occupants
    - Zone status
- Activity log
    - Access requests
    - Identification decisions
    - Access decisions
    - Door openings
    - Sensor readings
    - System administration tasks

Figure 6 shows a graphical representation of the elements of a general biometric access control system, sorted by category. Each of these elements and capabilities of a biometric access control system need to be present in order to provide the functionality expected of an access control system. The specifics of how a system is implemented will vary based on the collection of devices being used. For example, a simple biometric access controller might combine all of the functions, operations and data management into a single, stand-alone device. There might be an input keypad, a biometric reader, a small display or indicator lights, and a processing unit. Both enrollment and verification would be accomplished using the same device, which would store all of the data files and algorithms necessary for operation. The device might also include output relays to control door locks, and sensor inputs for request to exit and door position.

At the other end of the spectrum, the access control system might be highly distributed, with separate readers, access point controllers, central data server, and operator's workstation. The access control application could be controlling multiple access points, and need to exchange biometric data and access control requests and commands with a multitude of devices. Such a large comprehensive system would need to be broken down into its components, and have a sequence of control and operation established in a manageable fashion.

Figure 7 shows a general flow diagram for biometric access control. It depicts, in a general way, the logical flow and exchange of information required to incorporate biometric authentication into access control. Two basic sequences of operation are given below.

Biometric Access Control Sequence of Operation- Single Mode

1. User requests entry
2. User makes identity claim
3. System checks user database to see if requestor is a valid user
4. If valid user, system retrieves user data
5. System prompts user to enter biometric sample
6. User provides live biometric sample
7. System reads live biometric sample
8. System converts live biometric sample to live template
9. System applies algorithm comparing live template to reference template, and determines match score
10. Match score is compared to threshold
11. If score is greater than threshold, ID is verified
12. System retrieves access rights for user
13. System applies access rights and rules to determine access decision
14. If access is granted, system sends command to unlock door
15. System updates logs

Biometric Access Control Sequence of Operation- Multimodal

1. User requests entry
2. User makes identity claim
3. System checks user database to see if requestor is a valid user
4. If valid user, system retrieves user data
5. System prompts user to enter biometric sample
6. User provides live biometric sample
7. System reads live biometric sample
8. System converts live biometric sample to live template
9. System applies algorithm comparing live template to reference template, and determines match score
10. Match score is compared to threshold
11. If score is greater than threshold, ID is verified locally

12. System retrieves data from previous biometric authentications, either identity decisions, matching scores or biometric samples
13. System applies multimodal fusion algorithm
14. System makes global identification decision
15. If ID verified, system retrieves access rights for user
16. System applies access rights and rules to determine access decision
17. If access is granted, system sends command to unlock door
18. System updates logs

5. Summary

A biometric testbed was developed and implemented as an enhancement to the BFRL Virtual Cybernetic Building Testbed (VCBT). The biometric testbed included three biometric readers and a smart card reader, along with a workstation and a server. A custom access control application was created to link the physical biometric readers to virtual access points and zones, to allow the simulation of access control in a multi-zone building. Another application provided communication with the biometric readers using BioAPI. Data structures were implemented following the BACnet access control objects, which are currently in draft form, and network communication was accomplished using BACnet. The access control application managed the flow of information, and applied the access rights and rules to reach access decisions. It also kept track of the location of building occupants, and provided network visibility for the status of the access control system. The biometric testbed was used to simulate typical operations of an access control system, in order to develop and demonstrate the integration of biometric authentication with building access control.

6. References

1. S. Bushby, N. Castro, M. Galler, C. Park, J. House, "Using the Virtual Cybernetic Building Testbed and FDD Test Shell for FDD Tool Development", NISTIR 6818, National Institute of Standards and Technology, Gaithersburg, MD 20899, October, 2001

2. P. Reid, "Biometrics for Network Security", Prentice Hall PTR, Upper Saddle River, NJ, 2004

3. J. Ashbourn, "Biometrics- Advanced Identity Verification", Springer-Verlag London Limited, 2000

4. L. Jain, U. Halici, I. Hayashi, S. Lee, S. Tsutsui, editors, "Intelligent Biometric Techniques in Fingerprint and Face Recognition, CRC Press, 1999

