International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 4 Issue 09, September-2015

Moblie Banking Security

A Review Paper on security methods use in banking

Nikita Sethi
Department of Computer Engineering
Poornima University
Jaipur, Rajasthan, India

Mrs. Swati Paliwal
Faculty Coordinator in Poornima University
Poornima University
Jaipur, Rajasthan, India

***Abstract*—Mobile phones are inseparable companions for many users, serving much more than just communication tool. In developing countries, the no. of mobile phone users exceeds the number of those having bank accounts. Banking service is part and parcel in the reformist society. Mobile e-commerce has dramatically increased due to the reason that the function of smart phone and PC are combined together. Due to proliferation of communication technology, instead of conventional paper based banking system, sms-banking and m-banking are get immense popularity. M-banking is thus more convenient, effective and timely through the new mobile communication system. In order to raise the security in mobile banking, there are various M-banking security techniques are used in recent years like digital watermarking technique, 2D barcodes, OTP and biometric verification scheme, payment system using QR codes and automatic lip reading. In digital watermark technique, a short message service (SMS) based M-banking protocol under GSM technology is defined. In various banking security prospective, one time password (OTP) and personal biometric have been combined for verification. OTP includes message verification whereas biometric includes fingerprint, iris, retina, image etc. verification. In automatic lip reading methodology, phone camera provides the ability to track the user's lip motion using lip reading algorithms to recognize the security words like passwords and receive passwords using visual information processing from the user's lips. Mobile banking tackles both concern of process as: speed of transaction and security, without complicating the process or making it undesirable to users.**

Keywords- Mobile banking security; watermarking techniques; one time password; Biometric; QR code; Automatic lip reading; lip tracking;

I. INTRODUCTION

Mobile banking is a term used to refer to systems that allow customers to do financial exchange to conduct a number of financial transactions through a mobile device such as a mobile phone or tablet. M-banking is the extension of internet banking. Mobile terminals are used to perform various banking transactions. The major concern while using mobile banking application is of security which can lead the user to the financial loss.

Currently, mobile banking could provide functions such as balance query, debit application, payment transaction, and etc. [1][2]. There are some popular service provided by M-banking such as announcement and notification, information providing, and business transaction. As adopting M-banking, there are some advantages listed in the following:

1. No restriction of location: The user can perform banking anytime in any place as possible.
2. High penetration: The popular utilization of mobile phones provides the sufficient assurance of the growth and utilization of M-banking.
3. Personalization: Each of the mobile phones is purely work for specific user. Therefore, it increases the effectiveness of user authentication [3].

There are several methods to authenticate the user in any banking application. The most common method use to authenticate the user is using username and password. Usually the password which includes the sequence of alphanumeric characters is entered by the phone's keyboard. However, it is not secure and it is often hacked or steals by key-loggers. Key-loggers can theft the typed password and enter the user's account. To overcome this problem, text based passwords are replaced by more secure, effective and innovative method. Some of the novel authentication methods are digital watermarking technique, one time password (OTP), automatic lip reading, voice-based authentication, image- based authentication and the use of biometric technologies. Banking become more versatile due to the various M-banking features invented for the sake of common people.

II. RELATED WORK

There are various methods used for authentication of users in the applications. Here we will discuss briefly about those methods.

A. One-time password (OTP)

In OTP method, every time a fresh password is generated for user by incorporating some special calculations. Thus, even if key-logger can detect the user's typed password, it cannot use it to log into the system next time. However, one of the existing problems in such systems is requiring an additional device as microcontroller should have been used for calculating and storing passwords to generate the passwords.

B. Voice-based authentication

Another method of authentication in mobile banking applications is using the voice-based passwords. The user can enter her/his password using voice and the application recognizes the password using the speech processing algorithms to authenticate her/him.

Voice-based method is secure against key-loggers but the main problem is that the password is said loudly therefore other people can identify the password. With the advancement in technology and the use of biometric identification, these systems can be enhanced and identify the users by extracting the speaker's voice patterns[4]. Biometric technologies do not rely on passwords and the PIN codes.

C. Image-based authentication

The third set of authentication methods is based on image. One of the graphic-based authentication methods is that the user selects a sequence of images and remembers them as her/his password used this method to authenticate the users.

