IJCSC International Journal of Computer Science & Communication Vol. 1, No. 1, January-June 2010, pp. 13-16

Secure Web Access Model for Sensitive Data

Anil Kapil[1] & Atul Garg[2]

[1]Professor, [2]Lecturer, MMICT & BM, MM University Mullana, Ambala, Haryana, India,

Email: [1]anil_kdk@rediffmail.com, [2]atulgargmullana@yahoo.com

ABSTRACT

The security of sensitive data on Web is a key to its success. Biometric technologies use individual's unique, measurable biological and behavioural traits to automatically establish or verify user's identities. These 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.

Keywords: Web, Internet, SWAM, SWAM-M, SWAM-FH etc.

1. 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 [7]. 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. Every day, millions of internet users surf the internet for variety of reasons. As the increasing of Web users the security of data is plays an important role [8].

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 [9]. The user of the secure information must be accurately authenticated, properly authorized.

Biometrics is directly linked with the distinguishing characteristic of an individual, it has been advocated that biometric authentication will achieve increasing levels of assurance of identity verification [11]. Biometric technologies use individual's unique, measurable biological and behavioural traits to automatically establish or verify user's identities. 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 [10]. Biometrics-based personal identification techniques that use physiological or behavioural characteristics are becoming increasingly popular compared to traditional. One of the main reasons for this popularity is, the ability of the biometrics technology to difference between an authorized person and an impostor who fraudulently acquires the access privilege of an authorized person [1].

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. Fingerprint verification is an important biometric technique for personal identification. In this paper we are using a most popular fingerprint biometric for authentication. Fingerprints are distinct to each person and are different even in twins. Fingerprint patterns remain unchanged throughout the entire adult life and are easily produced for identification. It provides a rapid, convenient, and transparent data security service for Client/Server applications.

2. 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 [4].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 [5]. 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 [3]. The Three main components of secure system [2] are:

a. *Confidentiality:* This refers to the requirement for data in transit 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 [13].

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 [12].

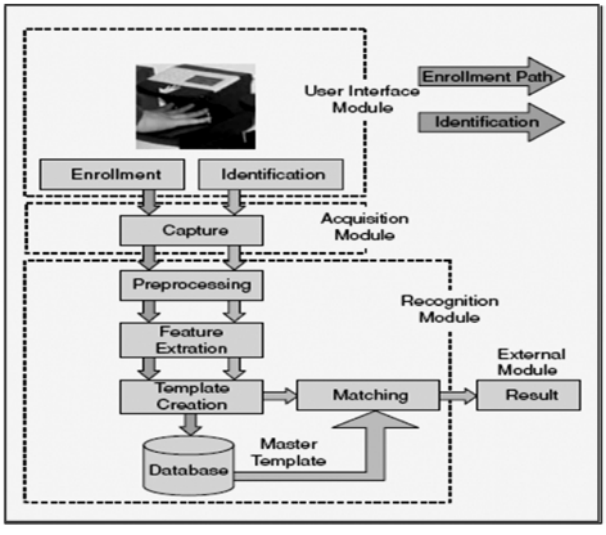

Fig. 2

The most widely used biometric technology is fingerprint recognition, based on the pattern of ridges on the fingertips. Fingerprint 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 be very high [6]. Different types of Fingerprint scanners are easily available in the market. Fingerprint scanners (as shown in Fig. 1) with USB connections are portable.

Fig. 1

The accuracy of the currently available fingerprint recognition systems is adequate for authentication systems involving a few hundred users. Multiple fingerprints of a person provide additional information to allow for large-scale identification involving millions of identities [14]. A generic biometrics system is shown in Fig. 2 [15]. In the enrolment stage, the biometric characteristic of an individual is first captured in the acquisition module, and then processed and stored in the prototype database. Similarly, in identification stage, biometric characteristic is captured and identified, and then the system makes a real-time respond according to recognition result [15].