5. S. Liu, M. Silverman, "A Practical Guide to Biometric Security Technology", http://www.computer.org, Institute of Electrical and Electronics Engineering, 2001

6. The Bio API Consortium, "BioAPI Specification Version 1.1", http://www.bioapi.org, 2000

7. ANSI/ASHRAE Standard 135-2004, "BACnet- A Data Communication Protocol for Building Automation and Control Networks", American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc., Atlanta, GA, 2004

8. C. Kaufman, R. Perlman, M. Speciner, "Network Security- Private Communication in a Public World", Pearson Education, Prentice Hall, Upper Saddle River, NJ, 1995

9. M. Krause, H. Tipton, "Handbook of Information Security Management", Auerbach Publications, CRC Press LLC

Figure 1. Schematic diagram of biometric access control testbed

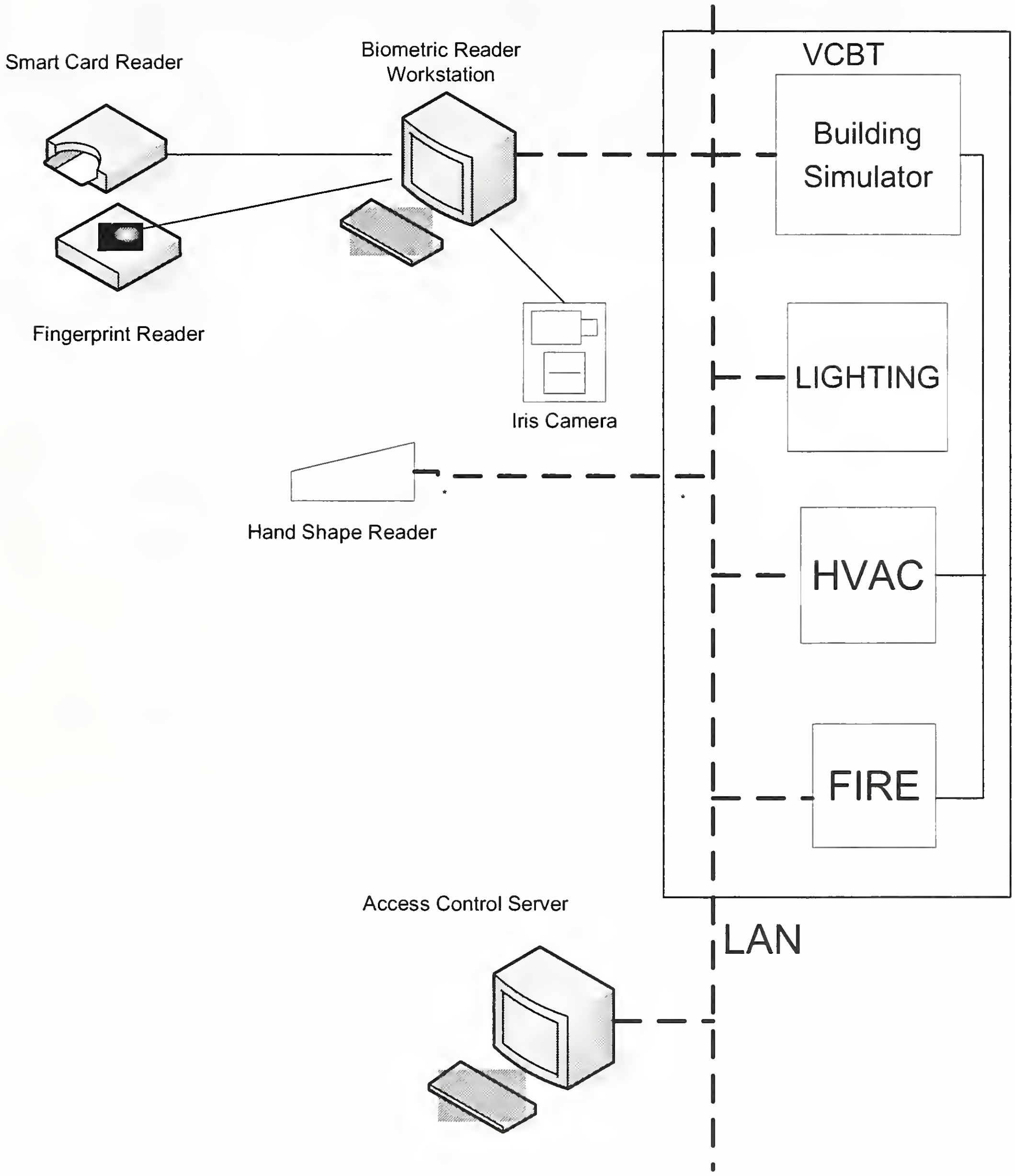
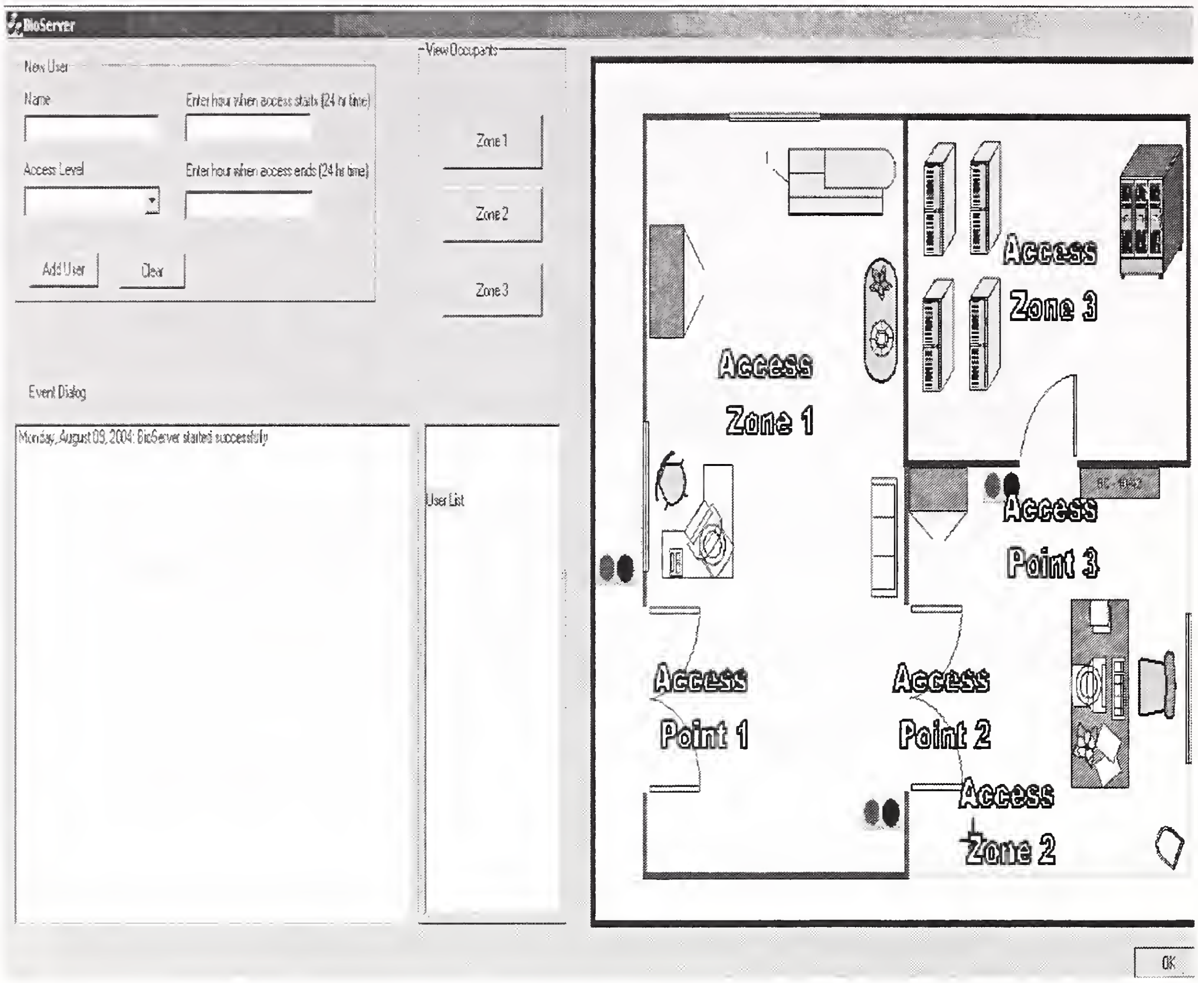
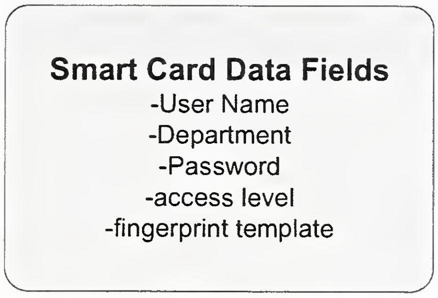