D. Biometric authentication systems

There are several biometric techniques used for authentication in mobile devices. Some of the biometric features include finger prints, face, hand geometry, iris, voice, signature and the key stroke recognition.

One of the famous biometric methods is the face recognition. Mobile payment methods usually belong to one of the three models based on the entities that are involved in the process. The four potential mobile payments business model scenarios are as follows:

A. Operator centric model

In this case, the mobile operator provides the technology, process the transactions and compensates the system. In this model, it is necessary to connect the mobile-payment system and banking accounts or cash deposits. The applications may support a prepaid stored value model or the charges may be coordinated into the customer's mobile bill. The mobile operator usually provides the merchant with a wireless POS system for operations.

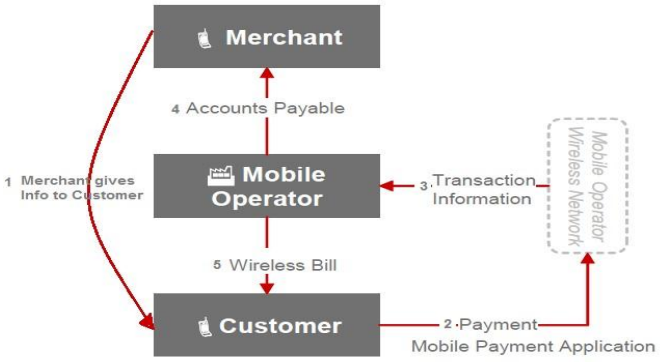

Fig. 1 Operator Centric Model

B. The bank centric model

In this model a bank is involved in the process. The customer gives the needed info (using NFC) in order to make the payment for the merchant. The merchant bank will contact the customer bank to get the payment transaction done.

The Bank Centric Model can be considered as an evolution of the credit card model.

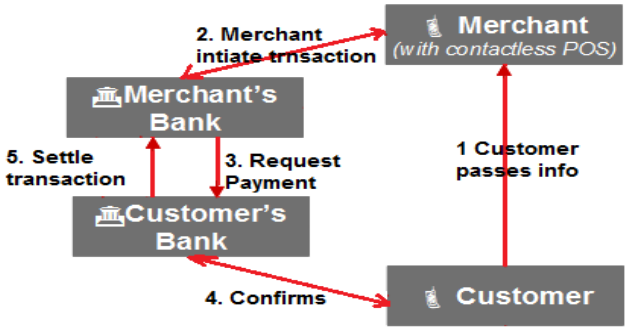

Fig. 2 Bank Centric Model

C. Peer to Peer model

In this model, an independent peer-to-peer service provider provides secure mobile payments between customers or between customers and merchants, where both merchant and customer should have accounts with the service provider. Via the established accounts, the service provider will be able to charge the needed payment to the customer and transfer it to the merchant. The service provider could be either a financial instate, such as a credit card issuer, or just a trusted mediator among banks that hold the real customers and merchant accounts.

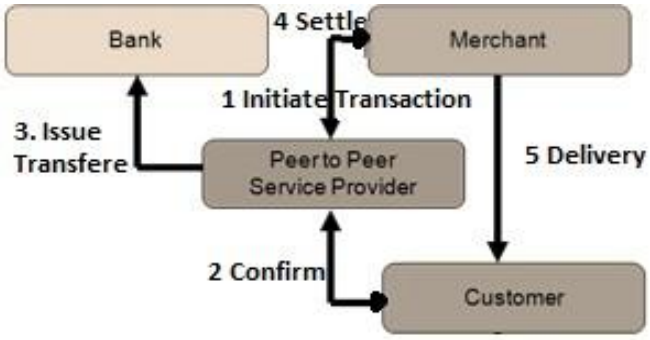

Fig. 3 Peer-to-Peer Model

III. PROPOSED PROCEDURE

There are various techniques used for secure transaction in the field of mobile banking in past few years. Various proposals are as follows:

A. Digital watermarking

Upon results of the access code, the SMS including the transaction information will be watermarked. The watermarked SMS has its own format. This operation is carried out by the SME using a predefined template.