3. OVERVIEW OF SECURE WEB ACCESS MODEL (SWAM)

The proposed model secures the sensitive data on Internet. The design on SWAM consists of single fingerprint scanner device and event handler. The SWAM-M (Secure Web Access Model - Module) will support all the existing services and all the other future communication services. To access sensitive data and secure transactions on Web SWAM-M will be used by the users with the help of fingerprint scanner device. As shown in Fig. 4, 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 new User-Id (UID), password and scanning of his/her finger/thumb 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. 3 to facilitate the Web services to new user to access the sensitive data or to do on-line transaction. The Web Administrator in the organization create the unique user-id (UID) and password for the new user. Later on the user can change the password, but can not change or modify the finger/thumb impression without the permission of Web Administrator. The user can access the Web site of the

organization via the UID and the password, but if one want to access the sensitive Web services then he/she has to use SWAM as shown in Fig. 4. The fingerprint scanner 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 consist of set of protocols to provide necessary connection links between the client and Sever. The following steps followed:

- The user can login the site in a normal manner,
- In case of to use some sensitive data or to do some transaction on the Web site the fingerprint scanner device shall be automatically enable.
- And a message displayed on the screen to use the finger print device (As given in Fig. 4).
- Otherwise the fingerprint scanner 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.

4. SIMULATION OF SWAM

In the SWAM 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 a new user wishes to use the Web services of the organization then 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 the secret key. In this simulation as shown in Fig. 3, the Web Administrator will (1) check all formalities, (2) create the UID and Password, (3) Set the Secrets (for e.g., unique finger) for the user's unique Identity and (4) Click on event for new user. After the event (5) Fingerprint Scanner Device will enable. The user will provide his/her (6) finger impression via authorized fingerprint scanner device. The fingerprint (7) device will scan the unique Identity and produce a unique code. The code will be (8) saved and send to the database of the server. The fingerprint scanner (9) device will disable. A UID (user-id) and Password will be (10) assigned to user.

In the second simulation as shown in Fig. 4 there is no need of Web Administrator to use the Web Services. The user can use all the Web Services with UID, Password and unique secret key. 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.

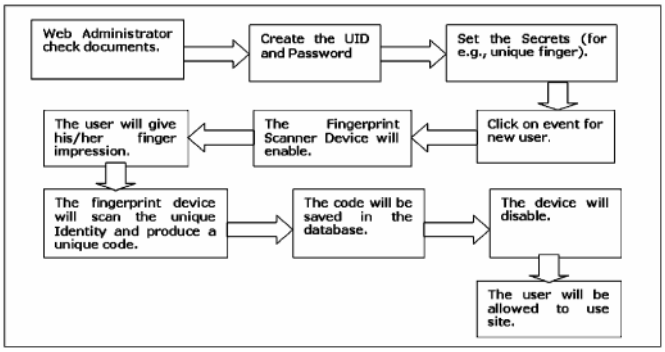

Fig. 3

The initial page of the site will be displayed on the screen. The user has to enter (1) UID and Password to access the contents of the site. As the user (2) click on the link on sensitive Web service or wish to do some transaction available on the Web page. The fingerprint scanner device available on the client side will be (3) enabling and a message (Please use your secret impression for your Identification) on the user's machine should be displayed. The user will use his/her a (4) specific finger for impression as a secret key. The fingerprint scanner device (5) scan the unique secret key and produce a unique code. The fingerprint scanner device (6) send this code bit by bit to the server. The fingerprint scanner (7) device will disable. An application at the server (8) matches this code with the existing code available in the database. The matched code (9) produce a transaction or sensitive data window to the user. The mismatch codes will (10) produced a message (Try again for secret key) to the user. And the finger print scanner device will be enable. The server accepts the code after generating a connection between the fingerprint scanner device connections. If the fingerprint scanner device did not found a message, then a message (Check your Device) should be displayed on the screen.

