A Prototype for Secure Digital Library Accessing System using Multimodal Biometric System

D. Gayathri[1], Dr.R. Uma Rani[2]

Assistant Professor, Dept. of Computer Science, Periyar University College of Arts and Science, Salem, India [1]

Associate Professor, Dept. of Computer Science, Sri Saradha College For Women, Salem, India [2]

Abstract: For some applications it is necessary that the user has to get authenticated himself either by using his password or any biometric features. No doubt that this gives protection against unauthorized entry in to the application or system. Secret information needs security in a multi user environment. Any automatically measurable, robust and distinctive physical characteristics or personal trait that can be used to identify an individual or verify the claimed identity of an individual, referred to as biometrics, has gained significant interest in the wake of heightened concerns about security and rapid advancements in networking, communication and mobility. Encryption alone is not sufficient in many cases. In this article we are providing a prototype for secure Digital Library accessing system with more than one Biometric features such as face and fingerprint.

Keywords: Web, Internet, SDLAS-MBS, UID, Multimodal Biometric

I. INTRODUCTION

A Digital Library is one in which collections are stored in digital formats (as opposed to print, or other media) and accessible via computers.]The digital content may be stored locally, or accessed remotely via computer networks. A digital library is a type of information retrieval system [6]. Many academic libraries are actively involved in building institutional repositories of the institution's books, papers, theses, and other works which can be digitized. Many of these repositories are made available to the general public with few restrictions, in accordance with the goals of open access, in contrast to the publication of research in commercial journals, where the publishers often limit access rights. Institutional, truly free, and corporate repositories are sometimes referred to as digital libraries. In this article we are providing a new prototype called Secure Digital Library Accessing System -Using Multimodal Biometric System (SDLAS-MBS).

II. BIOMETRICS

Biometrics are automated methods of recognizing an individual based on their physiological (e.g., fingerprints, retina, face, iris) or behavioral characteristics (e.g., gait, signature). The availability of inexpensive biometric sensors and computing power, it is becoming increasingly clear that widespread usage of biometric person identification is being stymied by our lack of understanding [1]. One of the main reasons for this popularity is, the ability of the biometrics technology to differences between an authorized person and an impostor who fraudulently acquires the access privilege of an authorized person.Even though, the biometric who fraudulently acquires the access privilege of an authorized person.Even though, the biometric identification systems out-perform peer technologies, the unimodal biometric systems have to contend with a variety of problems, namely, noisy data, intra-class variations, restricted degrees of freedom, non-universality and spoof attacks. Many of these limitations can be addressed by deploying multimodal biometric systems that integrate the evidences presented by multiple sources of information [2]. Further, multimodal biometric systems provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user. Thus a challenge-response type of authentication can be made possible by the use of multimodal biometric systems.

III. BACKGROUND RESEARCH

The increasing availability of the Digital Library on Internet has allowed tremendous amounts of data to be stored and accessed by the users of the web. This in turn has brought up an expectation to access data widely distributed in nature in an efficient manner. Only the authorized people are allowed to access digital library information system. The Internet users are becoming more concerned about security due to numerous coverage given to Internet threats aimed at causing financial losses and identity theft. As time goes on, more and more new technology will be developed to further improve the efficiency of communications. At the same time, breakthroughs in technology will provide even greater network security.

The enterprises stay on top of emerging technology, as well as the latest security threats and dangers, the benefits of networks will most certainly outweigh the risks. The three main components of secure system are[3]:

A. *Confidentiality*: This refers to the requirement for data in trait between communicating parties is not made available to third parties that may try to listen to a private conversation on the communication.

B. *Integrity*: If information has been tampered, this tampering should be detected.

C. *Authentication*: This refers to checking that, the user is authorized to access a service.

Authentication systems based on biometric features (e.g., fingerprint impressions, iris scans, human face images, etc.) are gaining widespread use and popularity. Often, vendors and owners of these commercial biometric systems claim impressive performance that is estimated based on some proprietary data.

Biometric technologies are critical to domains such as person authorization in e-banking and e-commerce transactions or within the framework of access controls to security areas [4]. These systems require not only advanced biometric technology interfaces but also the ability to deal with security and privacy issues. Integrating biometrics with access-control mechanisms and information security is another area of growing interest.

A generic biometrics system is shown in fig.1 as below.