The hidden information is sent to the BS via computer network and the marketing gateway. Watermarking ensures that the exchange of financial information is no longer crystalline to an intruder or even to the mobile operator.

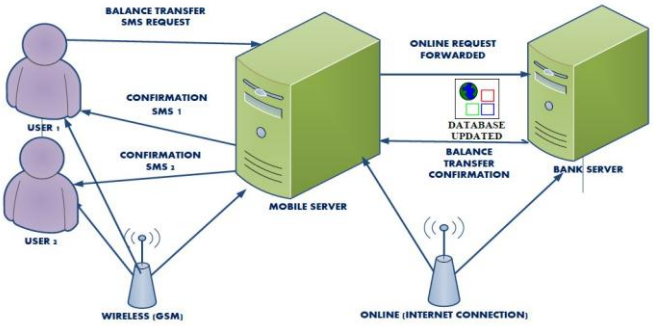

Fig. 4 Transaction Procedure

Basically, digital watermarking is a technique used to the ownership and the authenticity of digital in- formation, which can be any information like an audio, image, video or text file. However, digital watermarking in this work has been used in a rather inappropriate way so as to explore the security of SMS based banking. The method proposed here uses text watermarking for hiding the SMS containing exchanging financial information into another duplicate text file (DTF) in order to make the transactions

unidentifiable to the intruder. Digital watermarking techniques for text are rather of very small range because of the binary nature of text documents which lack rich high scale information. The basic requirements to be completed for digital watermarking are deliberately, security, and robustness.

1) Performance Analysis

An important concern in m-commerce is data integrity of the transaction information. From this idea, we have discovered here the immunity of different approaches of water- marking against pseudo random and flip noise. Assuming stable sequencing, the results of noise signals having different signal to noise ratios (SNRs) are identified for the 7 possible entries of the data bit. The effects of flip noise are more severe when compared with different random noise as flip noise instatntly changes an information bit. To analyze the impact of flip noise, we have defined here a term *ACCURACY=1- BER*. If information is hidden into the 1st bit, then flip noise at LSB can completely destroy the information and hence an accuracy of zero [5].

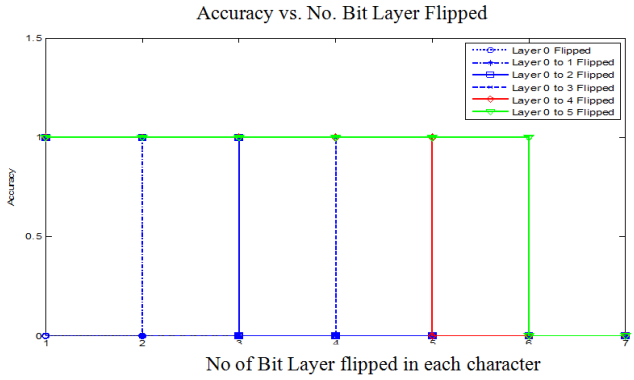

Fig. 5 Accuracy Graph

As the index of combined data increases, so does the robustness against flip noise. However for flip noise, the accuracy cans variants suddenly from 100 to 0 if watermarking is done using the direct sequencing method.

B. OTP and Biometric verification

Traditionally, M-banking by utilizing OTP for transaction authentication is initiated as the client side presents the request of transaction application. The server side will then generate an OTP and transmit to the mobile phone that defined by the client side through Internet. After then, the user needs to key-in the received OTP via webpage of M-banking for verification to gain the authority of transaction application. However, if the user does not perform key-in correctly, the client side will need to apply for a new OTP. Thus, it will increase the risk of OTP broken or interception.

The private biometric technique has been used and combined with the OTP for verification of M-banking. As the users register online on website of M-banking with ID and password, they can perform the process of query that without modifying the account's information. If the users need to perform business transaction, they need to present the request to the server side. The server side will then reply with accuracy for this request before further process. There are some approaches included OTP, smart card, and user defined password offered for reconfirmation.

The detailed procedure of using the mobile phone for M-banking is depicted as the following.

Step 1: User login with their ID and password.

Step 2: Server side of M-banking verifies the validation of user ID and password. If the password is not correct, the server side will reject to provide service. If the ID and password of the user is correct, the user can browse the related restrict webpage and perform query process.

