ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

A Survey on Improving Security and Privacy of Mobile Banking through Authentication Assessment

Sudeep George, Reshma M

P.G Scholar, Dept. of Computer Science and Engineering, Cochin College of Engineering, Kerala, India

Assistant Professor, Dept. of Computer Science and Engineering, Cochin College of Engineering, Kerala, India

ABSTRACT: Secure authentication is essential for a banking applications running on mobile devices.Financial institutions are increasingly able to leverage mobile devices to empower customers to better secure online transactions, and to defeat malicious fraud attacks that attempt to highjack customer accounts. **“**The security risks of mobile devices are investigated focusing upon the current security challenges that mobile devices experience. Consequently, the need for more protection on mobile handsets is discussed. Current authentication approaches available on mobile devices are explored with in- depth analysis to identify the weaknesses and vulnerabilities of these approaches. This research presents an enhanced authentication approach for mobile devices, provides transparent (non-intrusive) and continuous identify verification of the user. Finally, additional techniques were discussed which aim to increase user convenience and stronger authentication.”

KEYWORDS: mobile banking assessments’, ‘authentication in mobile banking’, ‘security of mobile banking’, ‘Privacy in mobile banking’

I. INTRODUCTION

There are over 1.2 billion smartphone users worldwide.1 Individuals adopt smartphones not only to surf the Internet but to download and use entertainment, information, social sites, shopping, travel and banking apps [1] — among other things. This has led to numerous opportunities for organizations to roll out mobile applications that not only engage and drive loyalty but also garner additional revenue. Organizations are substantially increasing spend on mobile application development to help employees/customers increase their productivity while delivering a more intuitive user experience. [2]

Moreover, an increasing number of individuals are using mobile applications compared with traditional desktop/Web-based applications. A research report from ComScore shows that apps account for a majority of consumers’ mobile minutes, and 80% of their media time is spent on app usage compared with only 20% on Web browsers. [3] Recently published data from MQA Research shows that consumer interest in mobile banking and payments services in the U.S. has increased significantly in the past two years. Roughly 75% of those surveyed say they would consider using mobile banking services if offered, compared with only 49% who expressed their willingness to try mobile banking services in a similar survey conducted in 2006. [4]

Globally, banks offer a variety of mobile banking services; and those banks that do not currently provide m-banking services claim they plan to do so in the near future to remain relevant, according to a recent survey conducted by the Aite Group. [5] And according to a study from the University of Hamburg, Germany, m-banking mobile applications are growing exponentially; roughly 69% of banks already offer such services. [6]

However, there is a downside to this market momentum. The MQA survey revealed that security remains a major concern in adopting m-banking. Approximately 72% of respondents said they worry about the security of accessing financial data on a mobile device. Nevertheless, 79% of respondents said they would sign up for account balance alerts by mobile. Our research on consumer segments reinforces the importance of security features for choosing banks that offer mobile banking.

DOI: 10.15680/IJIRCCE.2017. 0504146

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 4, April 2017

II. Related work

The aim of this research is to review different methods of authentication in mobile banking. Finally, an advanced authentication system that increase security required for mobile devices and the model with 2 layers of security have been presented. By being able to authenticate a user without their knowledge, the system can be automatically monitored and maintained without the user's explicit interaction until such time that the system detects an imposter accessing the mobile devices.

Below is a list of some of the common authentication methods:

1. A PIN (personal identification number) code: it used for unlocking the smartcard
2. An ID / password: it used for opening a session on a computer or for authenticating on the Internet
3. An RFID card: for accessing a building
4. A fingerprint: to unlock a door
5. A one- time password token
6. A USB token
7. A facial recognition system with a webcam: it used for opening a session on the Internet

The authentication process is based on a combination of one or more authentication factors. The four important factors to authenticate humans are:

1. Something which user knows like a password, a passphrase, a PIN code and etc.
2. Something which is user owns such as a USB token, a smartcard, a software token, and etc.
3. Something which qualify the user such as a fingerprint, DNA fragment, voice pattern, hand geometry and etc.
4. Something which can user do like a signature, a gesture and etc.
5.

Nowadays approaches are still focused upon PIN/passwords or fingerprint authentication which requires users to provide a correct PIN or fingerprint before accessing to the mobile device.