Figure 2. Server screen with layout of virtual access points and zones



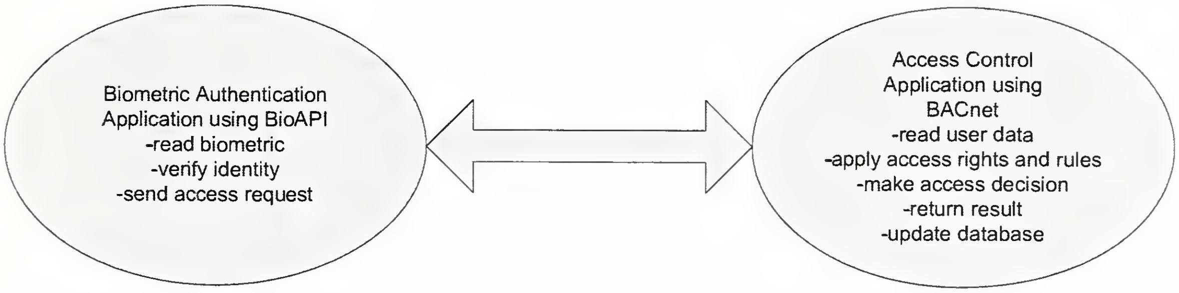
Monday, August 09, 2004: BioServer started successfully

Figure 3. Enrollment with Smart Card



Smart Card Data Fields
-User Name
-Department
-Password
-access level
-fingerprint template

Figure 4. Basic Operation of Biometric Access Control Software



Biometric Authentication Application using BioAPI
-read biometric
-verify identity
-send access request

Access Control Application using BACnet
-read user data
-apply access rights and rules
-make access decision
-return result
-update database

