ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

Mobile Banking and its Security

Dr. S. Krishnaveni[1], N. Sathyadevi [2]

Assistant professor, Department of Computer Applications, Pioneer College of Arts and Science, Coimbatore, India[1]

Student, Department of Computer Applications, Pioneer College of Arts and Science, Coimbatore, India [2]

Abstract: The most of the people are using in Mobile Banking option. It is the easy way to transacting the amount. We can easily download this application on our Smartphone and we should access in this mobile banking option. If we want access the mobile banking, the security was very important think. So there are variety of securities are available like NFC security, QR security and etc. As millions of dollars have been exhausted on building mobile banking systems, reports show that potential users may not be using the systems, despite their availability, as they are not aware its benefits, uses and how they should depend and trusted it. This manuscript investigate the differences between using Smartphone as a platform for authentication, using near field communication (NFC) and other applications in banking processes as well as security of each [16]. Mobile banking is attractive because it is a convenient approach to perform remote banking, but there are security shortfalls in the present mobile banking implementations [17].

Keywords: Mobile Banking, Smartphone, NFC, Remote Banking, Security, Protocol

I. INTRODUCTION

Cash dealings placed over Internet are believed to be executed in real-time and have become extremely sensitive, since, shortly after their execution, they become very hard to recover. Modern Internet banking services, offering payments to freely selectable beneficiaries, follow the general advance of establishing at login a strongly authenticated and encrypted communication channel between the client end-device and the bank's server [1]. In the past decade, the number of online banking users has increased rapidly.

This has led many developers to investigate more convenient methods for customers to perform remote banking transactions. Mobile banking is a new convenient scheme for customers to perform transactions, and is predicted to increase as the number of mobile phone users increases [2]. The modern Internet environment is unimaginable without online payments. According to reports, 2012 saw over a billion online purchases worth a total of more than $1.2 trillion. Today, 60% of users regularly use the Internet for banking and buying online[2]. Security experts tend to believe that data is most at risk when it's on the move. Data must be accessed and used by employees, analysed and researched for marketing purposes, used to contact customers, and even shared with key partners. Every time data moves, it can be exposed to different dangers [3]. The main idea of this mobile banking system is to provide door step banking in the rural areas.

The bank should employ special persons who are licensed as the Business Correspondents (BC) to carry a micro bank machine with them. Each BC will be allocated to a particular area and they are provided a hand held banking device.The customer who needs this micro bank service must call the customer care of the corresponding bank and have to inform whether he wants to withdraw/deposit money[4]. The bank server will choose the appropriate BC. The server will send OTP to the customer. Once the BC reaches the customer he will cross check with it and after the verification, the transaction will be started. Initially the device will be unlocked by the banker. This device can run in both offline and online mode. In online mode, the details about the customer will be directly retrieved from the server automatically. In the offline mode the customer have to give the details such as customer name, account number. The time limit will be enabled [5].

II. WHAT IS MOBILE–BANKING?

Mobile banking and Internet banking are very similar, except you are using a smart phone to bank alternately the computer. The applications of many smartphones connect you directly to your bank, allow you to transfer money, and some banks even allow you to make deposits by taking a picture of the check[6].In the mobile banking option we can be transacting our amount anytime, anybody and anywhere.

Mobile devices, smartphones, and tablets can be taken here and there easily. Furthermore, they provide users access to personal and financial data easy via applications that allow the movement also locally storage of data on the devices and allow data to be sent and to be stored with a third force. Although, they can also be robbed, poison with malware and fraud. Howbeit, smartphones are here to stay.

Through the web browser on the mobile phone, to achieving the bank's web page via text messaging, or by using an application downloaded to the mobile phone, the mobile banking can be done[7]. Bank management technologies are among the major changes in internal banking systems that also have exercised a positive influence on banking achievement and propriety[8].We can getting the most of the benefits to using the Mobile Banking. Some mobile banking benefits are mentioned here.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

Benefits of mobilebanking :

If we want to use the mobile banking option, we got more benefits like saving our time, we don't go the bank in spit of we can do our process.With mobile banking, customers can do their banking activities anytime, anywhere, and cheaper [9]. In other words, the bellow points have shown the benefits of mobile banking.

