International Journal of Professional Development

Vol.10,No.1,July-Dec 2021 ISSN: 2277-517X (Print), 2279-0659 (Online)

Impact Factor: 3.115

Security of Digital Library Using Biometric Technology and its Applications

Balvinder Kumari
Research Scholar, JJTUniversity, Rajasthan

Dr. R.N.Malviya
Research Supervisor, , JJTUniversity, Rajasthan
librarian,Rishihood University,Sonepat)

Abstrcts

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. Biometric identification refers to a technology that uses scanned graphical information from many sources for personal identification purposes. The biometric technology helps the libraries to ensure safety and security to its invaluable collections, infrastructure and human resources. It is the duty of the librarian to keep the library buildings, shelves and stacks open and free without losing items to make available or putting individuals at unacceptable risk from the malicious, avaricious or senseless acts of others. The security of materials and information in a library is quite essential. 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 a novel patron authentication approach in an automated and modern library based on the biometric recognition

Keywords: Biometric Authentication/ Finger Print Technology / Sensors /Biometric Network / Biometrics, Library Security, Access Control, Computer Crimes, Cyber Crimes

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

A Library is a temple of learning□ which plays a pivotal role in the overall development of a society. But, it is a known fact that libraries are not always safe and secure places and they are facing a variety of security concerns which includes the theft, mutilation of library materials and other unethical losses. But, it is the duty of the librarian to keep the library buildings, shelves and stacks open and free without losing items to make available or putting individuals at unacceptable risk from the malicious, avaricious or senseless acts of others. Further, the Library and Information professionals are now handling huge database, provide access to online journals and web-enabled online public access catalogues in the networked digital environment where there are a lot of scope for compute /cyber crimes. Most of the libraries, especially the academic libraries follow open access system which allows its users directly to the stakes to ensure optimum utilization of the knowledge resources available in the library. Due to the open access system, books are often found on the library shelves with pages torn from the spine. Sometimes books are damaged beyond repair and almost all academic libraries including libraries in advanced countries are suffering from book or document theft by its members. Theft of library materials is not a new problem, not just an Indian problem. It is a universal problem which includes developed countries including USA, UK and European Union. Therefore, it is important to provide a safe and secure environment for library staff, library resources and equipment, and library users. In this regard, the biometric technology is really a boon for the LIS professionals.

Biometric recognition, or simply biometrics, refers to the automatic recognition of individuals based on their physiological and/or behavioural characteristics. Biometrics can be used to identify the person as person. 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.(*http://www.ibia.org*)

Any human physiological and/or behavioural characteristic can be used as a biometric characteristic as long as it has the following prerequisites.(Jain, Flynn and Ross, 2007).

Universality: each person should have some characteristic;

Distinctiveness: any two persons should sufficiently be differentiable in terms of the characteristic;

Permanence: the characteristic should sufficiently be invariant (with respect to the matching criterion) over a period of time;

Collectability: the characteristic can be measured quantitatively;

Acceptability: easy to accept the particular biometric identifier (characteristic) as people mostly used it in their daily lives;

A ***biometric system*** **is** essentially a pattern recognition system that operates by acquiring biometric data from an individual, extracting a feature set from the acquired data, and comparing this feature set giants the template set in the database.

Biometrics - What is?

Biometrics is automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioural characteristic. Examples of physiological characteristics include hand or finger images, facial characteristics, and iris recognition. Behavioural characteristics are traits that are learned or acquired. Dynamic signature verification, speaker verification, and keystroke dynamics are examples of behavioural 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). 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).

Various Biometrics technologies

A number of biometric characteristics exist and are in use in various applications. Each biometric has its strengths and weaknesses, and the choice depends on the application. No single biometric is expected to effectively meet the requirements of all the applications. The commonly used biometrics are DNA, Face, Ear, Facial infrared thermo gram, Fingerprint, Gait, Hand and Finger geometry, Iris, Keystroke, Palm prints, Signature, Voice etc.