Step 3: As the user presents the business transaction request, the server side will then generate an OTP and transfer to the default receiving equipment, i.e. mobile phone of the user.

Step 4: The server side will request the user to key-in the valid OTP in specified time period.

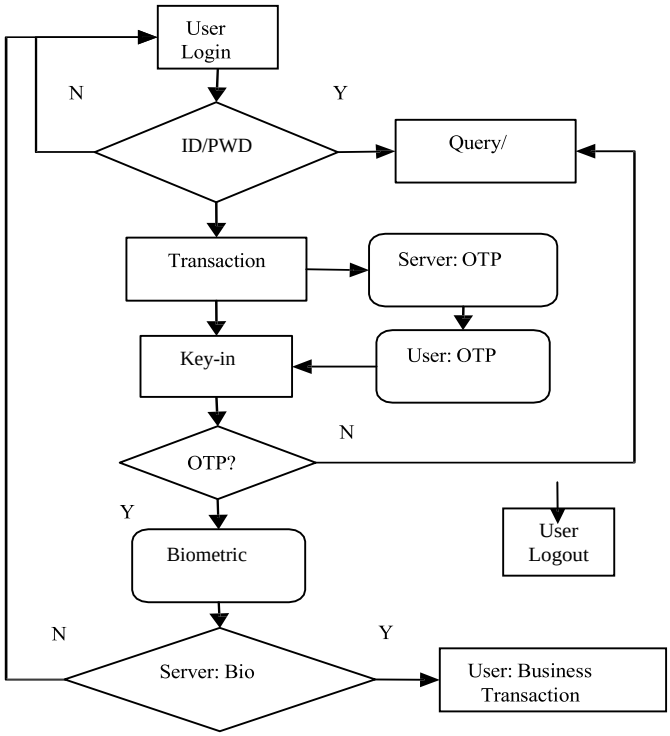

Fig. 6 Proposed schemes for performing M-banking

Step 5: The server side will perform the verification of OTP. If the input OTP is not correct, the server side will reject the request of business transaction and indicate OTP not valid and remind the user whether if the user needs to perform business transaction or not. If the user's answer is yes, the server side will then generate and transfer another new OTP for the user to register again. If the user does not need to perform the business transaction again, the process will retain on the privilege of browsing and query function.

Step 6: If the input OTP is correct, the user will be request to capture new biometric data and upload to the server side in real time with hash function process for authentication to increase the needed security[6][7].

Step 7: The server side will compare and verify the uploaded biometric data if it is identical to the user. If the answer is "yes", the user then can perform those available

business transaction services. Otherwise, the server side will reject the transaction process and request the user to Login again to prevent the possible defrauding.
Step 8: Logout and finish the M-banking activity.
However, the uploading of personal biometric and verification does take times. Besides, the transmission of OTP and biometric data still possess high risk of interception via Internet or telecommunication

A. QR Code

Recalling the traditional payments via Credit Card, at least two tokens are expected from the customers to prove an authenticated transaction. These two could be the existence of the card itself, and the signature or the PIN number which is getting more popular in POS's than signatures.
Both tokens exist in different places with the customer. The credit card is placed in the customer's wallet, while the signature or the PIN number usually exists in the customer's brain. Following the same concept, this paper requires two tokens to verify identity. One is the mobile phone which is placed in the customer's pocket, while the other token is proposed to be a QR code, which will exist in the customer wallet, or simply a PIN number.
While the customer waits in line for the cashier or is about to perform a transaction, the customer scans a QR code placed in his wallet and specifies a ceiling limit to the amount to be paid at the cashier. The time the QR code is scanned is also essential to the transaction to prevent fraud. The purpose is to acknowledge the identity of the mobile phone holder. Once the merchant is ready to initiate the transaction, the Merchant displays a QR code that includes information on the transaction. Upon scanning this QR code, a one way private key gets generated once mixed with the owner [8].
A further security step could be added when scanning the customer QR code. This step is to enter a PIN number. However, we believe that this is not necessary especially that mobile phones are usually locked. The above mentioned scanning process assures the identity of the customer and sets a limit to the amount to be paid. Furthermore, since there is no handshaking for transaction confirmation between the third party and the customer, the processing time is expected to be faster than a credit card payment process.

