IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 1, Ver. IV (Jan.- Feb. 2018), PP 22-25
www.iosrjournals.org

Enhancing Security of Internet Banking Using Biometrics

Darshan Khachane, Yatharth Sant, Yogesh Sachan, Ajeet Ghodeswar
Computer Engineering, Atharva College of Engineering, Mumbai University, India
Corresponding Author: Darshan Khachane

Abstract: *Internet banking system facilitates the banking services via internet using web-based application. Here user id and password are the two parameters used for authenticating the user. This paper highlights the technologies used in internet banking and aims for improving the security associated with the internet banking services. In addition to current security, biometric of the user can be used. And this communication can be secured by using Cryptography and Steganography. Cryptography can be implemented by Transpositional pixel by spiral method and Steganography by LSB replacement method.*
Keywords - *Biometric authentication, Cryptography, LSB, Steganography, Transposition pixel.*

Date of Submission: 13-02-2018 Date of acceptance: 01-02-2018

I. Introduction

Online banking gives you the ability to manage money online with your computer. There's no need to visit a bank branch, and you can do what you need to do when it's most convenient for you. Money is increasingly electronic. The way of payment has largely shifted from cash to electronic payment, which are user friendly and inexpensive. They also facilitate easy accounting. Though it is easy and convenient to use internet banking, since it uses internet its security can still be compromised. There are many cybercrimes prevalent. Some of the examples are:

1. Fraud: Any dishonest misrepresentation leads to encourage loss, which is computer fraud. Fraud results in altering computer input in unauthorized manner, destroying or stealing output, deleting data, misusing system tools and software packages[10].
2. Phishing: It is an attempt to acquire information which is sensitive to get the money indirectly like acquiring passwords, username, credit card details by disguising as a trustworthy entity for malicious reasons[10].

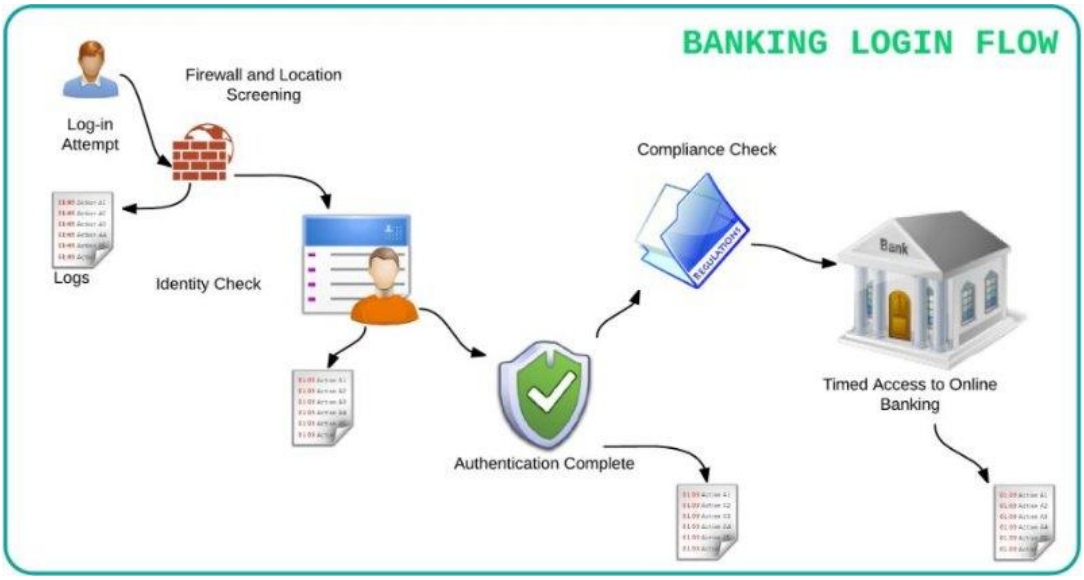

Figure 1: Login Flow of Internet Banking

The existing system makes use of username and password which is easy to hack even though encryption is used in the back end. The reason for such vulnerability in existing system is that on hacking a user's session the intruder can get a complete control over the system. In order to incorporate additional security some devices which are capable to connect to the internet can be used. Such devices are already equipped with

computational intelligence and are called as IOT devices. One way of making the system secure is by using biometrics with the help of IOT devices.

II. Related Works

The idea of Internet banking has been concurrently emerging with the advancement of the world wide web. Programmers working on banking data bases came up with ideas for online banking transactions, sometime during the 1980s. The prolific process of evolution of these services were probably triggered after many companies started the notion of online shopping. The online shopping promoted the use of credit cards through Internet. Many banking organizations had already started creating data ware housing facilities to ease their working staffs. The evolution of these databases were widely used during the advancement of ATM's.

