Effective Method of Web Site Authentication Using Finger Print Verification

A. Yesu Raja and S. Arumuga Perumal

***Abstract*—Computer network is supported by network security, network security is facing a lot of problem in real world. The proposed authentication security system supports to avoid database hacking and spoof matching process of web-based network. The proposed security system combines the usage of both fingerprint biometrics and pin-number. The fingerprint biometrics includes the modules such as ridge enhancement, feature extraction, core detection and baseline matching. Applied biometric cryptosystem supports to save the fingerprint feature values and user mobile numbers as an encrypted format in the database. So the hackers can't steal the real feature database values. Corrupting the device through the masking techniques can be avoided using the multi security system. If hackers use masking image modal against database fingerprint feature value, it will give the matching ratio in between 80% to 90%. At that time a random pin will be generated and send to the registered mobile number, so the unauthenticated person can't access the device, at the same time the authenticated persons can login using the corresponding pin number. In the cloud network, the public cloud processes the encrypted database handling and the private cloud handles the decryption and the biometrics verification process. This multi modal authentication system surely increases the network security. This security system can be used in ATM, e-commerce website security and cloud network security.**

***Index Terms*—Fingerprint, encryption, enhancement, password, mobile, networking, verification.**

I. Introduction

The website based substantiation aspect implements website based substantiation, which is also known as Website Validation Proxy. You can use the website based substantiation feature to validate end users on host systems that don't run the IEEE 802.1X supplicant. User can be configuring the website based substantiation feature on Layer 2 and Layer 3 interfaces.

When a user initiates an HTTP session, the website based substantiation feature intercepts access HTTP packets from the host and sends web-design login page to the user. The user keys in their credentials, which the website based substantiation feature sends to the XXX server for validation. If the validation succeeds, website based substantiation sends a Login-Successful web-design page to the host and applies the right to use policies returned by the XXX server. If the validation fails, validation based validation feature sends a Login-Fail web-design page to the user, which prompts the user to retry the login effort. If the user exceeds the highest number of failed login attempts, website based substantiation sends a Login-Expired web-design page to the host process and the user can located on a watch list for a waiting time.

Website based multi-way substantiation is commonly found in electronic computer substantiation, where basic substantiation is the method of a requesting entity presenting some indication of its identity to a second entity. Website based multi-way substantiation seeks to lessen the probability that the requestor is presenting fake substantiation of its identity. The number of factors is significant, as it implies a high probability that the owner of the identity substantiation indeed holds that identity in a different realm. In realism, there are more variables to believe when establish the relative guarantee of honesty in an identity declaration than just how many factors are used [1].

Website based multi-way substantiation is often confused with other forms of substantiation. Website based multi-way substantiation requires to utilize of two of the three substantiation factors. The factors are recognized in the principles and system for right of admission to U.S. Federal Government systems.

Website based multi-way substantiation is not a novel concept, having been used all through history. When a bank client visits a neighboring automated teller machine (ATM), a substantiation thing is use a physical ATM card the client slides into the ATM machine. The next thing is the customer enters the PIN number through the keyboard. Without the corroborate substantiation of these factors, substantiation does not succeed. This situation illustrates the fundamental concept of the majority Website based multi-way substantiation systems: the grouping of a information factor and a control factor.

Website based multi-way substantiation (or multi-factor substantiation) is sometimes confused with "strong substantiation"; however, "strong substantiation" and "multi-factor substantiation" are basically dissimilar processes. Soliciting a variety of answers to challenge question may be measured strong substantiation but, except the process also retrieves, it would not be considered Multi-way substantiation. The United State Federal Financial Institutions Examination Council issue supplemental regulation on this topic in August 2006, in which they clarify, true multifactor substantiation requires the use of declaration from two or more of this category of factor. Using many solutions from the matching category, would not comprise multifactor substantiation [2]."

Manuscript received May 9, 2013; revised July 9, 2013.

A. Yesu Raja and S. Arumuga Perumal are with Research Scholar, Department of Computer Science and Research, S.T. Hindu College, Nagercoil, Tamil Nadu, South India (e-mail: a_yesuraja@yahoo.co.in, visvenk@yahoo.co.in).