C. Lip Reading

Different characters have been trained and stored in the lip models dataset and the dataset is saved on the user's mobile phone locally. This database has been trained by different speakers to increase its accuracy. The user's password is recognized offline on the phone to increase the speed and to reduce the server load. Then the user is authenticated by sending the username and password to the bank's server to match with the database. The system does not require the user's full face. Only the lips recording using the phone camera is adequate to enter the password.

1) The system architecture

At initial phase, each password character video is parsed into frames and each frame is entered into FPSS. In FPSS, user's lip is recognized and segmented. Then, the feature extraction method is applied on segmented lip to extract coordinates around the lip.

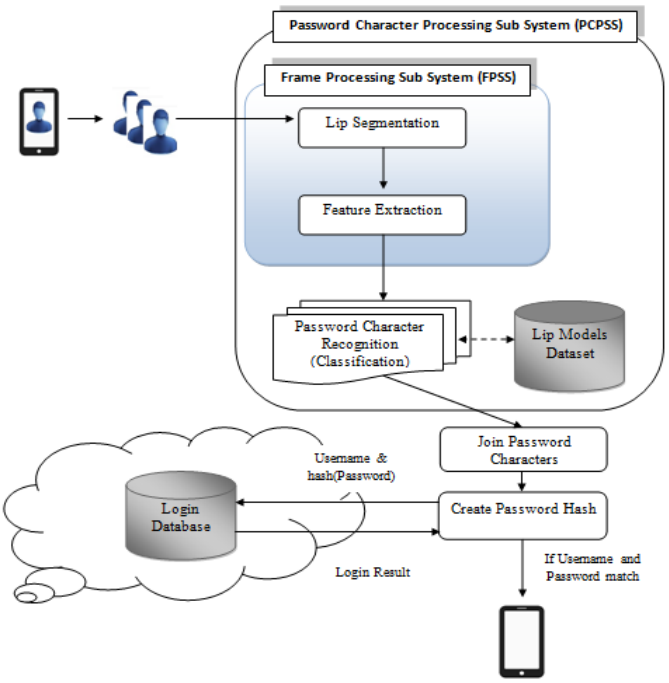

Fig. 7 Proposed system architecture

After feature extraction phase, all of the features of a video which are extracted from the different frames are combined and entered to the classification algorithm to recognize which character is in the video. The classifier calculates the distance between the extracted features and the stored lip models and returns the nearest character as a result.
Then the characters are combined to form the password. The system calculates the password hash and sends both password hash and the username to the bank server to check if they match or not. If the username and password are correct, the authentication is successful and the user is directed to the application to perform her/his banking procedures.

D. Developing m-bank prototype on android smartphones

A prototype of m-bank application was developed for the android smart phone. . In this application, the user types her/his password and has two options for entering the password. If she/he selects 'Lip Reading Password', she/he can enter password by moving lips without any voice.
The phone camera records the character videos to process them. Then the system recognizes the password and sends password hash and the username to the bank server. If the login is successful, the user can see the second page to perform some mobile bank stuffs like enquiring balance, monitoring last 3 transactions by detail, transferring funds to another account and checking check statuses. In this application, it is supposed that password has 4 characters. If the user does not select 'Lip Reading Password', she/he can enter password using typing.

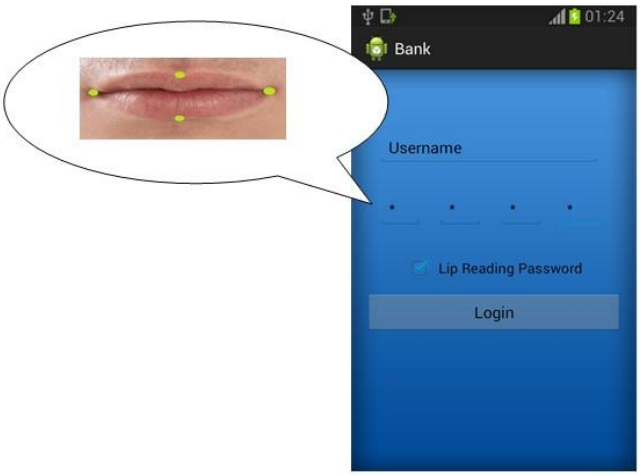

Fig. 8 M-banking list of jobs

Key-loggers can monitor touch pads in smart phones and log which characters are entered as password. Therefore the traditional methods for entering passwords are not safe against the key-loggers. Using lip reading as a method for entering password can protect system against key-loggers. On the other hand, the voice is absent in comparison to voice-based passwords, therefore the attackers cannot hear the password to eavesdrop it.