In addition, when user chose to not using authentication at the first time or once the identity of the user has been verified at login time, the mobile system is generally made available to the user since they leave the system. This can be lead to high risk environment which imposter targets a post authenticated session and result in financial, private and sensitive information loss to the user.

The aim of this research is to find an advanced authentication system that increase security for mobile banking system. As shown in Figure 1, the number of people using mobile is not the same in all over the world hence, the penetration is not too. Europe has the highest mobile penetration rate, followed by North America and Latin America where penetration rates exceed 100%. By our estimation, till the end of 2016, the number of mobile subscriptions will exceed the number of world populations with the global mobile penetration at 110% [7]. By this facts, we guess that in a few years every person will have at least one mobile phone.

A. Authentication mechanisms:

- **Personal Identification Number (PIN) Authentication**

Preventing PIN authentication will be deployed for an unauthorized person accessing a mobile and the Subscriber Identification Module. Generally speaking, a mobile PIN code contains between four to eight digits. A user is required to enter the correct PIN code before accessing the mobile device and most of the time the user will not be required to re-enter the PIN until the next reboots. However, a PIN can be set to be requested again after a certain period of time for additional layers of authentication. For preventing unauthorized persons accessing the SIM card, a PIN code is needed at "switch on" or when a SIM card is inserted into a mobile phone. The mobile device would not start and the SIM card would not authenticate with the cellular network without a correct PIN. In the case of entering SIM PIN code incorrectly for three times; the SIM card will be blocked; hence, a user cannot access the mobile network. For

DOI: 10.15680/IJIRCCE.2017. 0504146

unblocking key to unlock from network operators, the user has to ask for Personal Unblocking Key.

- **Password Authentication**

Password authentication has protected mobile devices from unauthorized user access. A user have to enter the correct password before accessing the mobile device. Passwords can contain a string of letters, special characters and numbers, which can provide a large number of set of passwords in comparison to PIN. The length of a password is dependent on the security policy of the particular application. Nevertheless, it could be difficult to type long password on small keypads.

- **Recognition-based passwords Authentication**

The length of a pattern is approximately between four and nine. However, there is limitation in this method which is a dot cannot be used more than one time. As a result, this technique provides less number of password patterns than traditional PIN and password. Although these techniques are available on mobile handsets, in practice, may users do not utilize a PIN or password to protect their devices [8]. The lack of use of PIN or password authentication has been stated that because users do not confident with the protection of it considered it is inconvenient [9]. As well as, many users the

one who utilize authentication do not use it properly. According to the survey [10], it is reported that majority of respondents use the default password that is given after initially purchasing the handset. More than one in ten respondents uses the same PIN across multiple devices and accounts, over half of users shared the same passwords with others and 15% save password information on their phone. These make the PIN/password based authentication technique inadequate as a protection for mobile devices [11]. Furthermore, two other authentication techniques are available, which are token and biometrics. Token based approach is considered which the user would need to carry them around with the mobile. Another issue is that if the authentication process requires the token to be placed into the device then it is highly probable that many users would leave it in mobile device. This can be illustrated by the use of a SIM card on current mobile devices. When the users do not want to use the mobile, users could remove it. However, removing the SIM card would be inconvenient. By utilizing contactless technology, it is possible to develop tokens that can be integrated within the item that users would always expect to have with them such as rings. Although this technique can increase user convenience over the secret-knowledge approach