- Saving time and saving energy.
- Easy to use.
- Reduce cost.
- More suitable than internet-banking[10].

III. SECURITY OF MOBILE BANKING

Different types of securities:

Client's financial security is highly important, which online banking could not be managed without it. Likewise the reputational risks to the banks themselves are important. Financial institutions have set up different security processes to reduce the risk of illegal online access to client's records, but there is no reliability to the various approaches adopted [11].

A) NFC security

After confirming deal on the Smartphone display, the client holds his account card up to the phone. The card generates the TAN and transmits it via NFC to the phone. This is more secure procedure than the text-message TAN, in addition it is easier than using a TAN generator, as further device is not needed nor does it cost more to start up or run. One in four smart phones on the market is NFC capable – and banks are already planning to introduce NFC-capable account cards [12].

B) ATM Security

ATM safe has been the always targeted by criminals, sometimes in quite violent ways. However, most recently, attackers have turned their attention equally to soft assets in the ATM, such as PINs and account data. Criminals use this stolen information to create imitation cards to be used for fraudulent transactions include ATM pull, purchases with PIN at the market, and purchases without PIN in card-not- present environments. PINs and account data are assets belonging to card holders and issuers. They are inevitably in "clear" form at the ATM, when the card and PIN are entered. By attaching, for example, a pinhole camera and a skimmer to the ATM, a criminal can steal PINs and account data before they can be securely processed by the ATM. These attacks require a relative low attack potential, in terms of both skills and material that is commercially available [13].

C) Credit cards Security

Identity theft can be categorized as the second type of fraud, a relatively new crime that is getting more serious. Perhaps the most prevalent use of identity theft involves credit cards. Criminals somehow obtain important personal information, such as Social Security numbers, credit card account numbers, or credit histories [14]. In addition to its costly drain on banks, these problems have the latent to erode consumer confidence in the credit card industry. Clients concerns about the security of credit cards and confidential information need to be addressed. Otherwise, consumers may become reluctant to continue using credit cards as freely as they do now [15].

D) Debit card Security

A debit card is no more or less secure than a credit card. After all, it's just a piece of plastic that can be used by anyone who forges signature on a receipt or orders something from a Web site. But debit cards are different. Under federal law, if a debit card is reported as stolen to bank or brokerage within 48 hours of the theft occurring, the most client will be held responsible for is the first $50 of purchases made with stolen card. If client wait between two and 60 days to report the theft, he'll responsible for up to$500 [18].

E) QR Security

The variation in clients acceptance of QR codesamongst various nationalities Display that people have different concerns about security sensitivity when using with QR codes [19].QR codes are absolutely secure standard for data encoding in their present state. There is, however, great room for improvement. New security standards such as Symmetric Encrypted QR codes, Public Key Encrypted QR codes, and Signed QR codes can be implemented within current QR standard [20].

Algorithm for Handheld Banking System:

The following algorithm steps are used to how to handle the Mobile banking system.

Step 1: Select config mode or demo mode. In config mode,record the customer details. In demo mode, click proceed.

Step 2: Once home screen displayed, receive the transaction details.

Step 3: The time limit and the distance limit are enabled.

Step 4: The customer details are shown.

Step 5: The fingerprint verification of both the customer and BC are verified.

Step 6: The account number, pin number are given by the customer.

Step 7: Money transaction takes place.

Step 8: The balance amount will be sent to the server as SMS through GSM

Step 9: The details such as the customer account number, transaction time, balance amount are printed and the receipt is given to the customer [21].