A number of discrete biometric technologies are available on the market today such as signature, fingerprint identification, iris identification, retinal identification, hand geometry, hand, palm, and wrist subcutaneous vein pattern identification, signature identification, voice identification, keystroke dynamics identification, facial feature identification, body salinity (salt) identification, body odor identification, and ear identification. In general, biometrics can be classified into two types□ viz., physiological biometrics and behavioural biometrics. The coverage of these two types is furnished

Below.

Physiological Biometrics

- Iris/Retina
- Fingerprint (including nail)
- Hand (including knuckle, palm, vascular)
- Face
- Voice
- DNA
- Odor, Earlobe, Sweat pore, Lips

Physiological Biometrics

Iris/Retina (Eye biometrics): The iris is the most accurate and invariable of biometrics, and that their system is the most accurate form of biometric technology as the human eye offers two features with excellent properties for identification. Both the iris (the colored part visible at the front of the eye) and the veins of the retina (the thin film of nerve endings inside the eyeball that capture light and send it back to your brain) provide patterns that can uniquely identify an individual. The pattern of lines and colors on the eye are, as with other biometrics, analyzed, digitized, and compared against a reference sample for verification.

Fingerprint: A highly familiar and well-established biometric science is fingerprinting. The traditional use of fingerprinting, of course, has been as a forensic criminological technique, used to identify perpetrators by the fingerprints they leave behind them at crime scenes. In the context of modern biometrics, these features, called fingerprint minutiae, can be captured, analyzed, and compared electronically, with correlations drawn between a live sample and a reference sample, as with other biometric technologies. Fingerprints offer tremendous invariability, changing only in size with age, are highly resistant to modification or injury, and very difficult to " forge" in any useful way.

Hand Geometry: Perhaps it is the most ubiquitous electronic biometric system. This system requires the subject to place his or her hand (usually the right hand) on a plate where it is photographically captured and measured. Made of 27 bones and a complex web of interconnected joints, muscles, and tendons, the human hand presents a sufficiently peculiar conformation of anatomical features to enable authentication.

Facial Recognition: In the field of biometrics, facial recognition remains one of the more controversial technologies because of its very unobtrusiveness. With good cameras and good lighting, a facial recognition system can sample faces from tremendous distances without the subject□ s knowledge or consent. The facial recognition technology works by two methods viz., facial geometry or eigenface comparison. Facial geometry analysis works by taking a known reference point (for example, the distance from eye to eye), and measuring the various features of the face in their distance and angles from this reference point. Eigenface comparison uses a palette of about 150 facial abstractions, and compares the captured face with these archetypal abstract faces. This technology may be highly useful for the libraries in security point of view.

Behavioral biometrics

- Signature
- Keystroke
- Voice
- Gait

Signature: The most familiar biometrics is the signature of an individual. Our ability to judge by sight if one signature matches another has made this a time-proven and legally-binding biometric. However, computers can do all these things, and quantify, analyze and compare each of these properties to make signature recognition a viable biometric technology. Being based on things that are not visible (pen pressure and velocity, for example), signature-based biometric technology, offers a distinct advantage over regular signature verification. The biometric signature verification system, shown in Fig.9, analyzes the act of writing and examines the pressure one applies while writing, the speed and rhythm with which one writes. This method also records the sequence in which one forms the letters. For example, some individuals may add dots and crosses as they keep writing or after they finish the word. These traits are very difficult to forge. Handwriting recognition system□ s sensors can include a touch-sensitive writing surface or a pen that contains sensors, which detect the angle and direction of writing as well as the pressure applied while writing.

Voice Verification : Voice verification is one among the biometric technology available in these days. Voice verification offers one great advantage, which is that it would allow a remote identification using the phone system, an infrastructure that□ s already been built and thus has zero client-side cost: no special reader needs to be installed in the library. Even without the phone system, the sampling apparatus, a microphone, remains far cheaper than competing, largely optically-based biometric technologies.

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. 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. 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.