II. Related Work

The existing research work found some password authenticated group key exchange protocol is used for the

DOI: 10.7763/IJCEE.2013.V5.769

secured communication of mobile ad-hoc networks. It is concerned with improving the security of the NEKED protocol. NEKED protocol is vulnerable not only to an attack against backward secrecy but also to an attack against password security. Same pair-wise key is used for two consecutive runs of setup and join. Same pair-wise key is used in computing two related parameters [3]. Proposed an Improved password based substantiation protocol for network security. Use PAKE protocol which is vulnerable to server compromise attack. This is meets some draw backs threats due to the low entropy of passwords, Amplified password file is impractical [4]. The proposed an improvement GPAKE protocol. This is securely established a session key between the client and the gateway. This still able to gain information of password by performing an undetectable on-line password guessing attacks [5]. It examines the passwords, security tokens and biometrics based on their characteristic for substantiation. Analysis is done based on knowledge based, object-based and id based substantiation. This is mainly meet this draw backs that are Multi-passwords are less security, Tokens are inconvenient and costly and Inconvenient the user by many false non matches [6]. The invented technology provides a solution for the online learning environment using biometric based substantiation. Using methodologies are handles five step processes to ensure the user substantiation but the user must be certified frequently for substantiation.

III. Proposed System

In this paper we mainly focus the new authenticated approach for web-based multi level substantiation compare to obtainable technologies. Fingerprint based authentication system is integrate with web browser and mobile device. In this method the following factors such as FAR, FRR and EER are analyzed and implemented the proposed work to give better result compare to the other exiting methodologies. At the same time the hackers using mask fingerprint techniques can generate unauthorized accessing problem. The above innovative system avoiding this type of issues and create effective substantiation method. The Authentication Architecture as explain in Fig. 1.

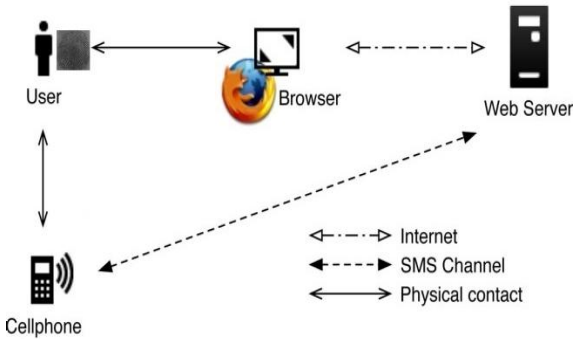

Fig. 1. Architecture of security system.

In this paper mainly focus two phases such as Enrollment and Authentication. In Fig. 2 clearly state the visual representation of the proposed methodology.

A. Enrollment

This enrollment process is mainly included for image accusation, fingerprint features extraction and user mobile number are stored in encrypted form to the particular database. This section is used to do the registration process.

1) Image Accusation: Read the fingerprint image from biometric scanner of the user side. This device is used for convert the scanned image into digital form.
2) Fingerprint Enhancement: Various types of biometric scanner are used for image accusation. Some devices are generating more noise in the fingerprint image. These types of fingerprint images are generating FAR are very high. So we are using noise reduction and enhancement techniques. Gabor based ridge enhancement method is supporting for enhance the finger print ridges. So this type of fingerprint enhancement techniques is improving the TAR level [7].
3) Feature Extractor: Fingerprint features are used to fingerprint matching process. Feature extractor includes various processes.
   a) Binarization: This process converts the Fingerprint of various intensity levels to binary levels ie. 0 or 1. Using threshold, the systems convert the enhanced fingerprint image to binarization image.
   b) Thinning: This operation can be applied only for binary images. Morphological operation is supported to convert binary image into thinning image.
   c) Core point Detection: Apply ridge orientation based core point detection algorithm, to finding the core point in the fingerprint image.
   d) Minutia Extraction: Three types of minutiae are available in the fingerprint image; they are Bifurcation, Ridge End and Dots. Template Based minutia extraction method is used to extract the bifurcation minutia. Also the same method is used to extract the ridge-end minutia.
4) Cryptosystem: AES algorithm is used for extracted fingerprint features and mobile numbers. These are converted to encryption format to store the particular database [8].

B. Authentication

This is mainly includes two types of authentication, one is fingerprint matching and another one is mobile pin number matching. Pin number matching process is supported with mobile network. Authentication process also includes, fingerprint accusation, enhancement and features extraction. The user is given the finger print to the system via fingerprint reader. The query fingerprint is matched to the database fingerprint. If the query fingerprint is matched above 90% accuracy at that time the authentication successfully logged. The matching accuracy is below 90% and above 80% at that time the one time password is generates and the password is send to the user mobile. The user receive the password and enter via internet browser, one time password is same at that time login is successful. The one time password is wrong at that time the login process is failed. The fingerprint matching accuracy below 80% at that time the login process is failed.