Figure 5. Flow Diagram for Biometric Testbed

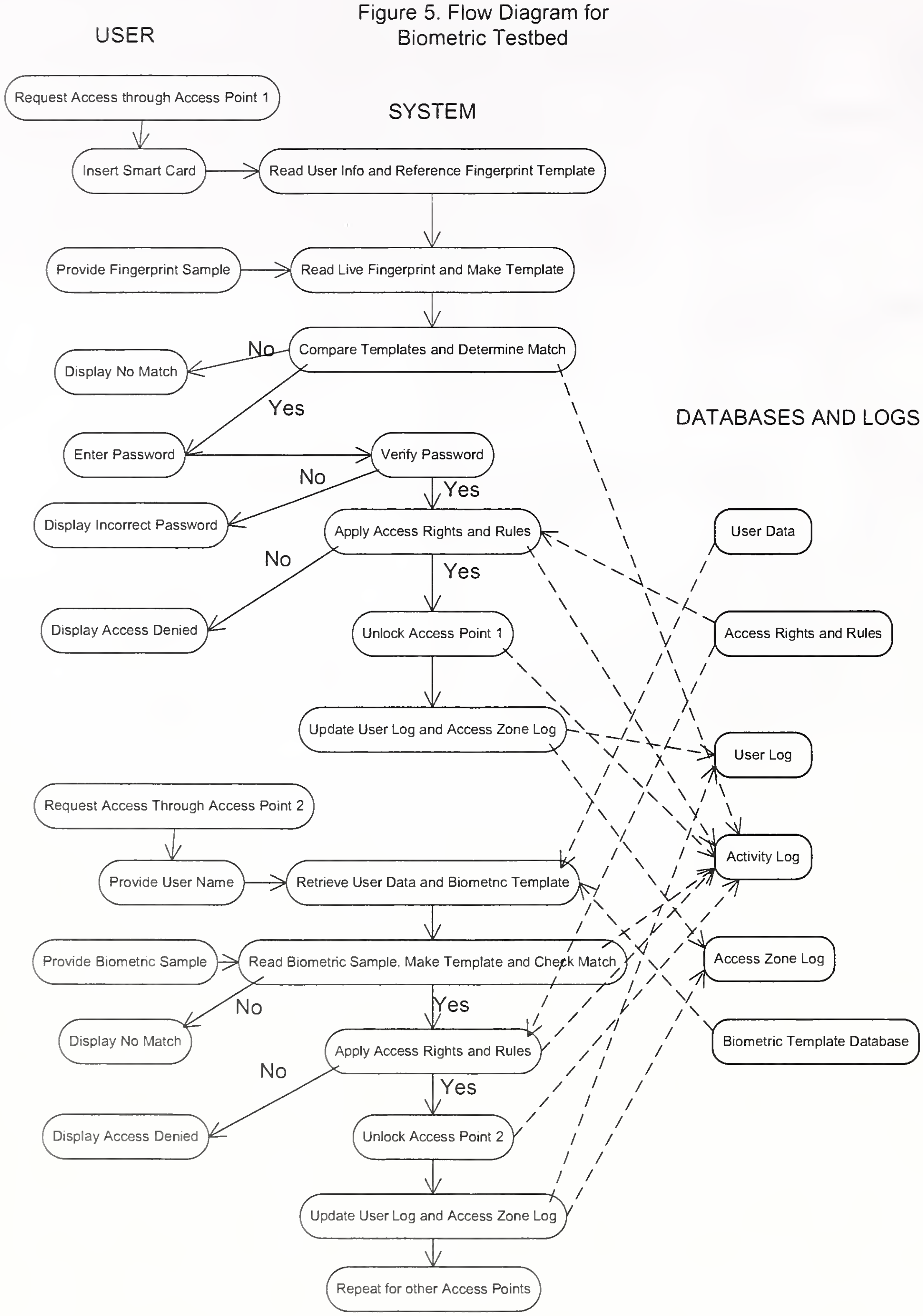

USER
SYSTEM
DATABASES AND LOGS
Request Access through Access Point 1
Insert Smart Card
Read User Info and Reference Fingerprint Template
Provide Fingerprint Sample
Read Live Fingerprint and Make Template
Compare Templates and Determine Match
No
Display No Match
Yes
Enter Password
Verify Password
No
Yes
Display Incorrect Password
Apply Access Rights and Rules
No
Yes
Display Access Denied
Unlock Access Point 1
Update User Log and Access Zone Log
User Data
Access Rights and Rules
User Log
Activity Log
Access Zone Log
Biometric Template Database
Request Access Through Access Point 2
Provide User Name
Retrieve User Data and Biometnc Template
Provide Biometric Sample
Read Biometric Sample, Make Template and Check Match
No
Yes
Display No Match
Apply Access Rights and Rules
No
Yes
Display Access Denied
Unlock Access Point 2
Update User Log and Access Zone Log
Repeat for other Access Points

