BIOMETRIC AUTHENTICATED LIBRARY NETWORK MODEL FOR INFORMATION SHARING

ATUL M GONSAI **NILESH N SONI**

Abstract

To provide the security to the library network or any other network, nowadays we have various newly developed mechanisms to provide security in the form of identifying the user and allowing specific access to the user. User Authentication can be achieved by the way of user name and password but it has very less level of impact to identify the proper user. For this reason the new mechanism like computer access is granted by checking a fingerprint. One can use Biometric Authentication Technique to apply in the library network to provide high level of security to identify the proper user. Biometric-based authentication applications include workstation and network access, application logon, data protection, and remote access to resources, transaction security. This paper discusses the application of Biometric authentication technologies in the field of library network by way of the library model which uses Biometric authentication in the form fingerprint scanning to identify the user and then gets the library resource.

Keywords: Biometric Authentication/ Finger Print Technology/Sensors/ Biometric Network

1. Introduction

The role of network operators has morphed from that of simple infrastructure providers to enablers of Next Generation Network (NGN) services. While this expanded role encompasses a lucrative and growing market opportunity, operators now face new challenges regarding security and privacy in the delivery of these services. Threats range from the nuisance of spam to the propagation of viruses and more serious forms of identity theft and intellectual property rights violations [2].

In order to achieve the objective of the paper, the libraries will need automation their services with support of bio authentication to identify the user. To automate library services efficiently and effectively one needs an integrated library automation, which will provide the bio authentication support. There is several commercial library automation packages now available but the costs of these packages are beyond the reach of most of the libraries especially the school and college libraries. Therefore this paper discusses the library model, which uses bio authentication technique [4].

2. Biometrics - What is?

Biometrics is automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. Examples of physiological characteristics include hand or finger images, facial characteristics, and iris recognition. Behavioral characteristics are traits that are learned or acquired. Dynamic signature verification, speaker verification, and keystroke dynamics are examples of behavioral characteristics. Biometric authentication requires comparing a registered or enrolled biometric sample (biometric template or identifier) against a newly captured biometric sample (for example, a fingerprint captured during a login) [3].

Biometric recognition can be used in Identification mode, where the biometric system identifies a person from the entire enrolled population by searching a database for a match based solely on the biometric. For example, an entire database can be searched to verify a person who is registered user of university library or not. A system can also be used in Verification mode, where the biometric system authenticates a person's claimed identity from their previously enrolled pattern. This is also called "one-to-one" matching. In most computer access or network access environments, verification mode would be used. A user enters an account, user name, or inserts a token such as a smart card, but instead of entering a password, a simple touch with a finger or a glance at a camera is enough to authenticate the user (L. Podio and Jeffrey S. Dunn 2002).

3. Types of Biometrics

Fingerprints: The patterns of friction ridges and valleys on an individual's fingertips are unique to that individual. For decades, law enforcement has been classifying and determining identity by matching key points of ridge endings and bifurcations. Fingerprints are unique for each finger of a person including identical twins. One of the most commercially available biometric technologies, fingerprint recognition devices for desktop and laptop access are now widely available from many different vendors at a low cost.

Face Recognition: The identification of a person by their facial image can be done in a number of different ways such as by capturing an image of the face in the visible spectrum using an inexpensive camera or by using the infrared patterns of facial heat emission. Facial recognition in visible light typically model key features from the central portion of a facial image. Using a wide assortment of cameras, the visible light systems extract features from the captured image(s) that do not change over time while avoiding superficial features such as facial expressions or hair.

Speaker Recognition: Speaker recognition has a history dating back some four decades, where the output of several analog filters was averaged over time for matching. Speaker recognition uses the acoustic features of speech that have been found to differ between individuals. These acoustic patterns reflect both anatomy (e.g., size and shape of the throat and mouth) and learned behavioral patterns (e.g., voice pitch, speaking style). This incorporation of learned patterns into the voice templates (the latter called

"voiceprints") has earned speaker recognition its classification as a "behavioral biometric. [5]

Iris Recognition: This recognition method uses the iris of the eye, which is the colored area that surrounds the pupil. Iris patterns are thought unique. The iris patterns are obtained through a video-based image acquisition system. Iris scanning devices have been used in personal authentication applications for several years. Systems based on iris recognition have substantially decreased in price and this trend is expected to continue [7].

Hand and Finger Geometry: These methods of personal authentication are well established. Hand recognition has been available for over twenty years. To achieve personal authentication, a system may measure either physical characteristics of the fingers or the hands. These include length, width, thickness and surface area of the hand. One interesting characteristic is that some systems require a small biometric sample (a few bytes). Hand geometry has gained acceptance in a range of applications.