Biometric Applications in Libraries

In India, most of the academic libraries use computers, Internet and network based services to extend effective and efficient library and information services to the students, research scholars, faculty members and scientists who form the membership base. They are widely using computers for various purposes viz. circulation, cataloguing, information services, collection development and serial control. Somebody either the library users or a mischievous staff may unknowingly or intentionally, conceal (hides or keeps secret), destroy (demolishes or reduces), alter (change in characteristics) or causes another to conceal, destroy, and alter any computer source code used for In India, most of the academic libraries use computers, Internet and network based services to extend effective and efficient library and information services to the students, research scholars, faculty members and scientists who form the membership base. They are widely using computers for various purposes viz. circulation, cataloguing, information services, collection development and serial control. Somebody either the library users or a mischievous staff may unknowingly or intentionally, conceal (hides or keeps secret), destroy (demolishes or reduces), alter (change in characteristics) or causes another to conceal, destroy, and alter any computer source code used for a computer, computer program, computer system or computer network in the Library. So, the LIS professionals should be very careful in this regard (Rathinasabapathy, 2007). Further, LIS professionals are handling huge bibliographical databases to cater to the information requirements of their user community. So, they should be aware of the data diddling where somebody may alter the raw data just before a computer processes it and then changing it back after the processing is completed. They should ensure enough safety and security to their databases. To ensure better safety and security to the rich information resource base and human resources in a library, the movement of documents and personnel should be controlled. At present, electronic surveillance and security systems are being used in some academic libraries. (Rajendran, 2007). However, these systems have got their own limitations. In this context, biometrics applications are highly useful for them. The following are some of the important types of biometric applications useful for the libraries.

Controlled Access to Library Premises

This type of biometric application will not allow any unauthorized person to open the door. In this application, fingerprints of the authorized users will be scanned and stored for verification. This fingerprint identification is really a secure, convenient, and cost-effective alternative to passwords, badges, swipe cards and PINs. The biometric reader mounts on a wall near the library main door. These biometric fingerprint scanners offer various levels of authorization for an individual. This authorization includes a scheduling mechanism for allowing access for individuals based on the time of day. This can be applied for the whole library or at least for the computer rooms and server/ network stations to avoid unauthorized access. This system increases security levels more than a ID card or ID badge system as the fingerprint can t be lost or stolen. It also reduces overall cost in eliminating portable devices and reducing administrative time as well. Further, there is no need to track down or reprogramme ex-employee cards and ID badges. The system is convenient and there are no more fumbling for keys and ID cards. The member need not worry about misplacing their cards. The premises access devices can be networked together so that the system can be controlled and maintained from a central location.

Controlled Access to Library Network

Nowadays, most of the libraries are working on digital environment where the library is connected with a local area network, wide area network or Intranet of the organization. In a world of cyber crimes, it is the need of the hour for any library to have control over the member access to the library network. Libraries are providing user name and password to the members to make use of the library computer systems and networks. However, too many passwords or inappropriate passwords lead to security lapses in which virtual credentials are lost, forgotten and hacked. To overcome this problem, advanced biometric solution is available which ensures network authentication and safeguard the library network against unauthorized intrusion. This kind of biometrics system will protect individual PCs and network access. It also reduces the password reset requests from the users. The library administrator can be able to authenticate who is accessing a PC, network, and application with exceptional accuracy. It associates a single fingerprint with as many as passwords or PINs on a system. Users can log on automatically without having to type in username and password. It eliminates the security risks of written down passwords and PINs. Further, it protects passwords from most key logging viruses and prevent stolen or borrowed passwords. The system is easy to install, enroll fingerprint profiles and use. Since, most of the intellectual properties of academic and special libraries are residing on personal computers, servers and networks, it is the duty of the librarian to protect them from unauthorized access which may cause serious risks to the invaluable library assets.

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

Biometrics Applications: Prospects

Application of biometric technologies in libraries offers the following major advantages.

- Biometric traits can not be lost or forgotten while passwords can be lost or forgotten.
- Biometric traits are difficult to copy, share and distribute. Passwords can be announced in crackers websites.
- Biometrics require the person being authenticated to be present at the time and point of authentication.
- The systems are easy to manage and cost efficient
- It is convenient to the users as they no longer responsible for passwords, swipe or proximity cards, PINs or keys.

Biometrics Applications in Libraries: Problems

Though the biometrics technology provides a number of advantages, there are some disadvantages

too. The following are a select list of problems associated with the system.