In the beginning of 1980s, finance and banking organizations in United States and Europe initiated reminiscent programming experiments and researches on the idea of 'home banking'. In early 80's when internet and computers were in the developing stage, 'home banking' basically made use of fax machines and telephones to facilitate their customers. The outspread of Internet and programming services created further opportunities for development of home banking.

The internet banking services was first initiated in 1983 in United Kingdom. The foundation of internet banking was formed by this service. This facility was not capable of handling large number of account holders, hence it was limited to perform very few functions and transactions[11].

Currently used technologies for securing internet banking are user identification, data encryption (below 128 bit), audits and alarms, card verification codes (CVV/ CVV2/CID), online security portal, virtual keyboard and dedicated fraud management team are some of the standard security measures implemented by banks.

2.1 Review of Related Literatures

Jebaline, G. Renee, and S. Gomathi[1] presented a method to enhance the security of ATM using biometrics. In their study they described the exact and detailed procedure of extracting the fingerprint features and using it as an additional level of security. They suggested that in order to ensure the availability, user should register his all ten fingerprints. In their study they made use of hit and miss algorithm which will compare only few points in the finger print image which is actually needed for finger print verification and hence provides flexibility to the user without imposing any unnecessary constraints.

Singh, Maninder, Shahanaz Ayub, and Raghunath Verma[2] presented a method to enhance security by averaging multiple fingerprint images. In their study they suggested that even after recording multiple finger print image it is necessary to actually determine the number of combinations for each user to ensure that the attackers are not able to get access over an account of a legitimate user. To find the valid number of combinations the number of finger print images needs to be taken into consideration. Since the images are internally represented as binarized array of pixels whose grid can be either a 0 or a 1. The total number of combinations would be approximately 2^n where n is the number of finger print images considered

Hyder Yahya Atown[3] presented a method to hide and encrypt fingerprint image. In his study he discussed a method to secure the communication of the fingerprint image by using cryptography and steganography. In his study he observed that it is possible to crack Cryptography and Steganography alone, but combining both the techniques makes the communication robust. He proposed that fingerprint image is first encrypted by transposition pixel by spiral method and then it is embedded inside an image using LSB steganography technique.

III. Methodology

The user will first opt in for using internet banking services with the respective bank. In order to access the services of internet banking the user will have to do one-time registration, for which he/she needs to provide fingerprints of all the ten fingers and bank will generate unique identifier. The user will have to collect the generated unique identifier from the nearest bank branch. This unique identifier is further used by the user as user id for login. This is the first step where the fingerprints will be recorded at the server side. The second step involves entering user name (given when the user has opened the account) and password which is initially given by the bank along with the user id. Then the user will have to set new password after logging in for the first time.