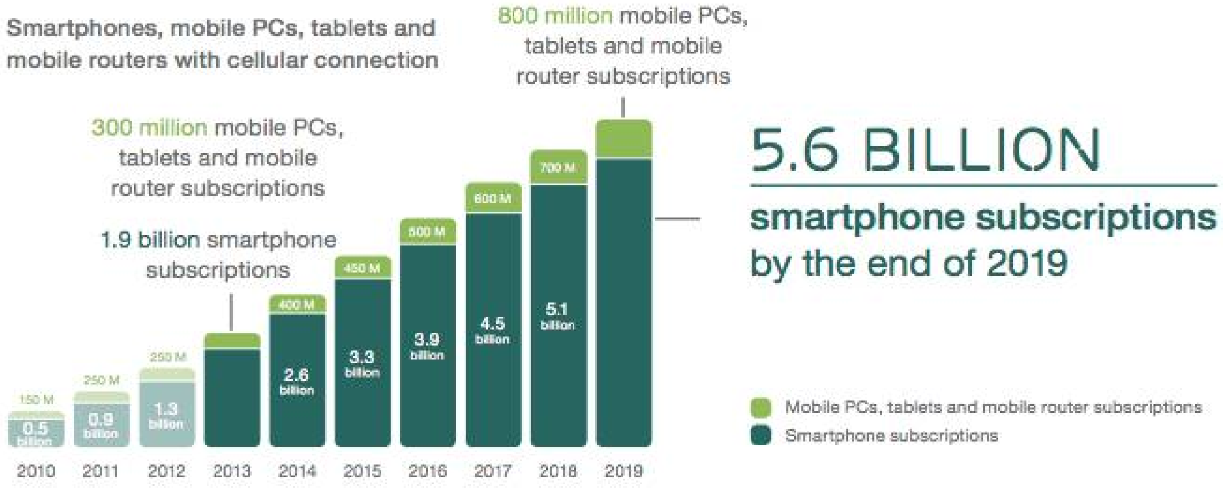

Fig 1. Mobile Penetration levels in different years

as no interaction is required. However, this approach requires the user to remember the token. The last approach to authentication is biometrics. This technique authenticates a user based on unique characteristics of the user such as fingerprint, hand and face. The biometric method does not require users to remember anything just being themselves.

"With the evolution of mobile devices and network technology, some mobile devices come equipped with fingerprint-reader or face recognition technology which can provide more secure authentication mechanism. However, although fingerprint and face recognition increased the level of security, these techniques remain point-of-entry- authenticate and intrusive to the user."

As described above it is clear that the point-of-entry authentication approach has been developed to determine permission over access to the device itself and provides no further protection during the usage session. However, in reality, the need for security will vary depending upon what the user is doing and different services and data should require different levels of security. Since each service carries a certain risk of misuse, this must be a factor in deciding the appropriate level of security.

"If the level of security is appropriately assigned to each service so that each service or function can require a certain level of authentication in order to grant access to the specific service." In this way, more critical operations could be assigned a greater protection and leave less risky operations to a low level of trust. As a result, an advanced authentication approach which is capable of continuously monitoring and authenticating a user based upon the users' legitimacy is desperately needed. This can be best achieved by using non- intrusive or transparent technique; so that users would not be aware that authentication is taking place, avoiding the user having to stop operation in order to re-enter a PIN for instance.

B. Biometric

Biometrics is quickly becoming a large part of our everyday lives. Every time we get a new passport, a photo is taken, a signature is used to sign off on important documents, or a fingerprint is scanned to unlock smartphone devices. The use of biometric technology is growing exponentially for the purpose of user authentication in industries such as government, retail, and now financial services.

With the growing number of data breaches, banks are being pressured to get away from personal identification information and towards a more impenetrable system. A survey conducted by the Bureau of Financial Institutions found that 75 banks and credit unions' losses due to data security breaches reached a total of over $2.1 million US. This is a significant loss that financial institutions must address in order to reduce fraud rates and protect users worldwide.

For many years, law enforcement agencies and governments have been using biometric technology for accurate identification, which has proven to be extremely successful in tracking data. Biometric password management increases authentication accuracy by ensuring that the right person has access to the right information.

Biometric technology however, does not work 100% of the time. Some iris scanners won't work with colored contacts, and eyeprint ID doesn't work if you can't hold your mobile device still enough for the scanner.

Apple's Magic Toolbar is a good example of how little time and effort it takes to authenticate a user due to the fact that all you have to do is touch the ID pad.

- ***Is It Secure and Safe?***

A main concern banks have is the threat of hackers stealing their customers' biometric data. Biometric authentication protects user credentials from being stolen as each physical trait is unique to each person and cannot be shared, duplicated, or easily forged.

The banks themselves are not keeping caches of actual fingerprints or eye patterns. Rather, they are creating and storing templates, or complex numerical sequences, based on a scan of a person's fingerprint or eyeball. It is possible that hackers could use the biometric template to penetrate the system. As a result, some organizations are implementing extra safeguards. For example, some voice authentication systems prompts the user to prove it is a living customer and not a recording. Many eye scans require users to blink or move their eyes to prevent a hacker from using a photo to gain access. In addition to these safeguards, banks also need to consider multi-factor authentication for an added layer of security.
MFA can be a combination of something the user knows and something the user is such as a set physiological traits that may include fingerprint, iris pattern, or voice recognition, that make it almost impossible to hack.