2) Experiment results

Lip reading prototype was tested using LiLiR dataset of English characters in which 10 speakers repeated each letter 3 times[9]. For testing our m-bank application, 7 of 10 speakers and a subset of characters contains 'B','F','H' and 'Z' were selected for training and testing. For each letter, 17 videos were used for training and 4 videos for testing, so the training set contains 68 letters and the testing set contains 16 letters. The success rate of lip reading implementation was about 70%.

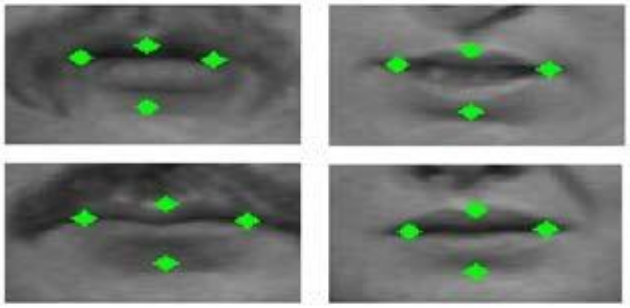

Fig. 9 Feature extraction phase on 4 speakers (in LiLiR dataset)

There are several problems in implementing lip reading systems. Different people have different face features. For example different skin colors, lip shapes or hair styles. In other hand, some people have beard and effect on lip reading algorithms. Another problem is detecting lips in people having cleft lips.

IV. CONCLUSION

V.

This paper defines an easy approach but effective way of SMS- banking technique for M-commerce. One major advantage of the proposed SMS-based scheme is that, it is suitable for developing as well as under-developed countries. While utilizing OTP M-banking, the OTP can be transmitted via Internet or telecommunication network. In addition, the OTP is generated randomly while transaction request presented. Thus, adopting OTP for M-banking is really a good choice. The proposed M-banking verification scheme requests the client side to capture biometric information and upload to the server side for verification in real time. . The processing speed, due to the lack of handshaking payment confirmations, is expected to be faster than a credit card payment process. a new method has been introduced to authenticate and lead to the users safely during mobile banking. One of the main concerns in implementing a m-bank application is security against key-loggers to avoid them from steeling the passwords. Lip reading could be used in such systems to help users entering their passwords. In this paper an m-bank application prototype for android smart phones is implemented and tested.

VI. REFERENCE

[1] 2011.http://en.wikipedia.org/wiki/Mobile_banking, Accessed on Nov 30, 2011.
[2] Hanáçek, P., Malinka, K., Schäfer, J., "e-Banking Security-A Comparative Study", IEEE Aerospace and Electronic Systems Magazine, 25(1), Pages 29-34, 2010.
[3] Atul Kahate, "Cryptography and Network Security", McGraw-Hill.
[4] Mikhail Khitrov, Talking passwords: voice biometrics for data access and security, Biometric Technology Today, Volume 2013, Issue 2, February 2013, Pages 9-11.
[5] Fadi Aloul, Syed Zahidi, Wassim El-Hajj, *"Two Factor Authentication Using Mobile Phones"*, 2009.
[6] RSA Laboratories (2009), PKCS #11 V2.3 Cryptographic Token Interface Standard, RSA Security Inc
[7] Housley, R., Ford, W., Polk, W., and Solo, D., "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, 1999.
[8] Clarke, N., and Furnell, S.: Authentication of users on mobile telephones – A survey of attitudes and practices. Computers & Security, 24(7):519– 527, 2005.
[9] Matthews, et al., "Extraction of visual features for lip reading". IEEE Trans. on Pattern Analysis and Machine Vision, 2002. 24(2): p. 198-213