IV.ARCHITECTURE OF GSM AND GPRS SEQURITY

Global System for Mobile Communications (GSM) is the most popular standard for mobile phones in the world. The following diagram shows the basic structure of the

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

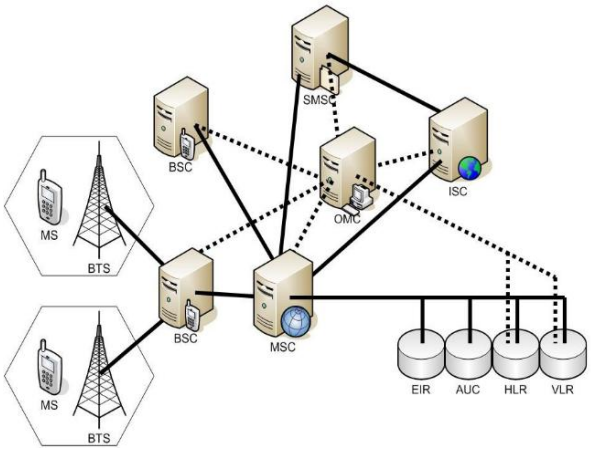
International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

GSM architecture; GSM provides SMS and GPRS (General Packet Radio Service) services.



Key:
MS -Mobile station
ISC –International Switching Centre
BTS -Base Transceiver Station
EIR –Equipment Identity Register
BSC -Base Station Controller
AUC- Authentication Centre
MSC -Mobile Switch Centre
HLR – Home Location Registry
OMC -Operation and Management Centre
VLR –Visitor Location Registry [17]
SMSC -Short Message Service Centre

Figure 1 : GSM Architecture

Secure Architecture of Mobile banking
The secure architecture of mobile has been divided to seven layers. From bottom to upper layers these layers are secure layer, applets layer, middleware layer, mobile application layer, communication layer, services broker layer and mobile service provider layer. These 7 layers can implement the secure mobile transaction systems and a framework for designing the system [22].

Security of the Secure GPRS Protoco:
The following subsections describe how the Secure GPRS protocol conforms to the general security requirements.

a) Confidentiality
This protocol has been designed to take care of the core banking security requirements. It ensures confidentiality of data between the bank and the mobile application through the use of AES encryption and one time session keys.

b) Integrity
In order to ensure integrity of data being communicated the protocol detects any changes made to the data on its way to either the bank server or mobile application through the use of RSA digital signatures.

c) Authentication
The protocol ensures both client and server trust and authenticate each other prior to sharing sensitive information. Mutual authentication is established by the use of SGP (Secure GPRS Protocol) certificates. Each mobile application is packed with the server s certificate, in this certificate there is the server s public key. This public key is used to authenticate the server. The server also uses the client s SGP certificate to authenticate clients.

d) Availability
In order to avoid replay attacks the bank server detects stale messages by checking the timestamps in each message it receives. The Secure GPRS Protocol is an abstract protocol which has been designed to run on any platform and can be implemented in any programming language[17].

Secure GPRS protocol
The Secure GPRS protocol is a tunnelling procedure that has been designed to take care of security in M-commerce applications. We have used this protocol to create and conduct secure connections between mobile devices and the bank servers. The Secure GPRS protocol consists of two main components; an initial client server handshake and the transfer of data packets (SGP record protocol) using the created secure tunnel and exchanged cipher suites. The SGP protocol uses some principles of Pretty Good Privacy (PGP) as described in [27].

Protocol message components (Message Structure)
Each SGP message sent between the client and server has 3 components i.e. the message timestamp, message, and the message type. The message timestamp is used by both the client and server to prevent replay attacks, and the message type is also used by both the client and server to identify the message sent. Figure 2 below illustrates this message structure.