Each human biometric characteristic is unique such as fingerprints, finger vein patterns, palm vein patterns, iris patterns, etc. Therefore, all of these modalities are hard to forge, copy, or spoof. Moreover, biometric technology is now more advanced with multi-factor biometric devices that are capable of capturing both fingerprint and finger vein images in one single scan. The use of biometrics as an alternative to passwords or in combination with passwords as two factor authentication is now considered the most secure form of security to prevent data breaches due weak passwords.

A biometric-based system consists of the following five main components: data collection, feature extraction, storage, classification and decision. Descriptions of each component are explained below:

- Capture component
- Feature Extraction component
- Storage component
- Classification component
- Decision component
- Enrolment process
- Authentication or verification process

The design objectives of a source authentication scheme should include the following:
Robustness of the fingerprinting method: It is what distinguishes one user from another which can be a particular pattern of frames. It used must be robust to efforts of a user to remove this distinguishing information.
Collusion problem: when a group members work together to use the set of differently watermarked streams to create a copy of the content. This content cannot be determined to contain the fingerprint of any of those receivers collusion is happened [12].
Asymmetric fingerprinting: Asymmetric fingerprinting allows the sender to identify the receiver of a recovered copy of data without knowing the fingerprinted data. Hereupon, the sender is not qualified of distributing the data.

C. Biometric system performance

- False Match Rate (FMR): an empirical estimate of the probability (the percentage of times) at which the system incorrectly declares that a biometric sample belongs to the claimed identity when the sample actually belongs to a different subject (impostor).
- False Non-Match Rate (FNMR): an empirical estimate of the probability at which the system incorrectly rejects a claimed identity when the sample actually belongs to the subject (genuine user).
- Equal Error Rate (EER): The rate at which FMR is equal to FNMR.
- False Acceptance Rate (FAR) and False Rejection Rate (FRR): FAR and FMR are often used interchangeably in the literature, so as FNMR and FRR. However, their subtle difference is that FAR and FRR are system-level errors which include samples failed to be acquired or compared.

$$FAR = \frac{Number\ of\ imposter\ Accepts}{Number\ of\ imposter\ Attempts}$$

DOI: 10.15680/IJIRCCE.2017. 0504146

- False Rejection Rate (FRR) False rejection rate has been Represented the percentage of times. This error rate is defined as follows:

$$FRR = \frac{Number\ of\ genuine\ Rejects}{Number\ of\ Genuine\ Attempts}$$

- True Acceptance Rate (TAR): It is defined as 1-FRR.
- Weighted Error Rate (WER): It is defined as the weighted sum between FNMR

  (FRR) and FMR (FAR).

D. Biometric requirements

1. Totality
2. Uniqueness
3. Perpetuation
4. Collectability
5. Acceptability
6. Performance
7. Circumvention

Biometrics offer the most secure and appropriate approach compared to techniques such as knowledge based and token based as it does not rely upon users remembering anything. The physiological based biometric approaches provide stronger protection as they are very unique between users and difficult to rehabilitate. The behavioural based biometric techniques join to offer more phenomenal and continuous protection as they can be performed during user normal interaction with a device. These days, for the purposes of identification and authentication, many biometric techniques such as fingerprint recognition and face recognition have been implemented.

III. PROPOSED METHOD

In this paper, different biometric techniques were investigated: behavioural profiling, keystroke dynamics and linguistic profiling. After examine the performance of each single biometric, the final experiment has been shown these findings through the fusion of the three individual techniques. For single modal biometric technique, the general biometric authentication system is illustrated in Fig.2.

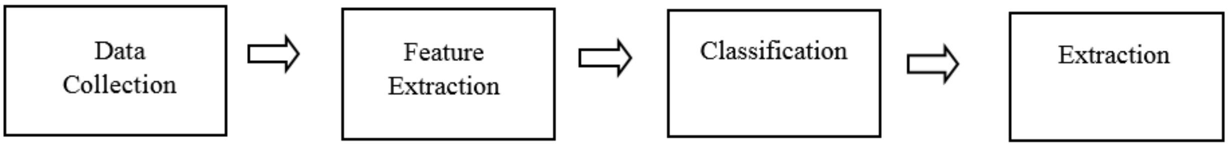

Fig2: Proposed Biometric system

Channel Manager is middle-ware software. It integrates Mobile Banking to core banking solution has been selected in our method. Channel Manager provides an API in form of web services to handle transactions or queries expected from Mobile Banking [13].