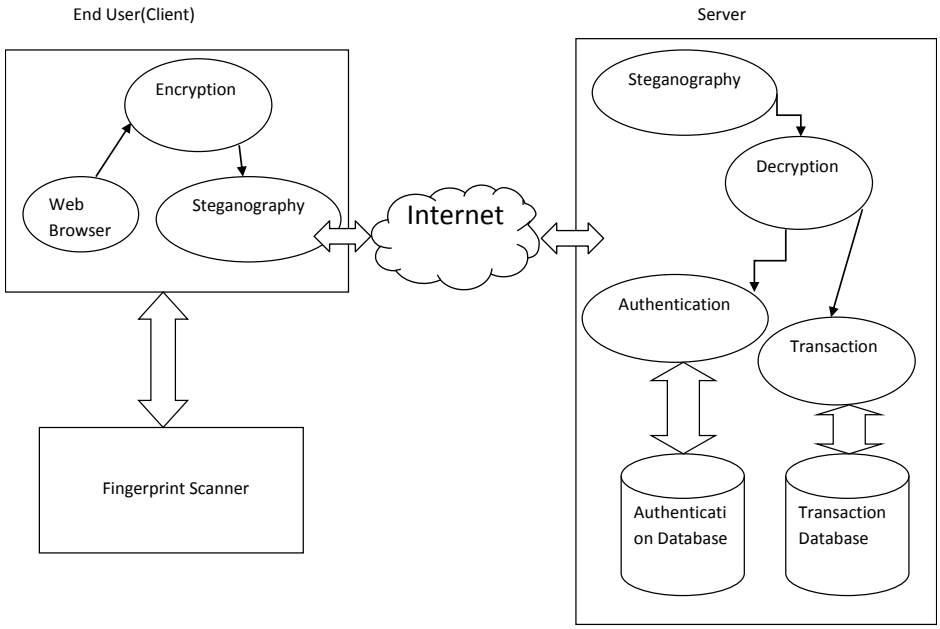

Figure 2: Block Diagram of Proposed System

The above process is the first-time registration. After which the user will login and it will consist of two steps. In the first step the user will provide the user id and will capture the fingerprint. This data will then be encrypted by using transpositional cipher. In this method for the plain text which is the user id will be break down in 4 parts and the 3 group of numbers will be swapped 6 times. And this generated cipher text will be transmitted using steganography where in the cipher text will be hidden behind stego cover image using the stego key which is only known to client and server. The fingerprint image will be encrypted using same encryption algorithm wherein the image will be represented as 2-dimensional array of pixels of size n x n. For the first pixel (which is (1,1)) will be swapped by the pixel with indices (n/2, n/2). The similar process will be followed for rest of the pixels in an incremental order. This process will be done six times. And this generated cipher text will be transmitted using steganography where in the cipher text will be hidden behind stego cover image using the stego key which is only known to client and server. This transmission is done through SSL link which is encrypted as per the RFC standard. On successful authentication of the above provided data the user will be redirected to next login page wherein the user will have to enter username and password. Which is transmitted using similar encryption process as specified for the first step.

User will be redirected the home page of the bank where he can access the services of the bank to he/she is subscribed. He/she is able to proceed for fund transfer. All the data provided by the user for this transaction to take place is also encrypted with the similar process as the first step. This data is transmitted through SSL link to the server for the further transaction to complete. User will get an acknowledgment once the transaction is completed successfully.

User can use internet banking services for online shopping too. If user wants to buy any goods online then with the help user net banking id he can pay for the goods. The payment site from where user has to buy some goods will be redirected to net banking webpage of the bank. He/she will be asked to do secure login and automatically the amount will be to merchant account. All the data for the communication of this transaction also undergo through similar end to end encryption as mentioned above for first step.

The registration data received from the client side will be stored by the server in the database which would be used for authentication purposes. On receiving request for login from client, in order to proceed with authentication, the server's steganographic process will remove the cover image to recover the encrypted data using the stego private key known only to the server. After recovery of the encrypted data, decryption will be done by using the decryption process which makes use of the server's private key. After recovering the original data, the server will do indexing using the user id provided by the client to fetch the fingerprint image stored in the database. If the fingerprints match (the fingerprint received in the request is matched with the fingerprint image stored in the database) then the client is authenticated and would be redirected to the second login page. The username and the password received from the second page will again go through the same process as that of the first login page content.

On successful authentication the client will get access to the subscribed services. Thereafter, any transaction data received from the client side will be fetched by passing the received data through the steganographic and decryption process respectively.

IV. Conclusion

The system implemented will be more secure, accurate and fast to get into internet banking services. All the banks who do not have internet banking services can use this system for starting such service. Even those banks who have existing internet banking services can use this system for more secure and accurate user authentication. Hence, the proposed system will be compatible with all types of currently existing systems and that too with minimum overhead.

References

[1]. Jebaline, G. Renee, and S. Gomathi. "A novel method to enhance the security of ATM using biometrics." Circuit, Power and Computing Technologies (ICCPCT), 2015 International Conference on. IEEE, 2015
[2]. Singh, Maninder, Shahanaz Ayub, and Raghunath Verma. "Enhancing Security by averaging multiple fingerprint images." Communication Systems and Network Technologies (CSNT), 2013 International Conference on. IEEE, 2013
[3]. Hyder Yahya Atown,"Hide and Encryption Fingerprint Image by using LSB and Transposition Pixel by Spiral Method", ICSJMC
[4]. Bhosale, S. T., and B. S. Sawant. "Security in e-banking via card less biometric atms." International Journal of Advanced Technology & Engineering Research 2.4 (2012): 457-462.
[5]. Bansal, Roli, Priti Sehgal, and Punam Bedi. "Minutiae extraction from fingerprint images-a review." arXiv preprint arXiv:1201.1422 (2011)
[6]. Dahikar, Minakshi S. TumsarePradeep B. "A Review of Security Aspects of Online and ATM Transactions in Banking Domain.",2015
[7]. Md. Shamimul Islam, Mahbuba Begum, Kanija Muntarina, Md. Golam Moazzam, "A Robust Technique to Encrypt and Decrypt Confidential Data within Image", International Journal of Engineering Science Invention(ISSN), November 2015
[8]. Gaurav, Mr. "A New Method for Image Steganography Using LSB and MSB." (2016).
[9]. Rohit Sharma, Dr. Anuj Kumar Agarwal, Dr. P.K. Singh, "Data Security by (Information XOR Image) Along with High Capacity Encryption to Overcome Steganography", ISSN, 2015
[10]. Hardik Runwal, Pooja Akulwar, "A Survey on: Cyber Crime & Information Security", IOSR, 2018
[11]. Wealth How: History of Internet Banking, https://wealthhow.com/history-of-internet-banking, Date Accessed 8th February, 2018

IOSR Journal of Computer Engineering (IOSR-JCE) is UGC approved Journal with Sl. No. 5019, Journal no. 49102.

Darshan Khachane. " Enhancing Security of Internet Banking Using Biometrics " IOSR Journal of Computer Engineering (IOSR-JCE) 20.1 (2018): 22-25.