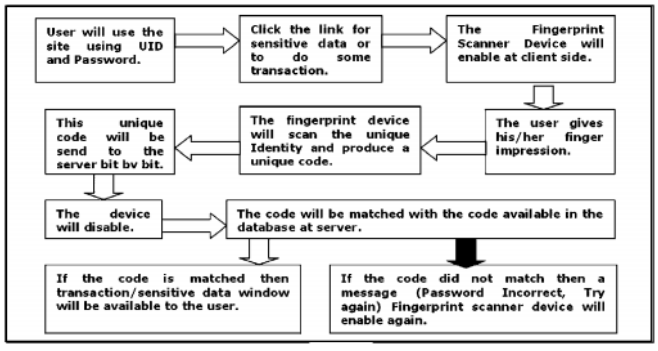

Fig. 4

5. CONCLUSION

The number of various sectors e.g. banking, on-line shopping, military etc. is facing the security problems regarding their sensitive database and transaction. We introduce a Secure Web Access Model (SWAM) in the context of fingerprint recognition. Online Web services will be more secure using the online Secure Web Access Model (SWAM). The proposed security model SWAM provide an interface to the authorized user's and reduce the threats regarding their sensitivity.

REFERENCES

[1] A. Jain, S. Pankanti, and R. Bolle, eds., Kluwer, Biometrics: Personal Identification in Networked Society, 1999.

[2] L. Josephine Mary, S.P. Rajagopalan, "Multi-Party Authentication Protocol for Web Services", *International Journal of Computer Science and System Analysis* **1**(2), July-December 2007; pp. 129-139.

[3] A Beginner's Guide to Network Security, Cisco Systems Copyright © 2001 Cisco Systems, Inc. All Rights Reserved.

[4] Cem Evrendilek, Query Optimization on the Web, Prosoft Info. Sys. and Consultancy Ltd. Izmir, Turkey

[5] "Internet Users More Savvy About Security", http://www.washingtonpost.com/wpdyn/content/article/2005/07/09/AR2005070900107.html?nav=rss_technology, July 10, 2005.

[6] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. New York: Springer Verlag, Jun. 2003.

[7] Mukesh Mohania, Vijay Kumart, Yahiko Kambayashil, Bharat Bhargavas, "Secured Web Access", 0-7695-1071-1/01 SI0 00 Q 2001 IEEE.

[8] T. Berners-Lee, R. Fielding, and H. Frystyk. Hypertext Transfer Protocol – HTTP/1.0, May 1996. RFC1945.

[9] K. Coe: Privacy, Security and E-Learning: AnIndustry Perspective,2004., http://www.nclbtechsummits.org/summit2/presentations/4.3.Coe.pdf

[10] Anil K. Jain, Sharath Pankanti, Salil Prabhakar, Lin Hong, and Arun Ross, "Biometrics: A Grand Challenge" Proceedings of the 17th International Conference on Pattern Recognition (ICPR'04)1051-4651/04 $ 20.00 IEEE.

[11] J. Ortega-Garcia, J. Bigun, D. Reynolds and J. Gonzalez-Rodriguez, "Authentication Gets Personal with Biometrics", *IEEE Signal Processing Magazine*, **21**, Issue 2, March 2004, pp. 50-62,.

[12] Anlong Ming and Huadong Ma, The Biometrics Grid: A Solution to Biometric Technologies, Published by the IEEE Computer Society, (vol. 8, no. 9), September 2007.

[13] Dass, S.C. Yongfang Zhu Jain, "A.K. Validating a Biometric Authentication System: Sample Size Requirements, Pattern Analysis and Machine Intelligence", *IEEE Transactions*, Dec. 2006, **28**, Issue: 12, page(s): 1902-1319.

[14] Anil K. Jain, Arun Ross, and Sharath Pankanti, "Biometrics: A Tool for Information Security", *IEEE Transactions on Information Forensics and Security*, **1**, No. 2, JUNE 2006.

[15] David Zhan, Wangmeng Zuo, "Computational Intelligence-Based Biometric Technologies", *IEEE Computational Intelligence Magazine* | May 2007.