Figure 6. General Access Control Elements

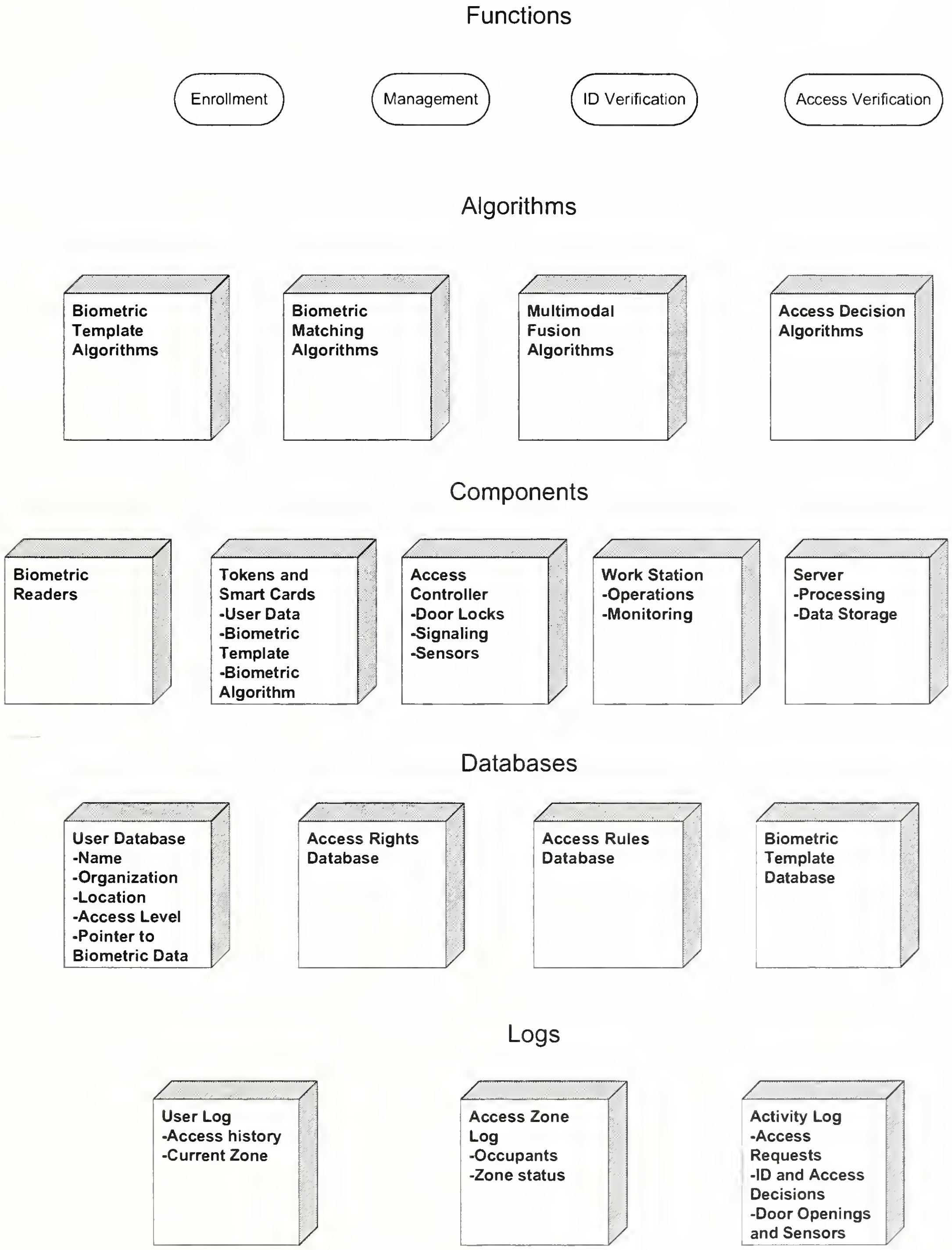
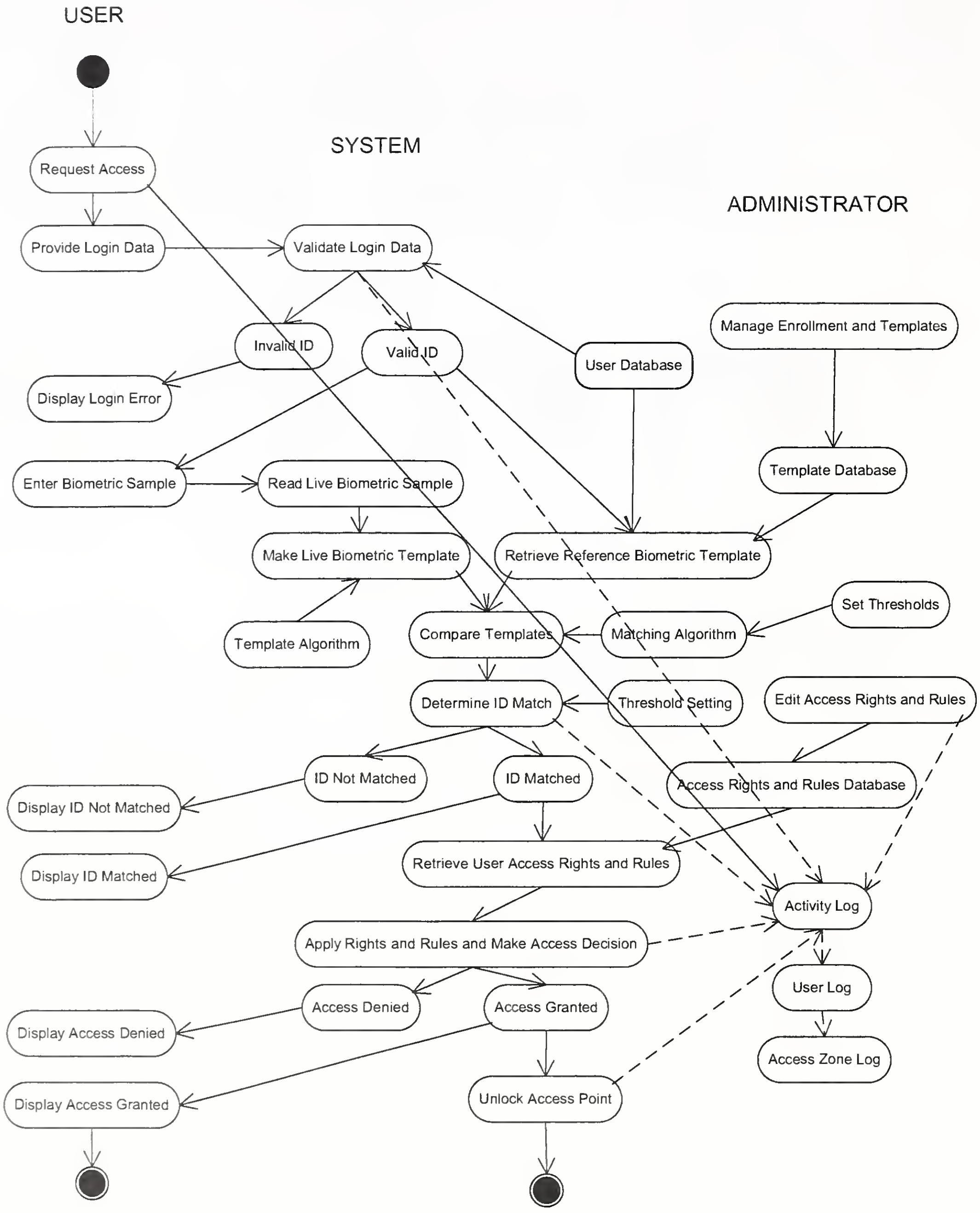