Requests only from known entities like mobile Banking and some other applications has been accepted from channel manager. For each entity which wish to perform an operation, it must get registered with Channel Manager Application. For each entity provide a separate shared secret key. Entity will be responsible to preserve this key securely, and use it to generate a checksum for every request sent out and verify checksum by Channel Manager Application for every request received [13]. In Channel manager there is two security layers:

1. Authentication

2. Authorization

As Authentication each entity which wishes to perform an operation is registered with Channel Manager. Each Entity is known as Vendor. Request will be rejected if any of attributes not permitted, or request specific mandatory attributes are not present, or attribute specific values does not pass through basic validation checks here, Password of the Service is in Encrypted format

IV. Conclusion and Future Work

To conclude, the research has been shown all the objectives initially set out in, with a series of experimental studies undertaken for the development of a multi-modal biometric technique. The full achievements are shown below:

A full investigation of the impact of mobile phone in Mobile- Banking. A comprehensive review of biometric authentication techniques.

A deep study into authenticating users based on individual and multi-level biometric technics. Finally, our proposed method has been discussed. Our method has been selected two parts of Authentication and Authorization. For Authentication, channel manager has been selected which is a middleware software. In addition, our method will authorize the Message format with Check sum, which is encrypted with 'SHA-256' format.

References

1. Ashok Bahadur Singh,"Mobile banking based money order for India Post: Feasible model and assessing demand potential", International conference on emergingeconomies-Prospects and challenges (2012)
2. Jeong, B. K., & Yoon,"An Empirical Investigation on Consumer Acceptance of Mobile Banking Services", Business and Management Research, 2(1), 31-40, T. E. (2013)
3. J. D. Pitts, "Surfing the Payment Channels, Mastering the Fraud Tsunami", JDP Enterprises, Carrollton, TX, (2010).
4. Balebako, R., & Cranor, L., "Improving App Privacy: Nudging App Developers to Protect User Privacy", Security & Privacy, IEEE, 12(4), 55-58, (2014)
5. Akhtar, Z., Fumera, G., Marcialis, G.L., and Roli, F. (2012) "Evaluation of multimodal biometric score fusion rules under spoof attacks", Proceedings of the 5th International Conference on Biometrics, pp.402-407
6. Aol tech (2011) "Orange and Barclaycard launch 'Quick Tap' NFC mobile payments in the UK", available at: http://www.engadget.com/2011/05/20/orange- andbarclaycardlaunchquick- tap-nfc-mobile-payments-in/
7. AxxonSoft (2011) "Face Recognition", available at: http://www.axxonsoft.com/integrated_security_solutions/face_recognition/index.php?phrase_id=3032106 [5] Berg Insight (2011) "Mobile Money in Emerging Markets", available at:http://www.berginsight.com/ReportPDF/ProductSh et/bi mm1-ps.pdf
8. Bours, P. and Shrestha, R. (2010) "Eigensteps: A giant leap for gait recognition", In 2nd International workshop on security and communication networks (IWSCN), Karlstad, Sweden.
9. Business Wire, (2013) "Barclays Uses Nuance Voice Biometrics to Identify Customers by the sound of their voice", available at: http://www.businesswire.com/news/home/20130508 05400/en/Barclays-Nuance-Voice-Biometrics-Identify Customers-Sound
10. Bustard, J.D. and Nixon, M.S. (2010) "3D morphable model construction for robust ear and face recognition", Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), pp.2582-2589
11. Cha, B.H. (2009) "Robust MC-CDMA-Based Fingerprinting Against Time-Varying Collusion Attacks", IEEE Transactions on Information Forensics and Security, vol.4, no.3, pp.302- 317
12. Leili. Nosrati, Dr. Amir Masoud Bidgoli, "Security Assessment of Mobile –Banking", IEEE International Conference and Workshop on Computing and Communication (IEMCON2015), University of British Colombia, Vancouver, Canada, October 2015, ISBN: 978-1-4799-6907-4.

DOI: 10.15680/IJIRCCE.2017. 0504146