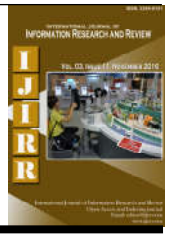
IJIRR

International Journal of Information Research and Review
Vol. 03, Issue, 11, pp. 3016-3018, November, 2016



Research Article

ACHIEVING PRIVACY PROTECTION OF MULTIFACTOR AUTHENTICATION IN CLOUD

[1,*]Ms.Teena Joseph and [2]Dr.Latha Parthiban

[1]Research Scholar, St.Peters University, Tamil Nadu, India
[2]Assistant Professor, Department of Computer Science, Pondicherry University Community College

ARTICLE INFO

Article History:

Received 18th August, 2016
Received in revised form
22nd September, 2016
Accepted 25th October, 2016
Published online November, 30th 2016

Keywords:

Cloud Storage,
Biometric,
Authentication

ABSTRACT

Recent day online transaction will be affected by various types of attackers. To protect our password from hacker or attacker, an efficient security mechanism is used. The main aim of this paper is to provide the security for the online environments using multifactor authentication like passwords, fingerprint etc. For this purpose this work proposes a virtual password concept involving a small amount of human computing to secure users' passwords in online environments. Here differentiated security mechanisms is proposed in which a user has the freedom to choose a virtual password scheme ranging from weak security to strong security. The tradeoff is that stronger schemes are more complex. Among the schemes, we have a default method (i.e., traditional password scheme), a system recommended function, a user-specified function, a user-specified program, and so on. A function/program is used to implement the virtual password concept by trading security for complexity by requiring a small amount of human computing. According to the fingerprint based security process can ensure the security in an online. The experimental result shows that, users can securely survey in the online transaction in an efficient and easy manner.

INTRODUCTION

Most current commercial websites will ask their users to input their user identifications (IDs) and corresponding passwords for authentication. Phishes attempt to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an electronic communication. Password Stealing Trojan is a program that contains or installs malicious code. There are many such Trojan codes that have been found online today. Key loggers capture keystrokes and store them somewhere in the machine, or send them back to the adversary. Shoulder surfing is a well-known method of stealing other's passwords and other sensitive personal information by looking over victim's shoulders while they are sitting in front of terminals. This attack is most likely to occur in insecure and crowded public environments, such as an Internet Café, shopping mall, airport, etc. A one-time password (OTP) does not use a static password, and therefore can prevent replay attacks. The proposed password scheme is dynamic and requires a user to make some computations. It was found that most of the respondents could complete the single digit calculation easily without help from the calculator.

Corresponding author: Ms.Teena Joseph,
Research Scholar, St.Peters University, Tamil Nadu, India.

The most of the surveyed people showed their need for more secure internet with the cost of spending a little extra time.

Problem Description

In the proposed system, one more new feature is added with the existing concept in order to offer more security in online environments. In addition the fingerprint based security during the registration process is also provided. So, the proposed concept can provide more security when compared to the existing concept. In registration time the user set the fingerprint. Then every login session they provide the fingerprint, if the fingerprint is not match the user can't perform the transactions. For fingerprint matching we first get the input from the database, then do the image enhancement named as pre-processing and then it can be performs the matching. For fingerprint matching the correlation based matching algorithm is used. After the successful completion of matching the user can enter into the online environment and perform the online transaction using online banking.

Problem Definition and Working Methodology

Registration

The primary process of this work is to enroll the details of every user whose need to enter into the online process.

For that they need to give the personal details like name, date of birth, user id and password. These all are the general enrollment in the online process. In this process the activity of fingerprint enrollment is included. Those details are enter into the process and stored in a database. The fingerprint can be stored and it can be retrieved during the time of login.