Functions
Enrollment
Management
ID Verification
Access Verification
Algorithms
Biometric Template Algorithms
Biometric Matching Algorithms
Multimodal Fusion Algorithms
Access Decision Algorithms
Components
Biometric Readers
Tokens and Smart Cards -User Data -Biometric Template -Biometric Algorithm
Access Controller -Door Locks -Signaling -Sensors
Work Station -Operations -Monitoring
Server -Processing -Data Storage
Databases
User Database -Name -Organization -Location -Access Level -Pointer to Biometric Data
Access Rights Database
Access Rules Database
Biometric Template Database
Logs
User Log -Access history -Current Zone
Access Zone Log -Occupants -Zone status
Activity Log -Access Requests -ID and Access Decisions -Door Openings and Sensors

Figure 7. Flow Diagram for Biometric Access Control


USER
SYSTEM
ADMINISTRATOR
Request Access
Provide Login Data
Validate Login Data
Invalid ID
Valid ID
Display Login Error
Enter Biometric Sample
Read Live Biometric Sample
Make Live Biometric Template
Template Algorithm
Manage Enrollment and Templates
User Database
Template Database
Retrieve Reference Biometric Template
Compare Templates
Matching Algorithm
Set Thresholds
Determine ID Match
Threshold Setting
Edit Access Rights and Rules
ID Not Matched
ID Matched
Access Rights and Rules Database
Display ID Not Matched
Display ID Matched
Retrieve User Access Rights and Rules
Activity Log
Apply Rights and Rules and Make Access Decision
User Log
Access Denied
Access Granted
Display Access Denied
Access Zone Log
Display Access Granted
Unlock Access Point