# A Prototype for Secure Web Access Model using Multimodal Biometric System based on Fingerprint and Face Recognition

[1]D. Gayathri, [2]R. Uma Rani
*[1]Department of Computer Science, Periyar University College of Arts & Science, Mettur Dam, Tamilnadu, India*
*[2]Department of Computer Science, Sri Sarada College For Women, Salem, Tamilnadu, India*

***Abstract*** **-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. The security of sensitive data on web is a key to its success. Multimodal biometrics is expected to be ultra-secure and reliable, due to the presence of multiple and independent- verification clues. In this study, a multimodal biometric system utilizing finger print and facial signatures has been considered. Face images are identified based on Eigen face approach using Principal Component Analysis. The success rate of multimodal system using finger print and face is higher when compared to individual unimodal recognition systems.**

***Keywords*— Web, Internet, SWAMP-MBS, SWAMP-EH, UID, Multimodal Biometric**

## I. Introduction

Web is a network of servers which are connected with each other via a common protocol and which makes web a universal repository of information. It provides unlimited and instantaneous access to information and communication. In addition to these, web links nearly all information residing on the Internet. The growth of the Internet and WWW(Web) has already had a significant impact on education, business, commerce, industry, banking, entertainment, government, shopping, communication, personal and working life etc. so the, Internet is becoming the most important medium for a large segment of the World's Population.

To be more useful today and in the future, the WWW(Web) needs to be secured. One has to authorize in many different places in order to use some services, applications or to get access to protected data. The user of the secure information must be accurately authenticated, properly authorized.

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. 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.

The security of sensitive data on web is a key to its success in any field which is using Web. Data protection measure means additional workload and responsibilities for users, system administrators, and security staff. In order to satisfy the basic needs of e-business, this paper puts forward a kind of secure Web Model, which includes secure authentication of the user.

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. 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.

## II. Background Research

The increasing availability of the 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. The type of access to such data, however, is currently in the form of non-database facilities.

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:

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. 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.

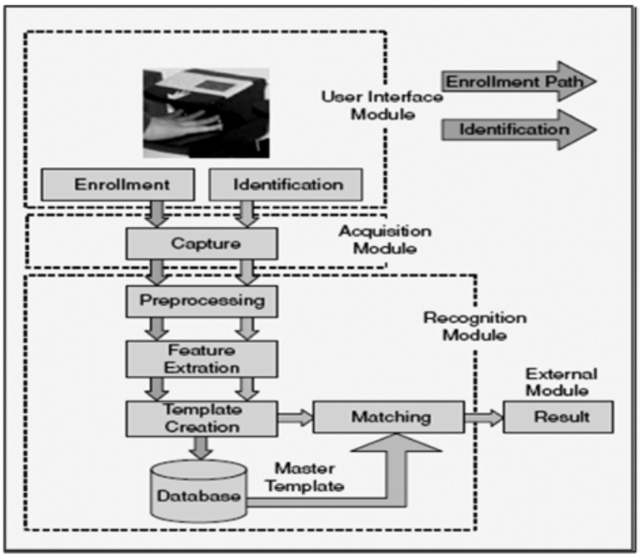

Fig.1 Generic Biometric system

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 another 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. 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.

## III. Overview Of Secure Web Access Model-Multimodal Biometric System(Swam-Mbs)

The proposed model secures the sensitive data on Internet. The design on SWAM-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 web SWAM-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 get permission from the web administrator to access the web services. For this he/she has to get permission from the web administrator for scanning of his/her finger impression and face impression. 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. 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.

**SWAM-EH** (Secure Web Access Model –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 SWAM-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.

## IV. Simulation Of Swam-Mbs

In the SWAM-MBS two simulations have been done. First simulation will be done at the registration time to access the web service and second at web service accessing time. 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 web services.

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

- Web administrator check the documents submitted by the user
- Create unique UID and password for the new user
- Set the secrets(e.g. Unique finger)
- Click on event for new user
- The finger print scanner device will enable
- The user will give his/her finger impression
- The device will scan it and produce the unique code
- The code will be saved in the database
- Device will be disabled
- By using the webcam, face impression is recorded
- A unique code will be assigned to user as in below fig.2.

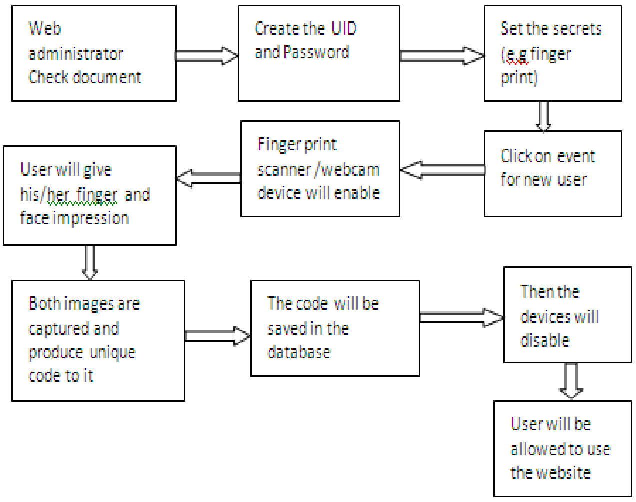
Web administrator Check document
Create the UID and Password
Set the secrets (e.g finger print)
Click on event for new user
Finger print scanner /webcam device will enable
User will give his/her finger and face impression
Both images are captured and produce unique code to it
The code will be saved in the database
Then the devices will disable
User will be allowed to use the website