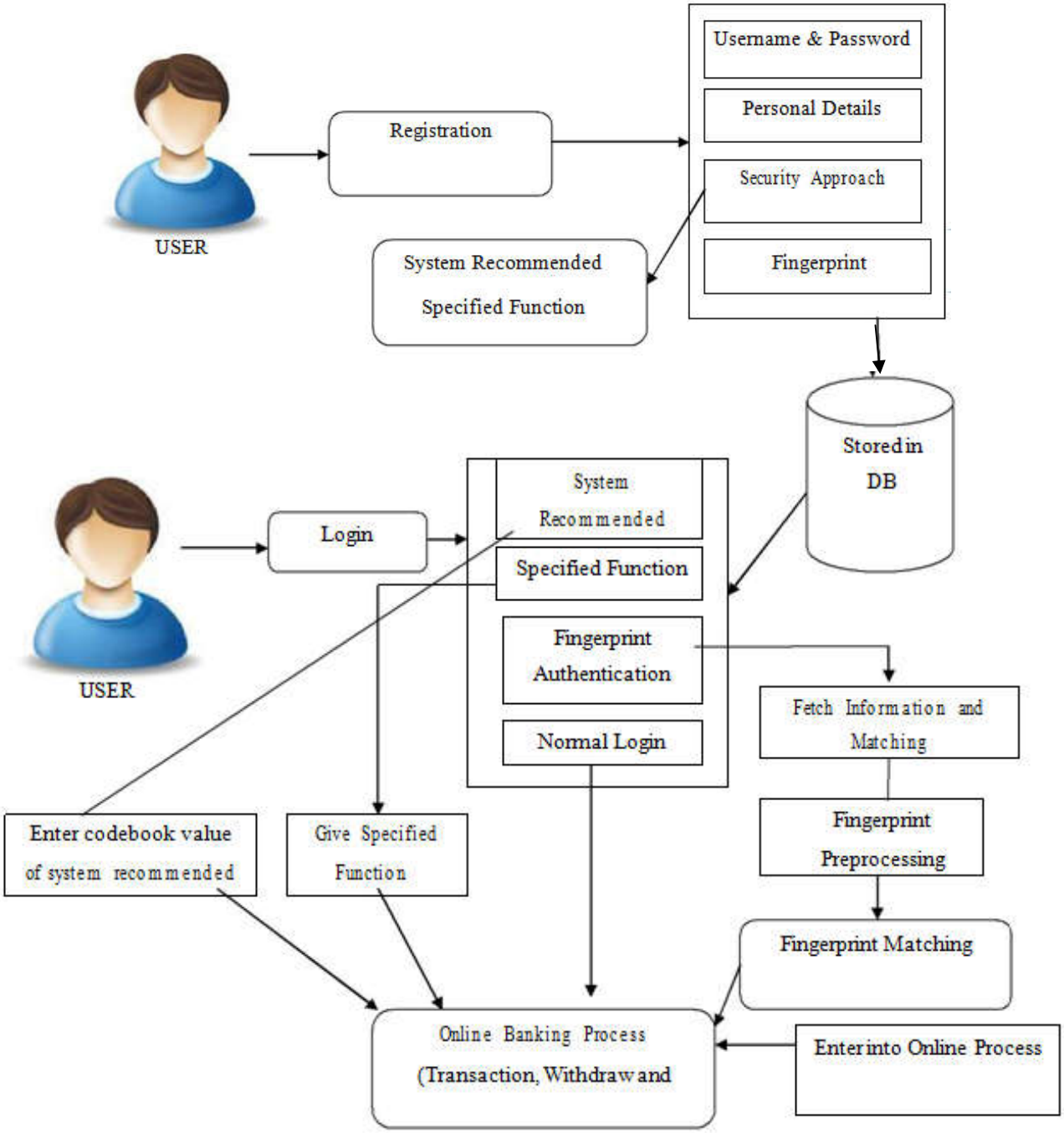
Fingerprint Pre-Processing

The fingerprint pre-processing can be done in the internal process of storage and retrieval process. Here, first, select the fingerprint to process, image enhancement can be performed. Additional process of image enhancement we can process the image conversion if the image as a grayscale. After that performing the structural extractions and then the image can be stored in the database.

Fingerprint Matching

The fingerprint matching will be done with the help of database. At the time user login they can enter the username and password and also their fingerprint for providing more security into the online. The given fingerprint image can be loaded into database for matching process. In that it could be processed at image enhancement and all the fingerprint pre-processing.

The fingerprint matching can be done with the help of correlation based matching algorithm. After that the finger can be matched with the stored image. If the finger can be matched into that stored image the user can enter into the online process otherwise they will not entered into the online process.



Online Banking Process

The final process is to enter into the online process. In online the user can purchase something for that they have to pay the amount. The amount has to be processed with the help of online banking. In online banking, the operations of amount transaction, withdrawal of amount and also the deposit of the amount are performed. These processes are performed in the online banking by the users. Figure 1.1 shows the system design of the proposed work.