- Biometric technology is inherently individuating and interfaces easily to database technology, making privacy violations easier and more damaging.
- Biometric systems are useless without a well-considered threat model.
- Biometrics are no substitute for quality data about potential risks.
- Biometric identification is only as good as the initial ID.
- Some biometric technologies are discriminatory.
- Biometric systems□ accuracy is impossible to assess before deployment
- The cost of failure is high.

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 simple fingerprint biometric system can be used, in place of the identity cards in the libraries. For this purpose a fingerprint scanner is necessary. The identity verification can be activated by comparing a user□ s pre- registered fingerprint patterns to the data read by a contact less fingerprint scan device linked to the libraries administrative terminal. The most common problems like unauthorized use of lost or stolen library cards, misuse of passwords (if you know the password of your friend you can access the PC or internet) to use the Internet, etc. The biometric authentication of users contributes to resource conservation also by reducing the number of cards issued. Even though the use of both CCTV and biometrics in libraries in India is in its infancy, it is necessary for all the libraries to switch over to these methods as early as possible. The personal computers of the future might include a fingerprint scanner, where one could place the index finger for the computer to assess the authenticity of the user. The computer would analyze the fingerprint to determine whether the user is authorized to access the data or not. At present many libraries are using bar-coding system, for data retrieval but with the increasing technology, we hope that it may not take very long time to go for biometric systems coupled with CCTV for better management of the libraries.

References

1. Biometric Consortium web site, Accessed on march 1st 2013 http://www.biometrics.org.

2. National Institute of Standards and Technology web site, Accessed on march 5th 2013 http://www.nist.gov.
3. National Security Agency web site, Accessed on march 5th 2013 http://www.nsa.org.
4. Common Biometric Exchange File Format (CBEFF) web site:, Accessed on march 1st 2013 http://www.nist.gov/cbeff.
5. NIST Biometric Interoperability, Performance and Assurance Working Group web site, Accessed on march 5th 2013 http://www.nist.gov/bcwg .
6. BioAPI Users and Developers Seminar web site, Accessed on march 1st 2013 http://www.nist.gov/bioapi-seminar
7. BioAPI Consortium web site, Accessed on march 1st 2013 http://www.bioapi.org
8. Teletrust web site: http://www.teletrust.de Accessed on march 1st 2013.
9. X9. F4 Working Group, ANSI X9 web site, Accessed on march 5th 2013 http://www.x9.org .
10. http://www.ibia.org Accessed on march 5th 2013
11. http://www.rfid-library.com/ Accessed on march 5th 2013.
12. Jain, A.K, Flynn P, & Ross A. " Handbook of Biometrics, Springer, 2007.
13. Jain, A.K, Ross, A.& Prabhakar S., " An introduction to biometric recognition" , IEEE Transactions on Circuits and Systems for Video Technology, Vol. 14,No. 1, pp.4-20, 2004.
14. Hong, L., Jain, A. K., & Pankanti, S. " Can Multi biometrics Improve Performance?" , Proc. AutoID□ 99, pp. 59-64, Summit(NJ), USA, Oct 1999.
15. Hong, L. & Jain, A. K. Integrating Faces and Fingerprints for Personal Identification, IEEE Trans. on Pattern Analysis and Machine Intelligence, Vol. 20, No. 12, pp.1295-1307, Dec 1998.
16. Lucence J. Jakarta Lucene Text Search Engine in Java, http://jakarta.apache.org/lucene/docs/index.html , Accessed on march 5th 2013).
17. "Fingerprint Technology Speeds School Lunch Lines, http://www.eschoolnews.com/showstory.cfm?ArticleID=2146 , eSchool News online, Accessed on feb 25th ,20013
18. "Best Practices Technology: This Minnesota High School Gives Fingerprint Scanning a Whorl" , http://www.eschoolnews.com/showstory.cfm?ArticleID=1277 , eSchool News online, Accessed on feb 25th ,2013.
19. F. Podio, J. Dunn, L. Reinert, C. Tilton, Dr. L. O'Gorman, M. P. Collier, M. Jerde, Dr. B. Wirtz, Common Biometric Exchange File Format (CBEFF), NISTIR 6529, January 3 2000.