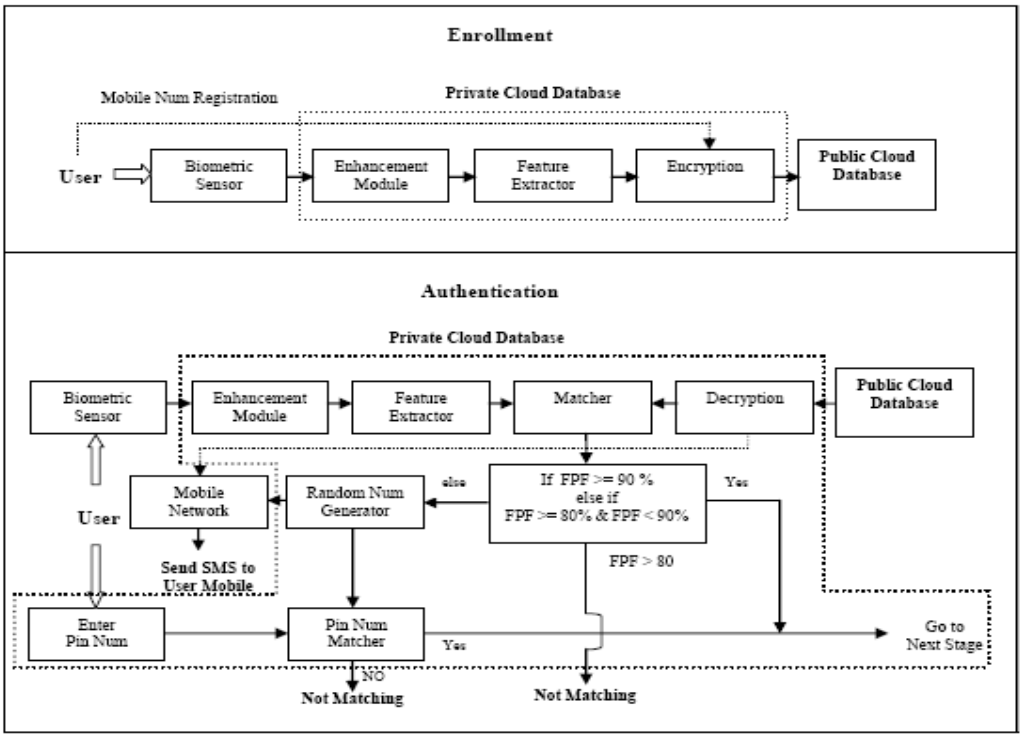

Fig. 2. Data flow diagram.

Database: Database has the fingerprint features and user mobile numbers, in encrypted format. At the time of Fingerprint matching, encrypted features are converted to decrypted format.

1) Fingerprint Matcher: Base Line Matching algorithm is used to match the query fingerprint features and decrypted database fingerprint features. If the matched result is given more than or equal 90% (FPF >= 90), at that time the authenticator allow the user to next stage. If the Matched result is given below 90% and above 80% or equal (FPF > 90 & FPF <=80 %), at that time the process will be go to the random number generator. This process is second level security. If the matched result is given below 80% (FPF > 80) at that time failure message will be displayed such as "fingerprint is not matched to the database", so the user is not an authenticated person.
2) Random Num Generator: Random Num Generator generating a random number and send the numbers to two areas. One is pin number matcher and another one is send to mobile network. Mobile network receives the pin number.
3) Pin Num Matcher: The pin number matcher receives the original pin number from random generator and check the pin number from user. If the pin numbers are same at that

Then the mobile network sends the pin number through SMS. The corresponding mobile number is taken form database. A user receives the pin number and enters in the appropriate area.

IV. Performance Analysis

The performance evaluation was done based on the proposed system consisted of 50 participants, each performing registration and login process. All participants suggested that the registration and login process are more user friendly. They accepted the high level security of the proposed system. The participants are chosen by the mixing category of computer familiar and computer non-familiar. Both categories of people can operate the system in easy manner. Many participants suggested the proposed system was highly suited for online banking, e-purchases and military related websites.