Signature Verification: This technology uses the dynamic analysis of a signature to authenticate a person. The technology is based on measuring speed, pressure and angle used by the person when a signature is produced. One focus for this technology has been e-business applications and other applications where signature is an accepted method of personal authentication.

4. Biometrics Why?

Using biometrics for identifying human beings offers some unique advantages. Biometrics can be used to identify you as you. Tokens, such as smart cards, magnetic stripe cards, photo ID cards, physical keys and so forth, can be lost, stolen, duplicated, or left at home. Passwords can be forgotten, shared, or observed. Moreover, today's fast-paced electronic world means people are asked to remember a multitude of passwords and personal identification numbers (PINs) for computer accounts, bank ATMs, e-mail accounts, wireless phones, web sites and so forth. Biometrics holds the promise of fast, easy-to-use, accurate, reliable, and less expensive authentication for a variety of applications [8].

There is no one "perfect" biometric that fits all needs. All biometric systems have their own advantages and disadvantages. There are, however, some common characteristics needed to make a biometric system usable. First, the biometric must be based upon a distinguishable trait. For example, for nearly a century, law enforcement has used fingerprints to identify people. There is a great deal of scientific data supporting the idea that "no two fingerprints are alike." Technologies such as hand geometry have been used for many years and technologies such as face or iris recognition have come into widespread use. Some newer biometric methods may be just as accurate, but may require more research to establish their uniqueness [6].

Another key aspect is how "user-friendly" a system is. The process should be quick and easy, such as having a picture taken by a video camera, speaking into a microphone, or touching a fingerprint scanner.

5. Biometric Fingerprint Identification

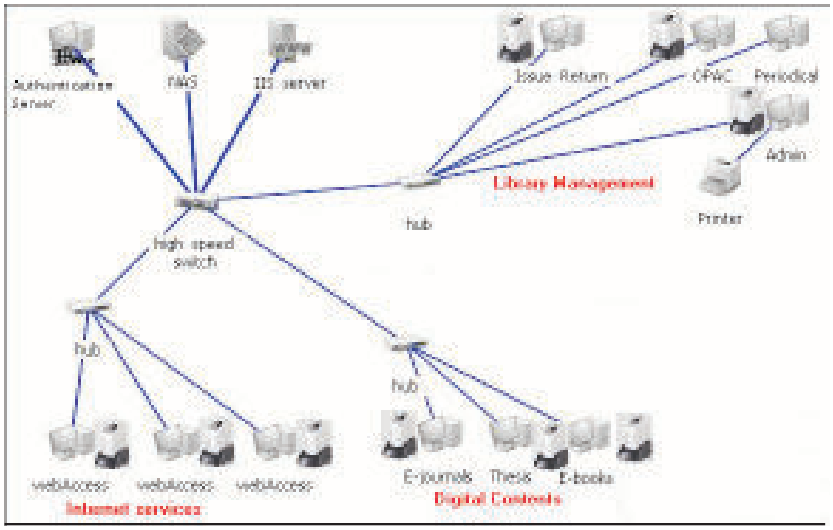
Biometric-based authentication applications include workstation and network access, single sign-on, application logon, data protection, remote access to resources, transaction security, and Web security. The promises of e-commerce and e-government can be achieved through the utilization of strong personal authentication procedures. Secure electronic banking, investing and other financial transactions, retail sales, law enforcement, and health and social services are already benefiting from these technologies. Biometric technologies are expected to play a key role in personal authentication for large-scale enterprise network authentication environments even for University libraries and other public libraries [12].

Fingerprint identification system uses a person Fingerprint to identify the person. Every individual fingerprint is different thus the field of fingerprint identification has been most widely researched and developed since it has highly recognizing rate, economical quality and easy to use. The modeled library network is also uses the facility of fingerprint to identify the user of the library network [10].

The libraries model discussed here is for university library, which uses fingerprint identification system, but it can also be used for other types of libraries like public library or research libraries.

6. Biometric Authenticated Library Network Model

A typical network diagram showing multiple computer Systems connected through a library network [13]. Each computer is assigned its own specific IP address. These systems can be set up in a master / slave configuration so that biometric template data is replicated automatically throughout the network. [9]



7. Components of Library Network

Library network require the various component to establish computer networks. From the above figure we can say that there is a need for following components:

- Computer systems for various need like for digital contents, internet access and for library management
- Servers for handling library management like SOUL server
- One switch and two hubs to provide connectivity
- Network Attested Storage (NAS) to store digital contents
- Web server to provide internet access to the users
- Finger print sensor to sense the user finger print

8. User access Rights

The above discussed model has three main library parts which library management to handle day to day activities of library, Digital contents to read by the user on library network like Ph.D thesis or any research data which is stored in NAS server and the last part is to provide the internet access to access digital libraries on internet (Manvish 2006).