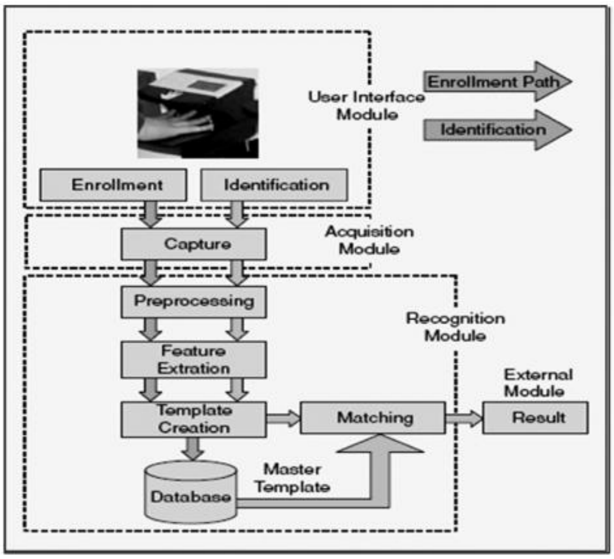

Fig.1 Generic Biometric system

The most widely used biometric technology is fingerprint recognition, based on the pattern of ridges on the finger tips. Finger print patterns have been used in law enforcement since the 1800s, and automated systems have been commercially available since the 1970s. Hand geometry, based on the dimensions of the fingers, joints, and knuckles, has been used for about 30 years to control access to secure facilities such as nuclear power plants. Fingerprints are used for personal identification for many decades and the matching (i.e., identification) accuracy using fingerprints has been shown to every high.

The other biometric technology is face recognition. Using human face as a key to security, the biometrics face recognition technology has received significant attention in the past several years [5]. Face biometrics is used for a wide variety of applications in both law enforcement as well as non-law enforcement. Facial recognition records the spatial geometry of distinguishing features of the face. As compared with other biometrics systems using fingerprint/palmprint and iris, face recognition has a distinct advantage because face images can be captured from a distance without touching the person being identified. For the above features webcam and fingerprint scanners with USB connections are portable.

IV. OVERVIEW OF SDLAS-MBS

The proposed model secures the sensitive data on Internet. The design on Secure Digital Library Accessing System - Using Multimodal Biometric System (SDLAS-MBS) consists of single fingerprint scanner device, webcam and event handler. It supports all the existing services and all other future communication services. To access sensitive data and secure transactions on Internet SDLAS-MBS will be used by the users with the help of fingerprint scanner and webcam devices.

As shown in Fig 2, initially the user has to login to the web site. Then click into the registration link to register new user with the fingerprint and face impression as input. This impression will be recorded in the database of the highly secured server. The web administrator has to follow all the steps as shown in Fig.2 to facilitate the Web services to new user to access the sensitive data or to do on-line transaction. The user cannot change or modify the finger and face impression without the permission of web administrator. The finger print scanner and the webcam for the service will activate only through the web page.

SDLAS-EH (Secure Digital Library Accessing System – Event Handler) with functionality defined as event handler will consists of set of protocols to provide necessary connection links between the client and server. The following steps followed:

- The user can login the site by giving their finger print and face impressions.
- In case of to use some sensitive data or to do some transactions on the web site the webcam device shall be automatically enable.
- And the message displayed on the screen to use the webcam device.
- Otherwise the webcam device will be disabled for the web services.

The SDLAS-EH protocols will use standard specific ports designated to secure the sensitive data on Internet which would be accepted and opened by all Telecom operators/ISPs.

V. SIMULATION OF SDLAS-MBS

In the SDLAS-MBS two simulations have been done. First simulation will be done at the registration time of new user and second at accessing data on Digital Library. In the first simulation the web administrator of the organization/institute will be included with the user. If the new user wishes to use the web services of the organization he/she has to complete all the formalities of the organization/institute. The organization/institute will set up some rules for them (For example their Permanent identity via voter identity card). After that user have to visit the web administrator appointed by the organization/institute to use the Internet services.

The **first** simulation will be applied at registration time for the Internet services and the modification time of secret key:

– Login to the Website
– Click on Registration link
– Finger Print Scanner and webcam device will enable
– The user will give his/her finger and face impression
– Images are captured and produce the unique code
– The code will be saved in the database
– Device will be disabled
– Then user will be allowed to access as in below fig.2.