- Error message
- Handshake message
- Go-Ahead message

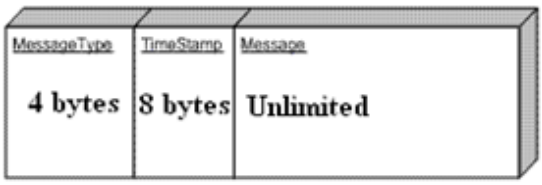


Figure 2: Structure of message sent [17]

Different types of protocols of mobile
1)Secure Electronic Transactionlection (SET) protocol
SET is the collection of security protocols which enables users to employ the existing private credit card payment infrastructure on an open network, such as internet in a secure fashion. The SET protocol supports three types of

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

transaction steps which are property request, authorization of Payment and Payment grab [23].

2) IKP Protocol

IKP is another collect of protocols. IKP has three parties. This protocol is based on public key cryptography [20]. The important drawback of SET and IKP Protocol is that they can be successfully implemented for wired networks in computation and security part. These two protocols are based on public key cryptography which involves encryptions and decryptions. Both of them uses RSA algorithm for encryption.At last payment gateway which has an important role between issuer and acquirer in transaction.Mobile networks have limitations such as low power storage capacity, computational capacity, resources, battery constraints, and so on [24].

3)Mobile ID protocol

The Mobile-ID protocol carries the context information of the man in the middle from the mobile client to the Mobile-ID server which then compares this information with the information belonging to the intended service provider and stops the protocol by notifying the mismatch [25].

4)GPRS Protocol

GPRS is a stand-alone medium for transporting packet data without overlying security protocols has proven vulnerable to some security attacks with evidence and confidence mechanisms having been cracked. This has led tothe implementation of overlying protocols such as WAP so as to enforce the security of transporting data over GPRS. Even though this protocol provides solid security for banking transactions there are some slight loopholes that could prove susceptible for mobile banking. A handshake algorithm of e-banking transaction has been presented between a client and a Bank Server. In addition, a general risk-analysis tree is presented which indicates all possible risks that each node in the e-banking system can face. This can help to protect each element from possible attack and security measures can be taken [26].

V. CONCLUSION

Using mobile device for accessing banking made customers do their banking jobs independent of time and location. Mobile banking allows customers to take full advantage of the latest technology [25]. The mobile banking technology is very useful technology for the people. In this technology is used to transacting the amount don't go the bank. In the given options are used to securing our mobile transactions. Mobile banking is protected and secure. Banks build in tough security procedures to defend people accounts; banks offer PINs and passwords on accounts; lock-outs and time- outs. After that, the application is locked ensuring others can't attempt to guess the PIN. And after three minutes of inactivity, the application may log users out, in case he forgets to close it [28]. Compared to NFC, QR Code is a much cost-effective and applicable option for banking processes today. Allowing mobile payments via QR Codes will primarily require software updates: First it requires Update to Mobile Application that includes QR Code Scanning and Generation features. Then it require Update to Merchant POS to accept payments processed by your service, no additional hardware is required. Even if small businesses do not have scanners, payment can still be made by the consumer via QR Codes [29].

REFERENCES

[1] T. Weigold and A. Hiltgen, "Secure Confirmation of Sensitive Transaction Data in Modern Internet Banking Services," in Draft paper submitted to WorldCIS 2011 Conference, 2011. [Online]. Available: http://www.zurich.ibm.com/pdf/csc/WorldCIS-draft.pdf. Accessed: Mar. 11, 2016. In-line Citation:

[2] "Protecting your bank account using Safe Money technology," in Kaspersky, 2012. [Online]. Available: http://www.kaspersky.com/downloads/pdf/kaspersky_lab_whitepaper_safe_money_eng_final.pdf. Accessed: Mar. 11, 2016.

[3] "Cyber Security Planning Guide," in Federal communication commission. [Online]. Available: https://transition.fcc.gov/cyber/cyberplanner.pdf. Accessed: Mar. 11, 2016.

[4] " Mun-Kyu Lee, 2014. "Security Notions and Advanced Method for Human Shoulder-Surfing Resistant PIN-Entry", IEEE Transactions On Information Forensics And Security, Vol. 9, No. 4, April 2014.