This new method was implemented and tested in windows operating system. TCP/IP network is chosen for applying this new concept. For Database handling SQL Server database is used. The SMS, Mobile Device, encryption methods and finger print recognition provides high security. The finger print recognition provides high security for this system. The False Acceptance Ratio (FAR) is calculated as Table I. Using this fingerprint enhancement algorithm user getting the False Acceptance Ratio is very minimum.

TABLE I: The False Acceptance Ratio

Finger	FAR
Good	5.3%
Better	7.8%
Worse	12.5%

The SMS Delay constraint is also considered for analyzing. From SMS Delay analysis it can be noticed that it is not a time taking process. The Table II is indicating about Average time taken and minimum and maximum time taken for login process.

TABLE II: Performance Overhead

	LOGIN	
Seconds	**SMS Delay**	**Total**
Avg Time	8.6	22.7
Min ,Max	7,11	20,35

V. Conclusion

All existing applications are having different types of security. Login security and data robbery are most important areas in internet security. Nowadays we are using security system in interdisciplinary areas example, ecommerce, internet banking, cyber security, cloud computing network etc.

But these all are met dissimilar difficult in login security. Because all existing login security systems are login to the particular site with username and password, higher security is supported to mobile pin generation. Some network hackers are burglary the login and password and they are misuse the another person account.

The propose system supports higher security to the login system because of username, password and fingerprint utilization. So this type of security is shunning the unauthorized login. Then this system stores all details in server to encryption model. Some time the hackers are create the duplicate finger print, at that time the multi security system is activate which is strengthened by pin number verification with mobile.

References

[1] A. Moini and A. M. Madni, "Leveraging Biometrics for User Authentication in Online Learning: A Systems Perspective," *IEEE Systems Journal*, vol. 3, no. 4, December 2009.

[2] H. M. Sun, Y. H. Chen, and Y. H. Lin, "oPass: A User Authentication Protocol Resistant to Password Stealing and Password Reuse Attacks," *IEEE Transactions on Information Forensics and Security*, vol. 7, no. 2, April 2012.

[3] J. Nam, J. Paik, U. M. Kim, and D. Won, "Security Enhancement to a Password-Authenticated Group Key Exchange Protocol for Mobile Ad-hoc Networks," *IEEE Communications Letters*, vol. 12, no. 2, February 2008.

[4] T. Kwon, Y. Park, and H. J. Lee, "Security Analysis and Improvement of the Efficient Password-based Authentication Protocol," *IEEE Communications Letters*, vol. 9, no. 1, January 2005.

[5] J. W. Byun, D. H. Lee, and J. I. Lim, "Security Analysis and Improvement of a Gateway-Oriented Password-Based Authenticated Key Exchange Protocol," *IEEE Communications Letters*, vol. 10, no. 9, September 2006.

[6] O'Gorman, "Comparing Passwords, Tokens, and Biometrics for User Authentication," in *Proc. of the IEEE*, vol. 91, no. 12, December 2003.

[7] L. Hong, Y. Wan, and A. Jain, "Fingerprint Image Enhancement: Algorithm and Performance Evaluation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 20, no. 8, August 1998.

[8] M. Mozaffari-Kermani and A. Reyhani-Masoleh, "Efficient and High-Performance Parallel Hardware Architectures for the AES-GCM," *IEEE Transactions on Computers*, vol. 61, no. 8, August 2012.

A. Yesu Raja received his M.C.A. and M.Phil Computer Science degree from Manonmaniam Sundranar University with first class. Currently he is a research scholar of S. T. Hindu College and he is also doing part time work in Ann Soft Systems, Nagercoil as a Programmer. He is the organizing secretary of Indra Gandhi International Research Networks (IGIRN). He has presented number of papers in National and International Conferences and also attended Workshops and Seminars. He has also organized many International Conferences. His area of research is Network Security with Biometrics. His trust area is Network Security and Image Processing.

S. Arumugaperumal is serving as an associate professor and HOD of Computer Science and research for the Last 25 years. He served as an EC member, Vice-Chairman, Chairman-Board of Examinations of IETE at Trivandrum center. He got best teacher award, IETE Brig M.L. Anand award and CSI academic excellence award. He as organized many IETE technical events,. He has authored many books and served as a chairman cum member in BOS for computer science in universities and autonomous colleges. He is an educationalist, academician and a researcher. He has delivered number of invited talks. He has visited Malaysia, Singapore, and Hongkong.