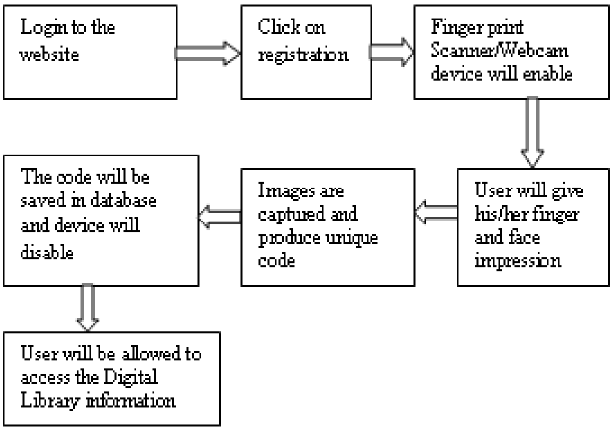
Login to the website
Click on registration
Finger print Scanner/Webcam device will enable
User will give his/her finger and face impression
Images are captured and produce unique code
The code will be saved in database and device will disable
User will be allowed to access the Digital Library information

Fig.2 Simulation at registration time

In the second simulation as shown in Fig.3, the user can use all the web services with this secret information. To use the web services the user have to use Internet connected computer machine with browser. The user has to input URL of the organization/institute in the address bar of the browser.

The **second** simulation will be applied at the time of accessing data on Digital Library as follows:

– Login to website
– on clicking link, the finger print scanner/webcam will enable
– user will use his/her specific finger for impression and face impressions
– images are captured and produce a unique code
– the device will send this code bit by bit to the server and device will disable
– matching process will take place
– if the code is matched, then the user can access the digital library data
– If the code is not matched, then the message like try again will appear and the scanner device will enable for the process again as in the below fig.3.

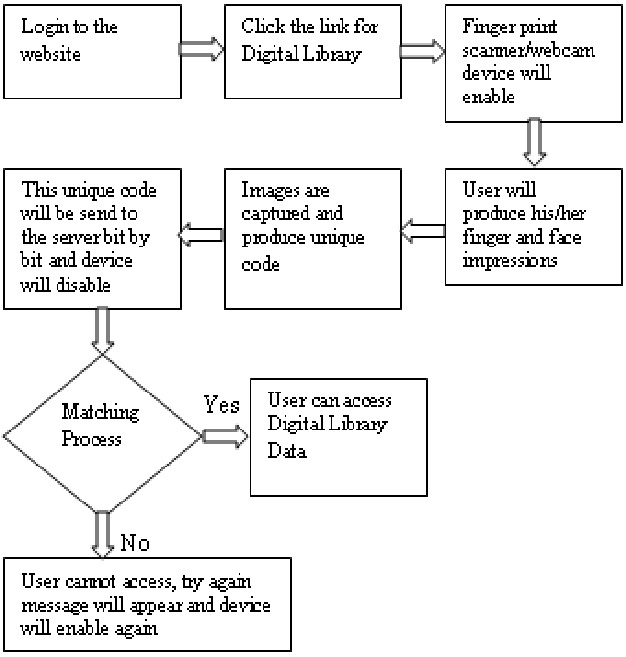
Login to the website
Click the link for Digital Library
Finger print scanner/webcam device will enable
User will produce his/her finger and face impressions
Images are captured and produce unique code
This unique code will be send to the server bit by bit and device will disable
Matching Process
Yes
User can access Digital Library Data
No
User cannot access, try again message will appear and device will enable again

Fig.3 Simulation at Digital Library Accessing time

VI. ADVANTAGES

The advantages of digital libraries as a means of easily and rapidly accessing books, archives and images of various types are now widely recognized by commercial interests and public bodies alike [6].Traditional libraries are limited by storage space. Digital libraries have the potential to store much more information, simply because digital information requires very little physical space to contain it. As such, the cost of maintaining a digital library can be much lower than that of a traditional library. A physical library must spend large sums of money paying for staff, book maintenance, rent, and additional books. Digital libraries may reduce or, in some instances, do away with these fees. Both types of library require cataloguing input to allow users to locate and retrieve material. Digital libraries may be more willing to adopt innovations in technology providing users with improvements in electronic and audio book technology. Conventional libraries may consider that providing online access to their OPAC catalogue is sufficient. An important advantage to digital conversion is increased accessibility to users. They also increase availability to individuals who may not be traditional patrons of a library, due to geographic location or organizational affiliation.