[5] https://www.circuitsathome.com/mcu/interfacing-lcd- via-spi

[6] Ashok Bahadur Singh,"Mobile banking based money order for India Post: Feasible model and assessing demand potential", International conference on emerging economies-Prospects and challenges (2012)

[7] 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)

[8] J. D. Pitts, "Surfing the Payment Channels, Mastering the Fraud Tsunami", JDP Enterprises, Carrollton, TX, (2010).

[9] Balebako, R., & Cranor, L., "Improving App Privacy: Nudging App Developers to Protect User Privacy", Security & Privacy, IEEE, 12(4), 55-58, (2014)

[10] Md. Shoriful Islam," Systematic Literature Review: Security Challenges of Mobile Banking and Payments System", International Journal of u- and e- Service, Science and Technology Vol. 7, pp. 107-116(2014)

[11] "Students develop secure new procedure for online banking," in Phys. Org., 2003. [Online]. Available: http://phys.org/news/2013-03-students-procedure-online- banking.html. Accessed: Mar. 12, 2016.

[12] "Information Supplement: ATM Security Guidelines," in Security Stranded counicle, 2013. [Online]. Available: https://www.pcisecuritystandards.org/pdfs/PCI_ATM_Security_Guidelines_Info_Supplement.pdf. Accessed: Mar. 12, 2016.

[13] K. P. Mueller, "Money matters: The dangers of debit cards," Better Homes & Gardens, 2016. [Online]. Available: http://www.bhg.com/health-family/finances/tips/money- matters-the-dangers-of-debit-cards/. Accessed: Mar. 12, 2016.

[14] D. Akers, J. Golter, B. Lamm, and M. Solt, "FDIC: FDIC banking review - A survey of current and potential uses of market data by the FDIC," in Federal Deposit Insurance Corporation, 2010. [Online]. Available: https://www.fdic.gov/bank/analytical/banking/2005nov/article2.html. Accessed: Mar. 12, 2016.

[15] "QR code," in Wikipedia, 2016. [Online]. Available: https://en.wikipedia.org/wiki/QR_code. Accessed: Mar. 12, 2016.

[16] Aody SH. Mahmoud General Directorate of Curricula Ministry of Education, Baghdad, Iraq, "Mobile Technology in Banking

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

ICITCSA 2017

Pioneer College of Arts and Science, Coimbatore

Vol. 6, Special Issue 1, January 2017

Process"- International Journal of Engineering Science and Computing, March 2016, Pg.No 2290.

[17] Kelvin Chikomo, Ming Ki Chong, Alapan Arnab, Andrew Hutchison Data Networks Architecture Group Department of Computer Science University of Cape Town Rondebosch 7701, South Africa- "Security of Mobile Banking"

[18] K. Krombholz, P. Fr¨uhwirt, P. Kieseberg, I. Kapsalis, M. Huber, and E. Weippl, "QR Code Security: A Survey of Attacks and Challenges for Usable Security," in SBA Research. [Online]. Available: https://www.sba research.org/wp-content/uploads/publications/llncs.pdf. Accessed: Mar. 12, 2016.

[19] K. Peng, H. Sanabria, D. Wu, and C. Zhu, "Security Overview of QR Codes," in Massachusetts Institute of Technology. [Online]. Available: https://courses.csail.mit.edu/6.857/2014/files/12-peng- sanabria-wu-zhu-qr-codes.pdf. Accessed: Mar. 12, 2016.

[20] B. Barrett, "Your phone will replace your wallet at the ATM, too," in Gadget Lab, WIRED, 2016. [Online]. Available: http://www.wired.com/2016/01/cardless-atms/. Accessed: Mar. 12, 2016.

[21] B. Darshini, PG Scholar, Department of Embedded System Technologies, Sri Ramakrishna Engineering College, Coimbatore, India- "Handheld Cash Deposit and Withdrawal Mobile Banking Device", Middle-East Journal of Scientific Research 24 (S1): 83-87, 2016

[22] