© 2017 IJSRSET | Volume 3 | Issue 3 | Print ISSN: 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Security Improvement of Virtual Banking Application Using Multifactor Authentication

Vinoth Kumar L *1, Mr. R. Saravanan*2
*1Post Graduate Scholar, *2Associate Professor
Department of Computer Science and Engineering, Saveetha Engineering College, Chennai, Tamil Nadu, India

ABSTRACT

In today's era, virtual banking are used by many people across the world. All banks are providing services to their customer and there are many security issues like fraudulent website, capturing user ID's and password, fake mails from banks and phishing. To overcome this issues we can use multifactor authentication methods. This method is used such as user know (e.g: username and Password), user possesses (e.g: mobile signature) and user is (e.g: finger vein pattern). This paper proposes a new architecture for virtual banking to use biometric characteristics such as finger vein pattern and signature recognition . A combination of these two factor can validate with application server, once it has valid the application server will generate OTP to user mobile device. Using OTP the user signing into android and web application, user has been authenticated only with valid OTP and application server scan the mobile devices IMEI number. The security in virtual banking application can be secured by using biometric characteristics for authentication process.

Keywords: Virtual Banking, OTP, Finger Vein Pattern, Signature Recognition, Biometrics

I. INTRODUCTION

Virtual banking is also known as internet banking, online banking and e-banking. This means electronic payment system that customer of bank system or financial institution to conduct range of transaction through online service provided by bank websites. According to Cronin, Mary [3], " virtual banking services over electronic media", were introduced in earlier 1980's.There were four major US banks such as Citibank, Chase Manhattan, Chemical bank and Manufactures Hanover and bank of Scotland from UK that introduced virtual banking for the initial period. For example, bank customer can perform non transactional task through virtual banking including viewing balance, statement of account and fund transfer. A Multifactor authentication technology may also include "out of band" control for risk mitigation. A multifactor biometric characteristics based authentication system provide a much effective and secure way to provide online banking services. Biometrics means "life measurement" the term derived with the use of unique physiological characteristics to identify an individual person. In biometric system can be either an identification system or a verification system. In identification system the biometric can be used to determine a human identity without his knowledge or consent. It can be one-many comparisons to establish the identity of the individual. For example scanning a fingerprint with optical scanner using fingerprint recognition technology which can be determine entire template from database for match. In verification system the biometric can be used to authenticate a person's identity by comparing pre-stored biometric template in the system. There are two types of biometric characteristics such as : physical and behavioral. The physical biometric is used for identification or verification purposes. In identification used to determine "who a person is". Example of physical characteristics include: DNA, face, fingerprint, iris and retina. The behavioral biometric used for verification purposes, which can be determine " if a person is who they say they are". Example of behavioral characteristics include: gait, signature and voice. The

comparison between biometric characteristics presented in table 1.

TABLE 1. COMPARSION WITH BIOMETRIC METHODS

Biometric	Security	Accuracy	Cost	Speed
Finger vein pattern	High	High	Low	Fast
Palm vein	Medium	High	Medium	Medium
Fingerprint	Medium	Medium	Low	Medium
Face	Medium	Medium	Low	Medium
Iris	High	High	High	Medium

II. LITERATURE REVIEW

A. Username and Static Password

It is the weakest possible method. It was used by Raiffeisen bank in Romania and many other banks. Example consider for "Non-Banking Financial Institution-Cetelem". The registration process consists filling form from cetelem desk, then receiving a mail from bank to activate the access to application and after activation another mail send to customer provided a link to set initial password. After setting password customer signing using his/her credentials. Disadvantage of this method is there in no link to reset the password in main page[1].

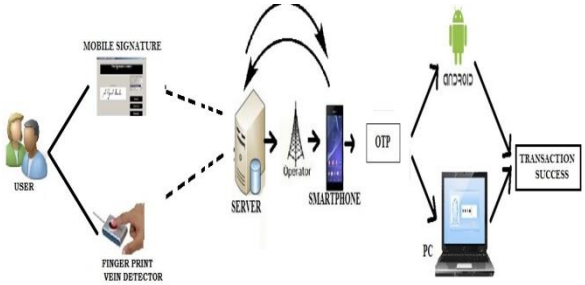
B. Username and Static Password, When using a Web Browser Certificate

This method consists of requesting a web browser certificate for online banking service. The customer applies for PIN at bank office and within 1-2 weeks an envelope containing it is delivered. After the customer receives certificate PIN and the customer can access the internet banking web page and which can providing link for requesting private certificate. The certificate is generated by Microsoft Active Directory Certificate Services, installed on Banca Transilvania CA. The certificate authority will store customer credentials and requesting certificate within every logon into application. Disadvantage of this method is private certificate can be only requested on internet explorer browser.

C. Username and Dynamic Password, Generated by a Token Device

When logging into an internet banking application, the secured webpage request username and password that is generated by token. It can provide code for electronic signature used signing into internet banking application. The token also has PIN that must be inserted every time password is requested. The token has serial number which can linked with user's account. It can't generate password to other account.

III. ARCHITECTURE



i) Requirement for Client

The minimum android version for virtual banking application cab be build from 2.1 operating system with 1GB memory and Minimum 256MB RAM is required for desktop computers. Both device needs Internet availability is must. Finger vein detector used for detector biometric characteristics.

ii) Requirement for Server

Minimum 4GB RAM and 1 TB hard disk is required for build application in server. Also Internet availability is required the server side.

IV. NEW SYSTEM DESIGN

In Proposed virtual banking is made used two different layer such as security layer and network/ control layer. The security layer is most important layer in proposed virtual banking and normally takes appropriate active when system is threatened. This layer can be categories into 5 level such as user authentication, device authentication, browser protection, transaction authentication pattern based intelligence and application security. The internet is global network which is intrinsically insecure. The security threats arising from denial of service attacks, spamming, spoofing, phishing, middle man perception. It is imperative that banks

implement strong security measures that can adequately address control these risk and security threats bank should provide the assurance that online login access and transaction performed over internet are adequately protected and authenticated. In proposed new architecture of virtual banking used to implements three module and they include:

- User Authentication Module
- Server Authentication Module
- Transactional Module

V. SECURITY AUTHENTICATION

The user authentication security module ensures that only authorized user gain access to the virtual banking application. This will be implemented using finger vein and signature recognition . The biometric is used desktop / laptop computer. This system equipped with signature recognition and finger vein sensor. This could require a security strategy to established to enable the following objectives to be met :

- Data Confidentiality
- System Integrity
- System Availability
- Customer and Transactional Authenticity
- Customer Protection

A. Signature Recognition

Signature recognition is behavioral biometric that identifies an individual on the basis of their handwritten text. It can be operated in different ways: static and dynamic. In static signature authentication uses only the geometric features of signature. This technique is also known as “off-line” model of recognition. For dynamic signature authentication uses geometric features and also some additional information such as velocity, acceleration, pressure and trajectory of the signature. This technique is also known as “on-line” model of recognition. In proposed works signature verification system comprises of two stages:

1. Enrolment Stage
2. Verification Stage

This two stage used to implement propose architecture of system.

i) Enrolment Stage

The user enrolls in system by giving multiple signatures which will be used to verify user credential. The user is giving a name with person ID registered ,after that during training phase provided space make user own handwritten signature with use of mouse. While drawing signature threshold values X and Y directions. The time threshold are checked and stored with database as a template. This values used for verification purpose. In figure 1 presented sample template signature.

Template signature #1 Template signature #2

Template signature #3 Template signature #4

Template signature #5 Template signature #6

Figure 1. Six Sample Template Signature

ii) Verification Stage

The user acquire an identity by inputting signature on system, which accepts the signature if the distance between the enrolled template corresponding to that identity. Finally user granted to access virtual banking services.

Authentic signature (accepted) Forged signature (rejected)

(a) (b)

Figure. 2. Signature For Verification With System

In figure 2(a) for left side signature is authenticated signature, which can match with registered signature and the system has accepted. In figure 2(b) for right side signature is forged signature which does not match with registered signature. so the system has rejected.

B. Finger Vein Recognition

Biometrics systems for individual identification have been developed for decades. Many methods have been proposed such as fingerprint, facial, iris, voice recognitions. Fingerprint identifying systems usually have low security. Fingerprint patterns are easy to be counterfeited because they are left everywhere whenever we touch a surface. Similarly facial and voice patterns can also be cloned easily. Iris scanning is uncomfortable because of producing a strong light to shine into subject's eyes.

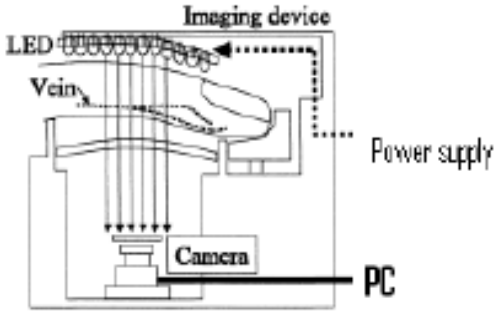


Figure 3. Finger Vein Recognition Device

In proposes system, finger vein recognition is method of biometric authentication. That uses pattern recognition technique based on images of human finger vein developed and patented a finger vein ID system. Finger vein authentication uses leading edge light transmission technology to undergo pattern matching and authentication [14].

Figure 4. Finger Vein Extraction Pattern

In figure 3. shown finger vein recognition devices. The near infrared light is transmitted through finger and partially absorbed by haemoglobin in the veins to capture a unique finger vein image using CCD camera. There are four step to follow signing into virtual banking such as

Step 1: Capturing finger vein image
Step 2 :Extraction of finger vein pattern
Step 3:Matching with finger vein pattern and pre registered vein pattern.
Step 4: If it is matched, authentication successfully.

These steps can presented in figure 4 for finger vein extraction pattern .

C. One Time Password

In order to secure the System, the generated OTP must be hard to guess or trace by hackers. The user authenticated with signature and finger vein recognition methods the application will generate OTP to user smart phone. The server randomly challenges the user with new indexes. The user logs into the service provider's website, or android application through corresponding OTP. At the same time application server check for smart phone IMEI. The user responds with this corresponding OTP and server compares the received OTP[17]. According to the server check valid OTP, the server will transfer an authorization execution .

VI. CONCLUSION

Implementing the multi factor security model used for virtual banking will offer safe transactions that protect both customers and banks. We chose combination of finger vein pattern and signature authenticated with server, so system is more secure as compared with other biometric characteristics. A finger vein extraction and Signature recognition should meet these requirements such as Higher Accuracy, High response time and low cost of devices. Hence proposed system more secure, efficient and reduce phishing attacks, man in middle attacks.

VII. REFERENCES

[1] C., Lupu, V.G., Găitan, V.Lupu, "Security enhancement of internet banking applications by using multimodal biometrics", IEEE 13th International Symposyum on Applied Machine Intelligence and Informatics (SAMI 2015), Jan. 22-24, 2015, Herl'any, Slovakia, pp. 47-52, ISBN 978-1-4799-8220-2, 978-1-4799-8221-9.

[2] C. Lupu, V. Lupu, "Biometrics used for authentication in internet-banking applications", Annals of the „Constantin Brancusi" University of Targu Jiu, Engineering Series, No.3/2014, pp. 57-63, ISSN 1842-4856.

[3] Cronin, M.J., "Banking and Finance on the Internet", John Wiley and Sons, ISBN 0-471-29219-2, p. 41, 1997

[4] Webster dictionary, http://www.merriamwebster.com/dictionary/biometrics.
[5] A. Ross, K. Nandakumar, A.K. Jain, "Handbook of multibiometrics", Springer, 2006, ISBN 978-0-387-22296-7.
[6] J.L. Wayman, A.K. Jain, D. Maltoni, D. Maio, "Biometric systems: technology, design and performance evaluation",Springer, 2005, ISBN 978-1-84628-064-1.
[7] A. S. Syed Navaz and K. Durairaj " Signature Authentication Using Biometric Methods", International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064.
[8] Napa Sae-Bae and Nasir Memon"A Simple and Effective Method for Online Signature Verification".
[9] Chin-Ming Hsu, Shih-Hsiung Twu and Hui-Mei Chao"A Group Digital Signature Technique for Authentication".
[10] Maged M.M. Fahmy "Online handwritten signature verification system based on DWT features extraction and neural network classification".
[11] Reetika and Kiran Gupta "Feature Extraction Technique based on Structure of Finger vein: Review" SSRG International Journal of Computer Science and Engineering (SSRG-IJCSE) – EFES April 2015.
[12] D.S. Guru and H.N. Prakash "Online Signature Verification and Recognition: An Approach Based on Symbolic Representation" IEEE Transactions On Pattern Analysis And Machine Intelligence, Vol. 31, No. 6, June 2009.
[13] Xiang Yu, Wenming Yang, Qingmin Liao and Fei Zhou "A Novel Finger Vein Pattern Extraction Approach for Near-Infrared Image".
[14] Chenguang Liu Yeong-Hwa Kim , "An Efficient Finger-Vein Extraction Algorithm Based On Random Forest Regression With Efficient Local Binary Patterns".
[15] Xiaoming Xi, Gongping Yang *, Yilong Yin and Xianjing Meng"Finger Vein Recognition with Personalized Feature Selection".
[16] Fadi Aloul, Syed Zahidi Wassim El-Hajj"Two Factor Authentication Using Mobile Phones".
[17] Mohamed Hamdy Eldefrawy, Khaled Alghathbar and Muhammad Khurram Khan," OTP-Based Two-Factor Authentication Using Mobile Phones".
[18] Lorette G. Plamondon, R. Automatic signature verification and writer identification - the state of theart. Pattern Recognition, 22(2):107–131, 1989. cited By (since 1996) 342.
[19] Miura, Naoto Nagasaka, Akio Miyatake, Takafum "Feature extraction of finger-vein patterns based on repeated line tracking and its application to personal identification" Vol. 15, No. 4,Year 2004.
[20] Xi, Xiaoming Yang, Gongping Yin, Yilong Meng, Xianjing "Finger vein recognition with personalized feature selection" Vol. 13, No. 9,Year 2013.
[21] Wang, Kejun Ma, Hui Popoola, Oluwatoyin P.Li, Xuefeng "A novel finger vein pattern extraction method using oriented filtering technology"
[22] Guru, D S and Prakash, H N "Online Signature Verification and Recognition: An Approach based on Symbolic Representation." Vol. 31, No. 6,Year 2009.
[23] Bhattacharya, Indrajit Ghosh, Prabir Biswas, Swarup "Offline Signature Verification Using Pixel Matching Technique" Vol.10, Year 2013.
[24] Fahmy, Maged M M "Online handwritten signature verification system based on DWT features extraction and neural network classification" Vol. 1, No. 1,Year 2010.
[25] Kulkarni, Vinayak Balkrishana "A colour Code Algorithm for Signature Recognition" Vol. 6, No. 1,Year 2007.