1) *No physical boundary*: The user of a digital library need not to go to the library physically; people from all over the world can gain access to the same information, as long as an Internet connection is available.

2) *Round the clock availability*: A major advantage of digital libraries is that people can gain access 24/7 to the information.
3) *Multiple access*: The same resources can be used simultaneously by a number of institutions and patrons. This may not be the case for copyrighted material: a library may have a license for "lending out" only one copy at a time; this is achieved with a system of digital rights management where a resource can become inaccessible after expiration of the lending period or after the lender chooses to make it inaccessible (equivalent to returning the resource).
4) *Information retrieval*: The user is able to use any search term (word, phrase, title, name, subject) to search the entire collection. Digital libraries can provide very user-friendly interfaces, giving clickable access to its resources.
5) *Preservation and conservation*: Digitization is not a long-term preservation solution for physical collections, but does succeed in providing access copies for materials that would otherwise fall to degradation from repeated use. Digitized collections and born-digital objects pose many preservation and conservation concerns that analog materials do not. Please see the following "Problems" section of this page for examples.
6) *Space*: Whereas traditional libraries are limited by storage space, digital libraries have the potential to store much more information, simply because digital information requires very little physical space to contain them and media storage technologies are more affordable than ever before.
7) *Added value*: Certain characteristics of objects, primarily the quality of images, may be improved. Digitization can enhance legibility and remove visible flaws such as stains and discoloration [7].
8) Easily accessible.

VII. CONCLUSION

The number of various sectors e.g. banking, on-line shopping, military etc. is facing the security problems regarding their sensitive database and transactions. We introduce a SDLAS-MBS in the context of fingerprint and face recognition. Online Web Services will be more secure using the Online Secure Digital Library Accessing System -Using Multimodal Biometric System (SDLAS-MBS). The proposed security model provides an interface to the authorized user's and reduce the threats regarding their sensitivity.

REFERENCES

[1] D. Gayathri & Dr. R. Uma Rani, "A Prototype for Secure web Access Model Using Multimodal Biometric System based on Fingerprint and Face Recognition", International Journal of Computer Science and Information Technologies, Vol.3(3), 2012.
[2] Mohamad Kashif Qureshi, " Biometric Technology : A Review", International Journal of Computer Science and Communication, December 2011.
[3] Cryptography and Network Security Principles and Practices- William Stallings, Fourth Edition.
[4] Anil Kapil and Atul Garg, "Secure Web Access Model for Sensitive Data", International Journal of Computer Science & Communications, June 2010.
[5] N.Radha & S.Karthikeyan, "An Evaluation of Fingerprint Security using Noninvertible Biohash", International Journal of Network Security & Its Applications, July 2011.
[6] European Commission steps up efforts to put Europe's memory on the Web via a "European Digital Library" Europa press release, 2 March 2006.
[7] Gertz, Janet. "Selection for Preservation in the Digital Age." *Library Resources & Technical Services.* 44(2) (2000):97-104

D. Gayathri has completed her M.C.A from J.K.K Nataraja College of Arts and Science, Komarapalayam, affiliated with Periyar University. She received her M.Phil Degree from Periyar University in June 2005. Now pursuing her Part time Ph.D., research in Periyar University, Salem. Now she is working as Assistant Professor, Department of Computer Science in Periyar University College of Arts and Science, Mettur Dam, Salem Dt. Her research area is of Information security.

Dr. R. Uma Rani has completed her M.C.A. from NIT, Trichy in 1989. She did her M.Phil. From Mother Teresa University, Kodaikanal. She received her Ph.D., from Periyar University, Salem in the year 2006. She has published around 50 papers in reputed journals and National and International Conferences. She has received the best paper award from VIT, Vellore, Tamil Nadu in an International conference. She was the PI for MRP funded by UGC. She has acted as resource person in various National and International conferences. Her area of interest includes Information Security, Data Mining, Fuzzy Logic and Mobile Computing. She is working as Associate Professor in Department of Computer Science, Sri Sarada College for women, Salem.