Fig.2 Simulation at registration time

In the second simulation as shown in Fig. there is no need of web administrator to use the web services. 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 web accessing, here

- on clicking link, the finger print scanner/webcam will enable
- user will use his/her specific finger for impression and face impressions
- the device scan the unique secret key and produce a unique code
- the device will send this code bit by bit to the server
- then the device will disable and the application at server matches this code with the existing code in the database
- if the code is matched, then the user can access the sensitive data,
- if the is not matched, then the message like password incorrect, Try again will appear and the scanner device will enable for the process again as in the below fig.3.

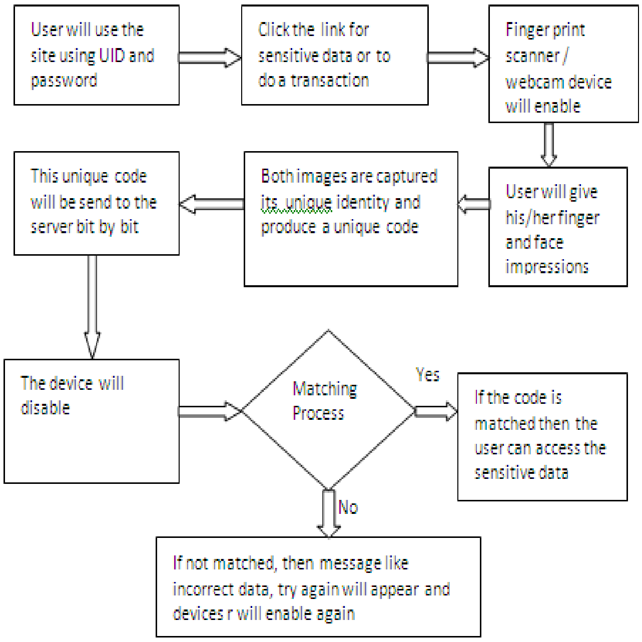
User will use the site using UID and password
Click the link for sensitive data or to do a transaction
Finger print scanner / webcam device will enable
User will give his/her finger and face impressions
Both images are captured its unique identity and produce a unique code
This unique code will be send to the server bit by bit
The device will disable
Matching Process
Yes
If the code is matched then the user can access the sensitive data
No
If not matched, then message like incorrect data, try again will appear and devices r will enable again

Fig.3 Simulation at Web Accessing time

## V. CONCLUSIONS

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 SWAM-MBS in the context of fingerprint and face recognition. Online Web Services will be more secure using the Online Secure Web Access Model-Multimodal Biometric System (SWAM- MBS). The proposed security model provides an interface to the authorized user's and reduce the threats regarding their sensitivity.

## REFERENCES

[1] Mohamad Kashif Qureshi, " Biometric Technology : A Review", International Journal of Computer Science and Communication, December 2011.

[2] Cryptography and Network Security Principles and Practices-William Stallings, Fourth Edition

[3] Anil Kapil and Atul Garg, "Secure Web Access Model for Sensitive Data", International Journal of Computer Science & Communications, June 2010.

[4] Raju Singh & A.K. Vatsa, "Confidentiality & Authentication Mechanism for Biometric Information Transmitted over Low Bandwidth & Unreliable Channel", International Journal of Network Security & Its Applications, March 2011.

[5] N.Radha & S.Karthikeyan, "An Evaluation of Fingerprint Security using Noninvertible Biohash", International Journal of Network Security & Its Applications, July 2011.

[6] Binsu C.Kovoor, Supriya M.H, and K.Poulose Jacob, " A Prototype for a Multimodal Biometric Security System based on Face And Audio Signatures", International Journal of Computer Science and Communication, June 2011.

[7] Sunil Kumar Singla & Ankit Sharma, "ECG as Biometric in the Automated World", International Journal of Computer Science and Communication, December 2010.

[8] Sri Shimal Das, Smt. Jhunu Debbarma, "Desinging a Biometric Strategy(Fingerprint) Measure for Enhancing ATM Security in Indian E-Banking System", International Journal of Information and Communication Technology Research, September 2011

[9] Gaurav Budjade, Ancy Abraham, Loveena Stephen and Imran Ali Mirza, " Secure and Effective Humanitarian Access Using Fingerprint", International Journal of Computing Technology and Information security", March 2011.

[10] D.Ashok Kumar, T. Ummal Sariba Begum, "A Novel design of Electronic Voting System Using Fingerprint", International Journal of Innovative Technology & creative Engineering", January 2011.

[11] Jitendra Kumar Gothwal, Shyam Sunder Yadav & Ram Singh, "Enhancing Fingerprint Authentication system Using Fragile Image Watermarking Technique", International Journal of Computer Science and Communication, December 2011.

[12] Uchale Bhagwat Shankar, "Image Compression Techniques", International Journal of Information Technology and Knowledge Management", December 2010.