DISCUSSION

In this work, for fingerprint matching the correlation based matching algorithm is used. In correlation-based fingerprint matching, the template and query fingerprint images are spatially correlated to estimate the degree of similarity between them. If the rotation and displacement of the query with respect to the template are not known, then the correlation must be computed over all possible rotations and displacements, which is computationally very expensive. Correlation step to ascertain the quality of each minutia match. The gray-level information of the pixels around the minutia points contains richer information about the local region than the attributes of the minutia points. Hence, the spatial correlation of regions around corresponding minutia points is a good measure of the degree of similarity between them. The correlation-based fingerprint matcher selects certain distinctive regions in the template fingerprint image and searches for those regions in the query image. Fingerprint authentication" describes the process of obtaining a digital representation of a fingerprint and comparing it to a stored digital version of a fingerprint. Electronic fingerprint scanners capture digital "pictures" of fingerprints, either based on light reflections of the finger's ridges and valleys, ultrasonic's, or the electrical properties of the finger's ridges and valleys.

These pictures are then processed into digital templates that contain the unique extracted features of a finger. These digital fingerprint templates can be stored in databases and used in place of traditional passwords for secure access. Instead of typing a password, users place a finger on an electronic scanner. The scanner, or reader, compares the live fingerprint to the fingerprint template stored in a database to determine the identity and validity of the person requesting access. The plusID security device from Privaris is a personal, mobile biometric fob, which uses fingerprint biometrics to secure access to buildings/ facilities (physical access) and computers and networks (logical access). plusID has a self-contained fingerprint scanner and secure processor to verify its owner's identity using fingerprint authentication. The device protects personal privacy and enhances user confidence by performing all biometric processing on the device and eliminating the need for a database of biometrics. Fingerprints are not - and can never be - released or transmitted from the device.

Conclusion

This work discusses of the challenges of protecting user's passwords on the internet and presented some related work in this field. How to prevent user's passwords from being stolen by adversaries is discussed.

Using fingerprint concept user can access the online transaction in efficient and secure manner. In existing system using virtual password for online transaction, it is complex to use and user must have the knowledge to generating the virtual password. But human fingerprint is one of the effective ways to use the online transaction. Fingerprint matching done by correlation based algorithm. After matching the fingerprint user can access their account. In this work achieving a better performance compared to other traditional techniques.

REFERENCES

Ampah, N., Akujuobi, C., Alam, S. and Sadiku, M. 2011. "An intrusion detectiontechnique based on continuous binary communication channels,"Int. J. Security Netw., vol. 6, nos. 2–3, pp. 174–180.

Chen, H. and Sun, B. 2011. "Editorial," Int. J. Security Netw., vol. 6, nos. 2–3,pp. 65–66, 2011. M. Barua, X. Liang, R.

Cheng, N., Govindan, K. and Mohapatra, P. 2011."Rendezvous based trustpropagation to enhance distributed network security," Int. J. SecurityNetw., vol. 6, nos. 2–3, pp. 101–111, 2011.

Chow, S. S. M. and Yiu, S. 2011."Exclusion-intersection encryption," Int. J.Security Netw., vol. 6, nos. 2–3, pp. 136– 146.

Desoky, "Edustega: An education-centric steganography methodology,"Int. J. Security Netw., vol. 6, nos. 2–3, pp. 153–173, 2011.

Fathy, A., ElBatt, T. and Youssef, M. 2011. "A source authentication schemeusing network coding," Int. J. Security Netw., vol. 6, nos. 2–3, pp. 112–122.

Jaggi, N., Reddy, U. M. and Bagai, R. 2011. "A three dimensional senderanonymity metric," Int. J. Security Netw., vol. 6, nos. 2–3, pp. 77–89.

Liu, L., Xiao, Y., Zhang, J., Faulkner, A. and Weber, K. 2011. "Hiddeninformation in microsoft word," Int. J. Security Netw., vol. 6, nos. 2–3,pp. 123–135, 2011.

Lu, and X. Shen, "ESPAC: Enabling securityand patient-centric access control for eHealth in cloud computing," Int.J. Security Netw., vol. 6, nos. 2–3, pp. 67–76, 2011.

Sharma, M. J. and Leung, V. C. M. 2011. "Improved IP multimedia subsystemauthentication mechanism for 3G-WLAN networks," Int. J. SecurityNetw., vol. 6, nos. 2–3, pp. 90–100.

Walker, D. and Latifi, S. 2011"Partial Iris recognition as a viable biometricscheme," Int. J. Security Netw., vol. 6, nos. 2–3, pp. 147–152.

Zhao, X., Li, L. and Xue, G. 2011. "Authenticating strangers in online socialnetworks," *Int. J. Security Netw*., vol. 6, no. 4, pp. 237–238.

****