Fingerprint Sensor : The fingerprint sensor is important component unit in the library network and can sense/capture the fingerprint for stored as template and also used for verification and identification. These sensor are most advanced Solid-state Silicon based Capacitive Fingerprint Sensor, which is extremely compact, versatile monolithic fingerprint pattern sensor implemented in a 0.5 um triple metal CMOS process. The sensor works by sensing the small variations in surface-capacitance when fingertip is placed on [1].

Fingerprint Matching : Each fingerprint registered within a particular storage is stored as a 512-byte template. The internal algorithm uses a pattern-matching algorithm to compare a newly retrieved fingerprint against the previously stored templates. Dedicated LSI circuitry carries out the fingerprint verification within the unit itself. Each fingerprint registered with the unit is capable of matching fingerprints internally in less than a second.

The user has to put his/her finger on finger print sensor, which will scan the finger image for authentication and then matches the image with stored image and generated the authentication result to give access to the user. The given model has desktop finger print sensor but it can also be used for networked sensor, which will sense the image on network so that network administrator can reduce the cost of sensors. This network model can work only if you want to use it for specific attendance of time or that type of application. While library network has different types of user and each user has

different need of data to access and also connected computers are located in far distance place, So that the model has desktop finger print sensors.

The system Administrator can set the access rights to each and every individual employee /user. The access rights can be set or modified by the Administrator for change of user and employee rights. Using Access rights functionality the following operations can be performed:

- Entry of a person for any specific library application or to any specific NAS storage material can be controlled and monitored.
- Entry of a person can be controlled for unauthorized access.
- Library user can be controlled and monitored
- Administrator can set and modify the access rights to each and every person.
- The access rights can be set or modified by the Administrator for employees or for users.
- Access time restriction can be set for every individual person or a group of individuals for issue of books or for use of Internet access.

9. Conclusion

Recent advances in biometric technology have resulted in increased accuracy at reduced costs; biometric technologies are positioning themselves as the foundation for many highly secure identification and personal verification solutions. Today's biometric solutions provide a means to achieve fast, user-friendly authentication with a high level of accuracy and cost savings. Many areas will benefit from biometric technologies like University libraries and public libraries to protect from unauthorized user to access library network and to give issue of book to only authorized persons.

The library model discussed here provides high level of security using biometric finger print scanner to identify the correct user for physical issue of books and on network to give restricted access of Internet and other digital data. Even this model provides security mechanism for employees to handle library management like issue and return of books, periodical section handling and OPEC.

References

1. Paul Reid, 2003, Biometrics for Network Security, Prentice Hall PTR, chapter-5
2. A white paper by the University of Southern California and VeriSign 2005 Building a Security Framework for Delivery of Next Generation Network Services United States
3. L. Podio and Jeffrey S. Dunn 2002, Biometric Authentication Technology: From the Movies to Your Desktop, National Institute of Standards and Technology (NIST), Information Technology Laboratory

4. Edited by Lori Ayre, Infopeople Project, 2003, Library Computer and Network Security Infopeople Project, http://infopeople.org/howto/security/.

5. Sarbari Gupta, 2004, Identity Authentication Identity Authentication using the using the PIV Token PIV Token, National Institute of Standards and Technology, India

6. Secure Computing Corporation, 2001, Authenticating with one of the safest devices: the biometric Sony Puppy, Secure Computing Corporation, 4810 Harwood Road, San Jose, CA 95124 USA

7. Biometric Consortium web site: http://www.biometrics.org 2006

8. International Biometric Industry Association, http://www.ibia.org 2005

9. Bioenable Technologies Pvt. Ltd. 2004-2005 http://www.bioenabletech.com/biometrics_india_pune_contact.htm

10. Securitex Electronic Systems Engineering, 2006, Fingerprint Identification system http://www.securitex.com.sg/

11. Manvish Embedded Services, 2006, Finger print sensors technology overview http://www.manvish.com/embedded/miFAUN/techoverview.php

12. TopAZ Solutions Pte Ltd, 2006, Biometric Fingerprint Security, http://www.topazsol.com/bio_door_access.htm

BIOGRAPHY OF AUTHORS

Dr. Atul Gonsai, Ph.D., MCA, BBA is Assistant Professor, Department of Computer Science, Saurashtra University, Rajkot. Dr. Atul Gonsai has received his Ph. D degree in the field of Computer Science from the same University. He holds total teaching experience of SIX years. He is the author of THREE books and over 35 research papers related to computer science and computer networking in International and National Journals and conferences. He is life Member of ISTE New Delhi.

Email : atulgosai@yahoo.com

Mr. Nilesh N Soni has completed his Graduation in Bachelor of Commerce and also Library & Information Sc. with Master degree in 1992. He is working as I/c University Librarian, Saurashtra University Library Rajkot. He has written 11-research papers.

Email : sulnilesh@yahoo.co.uk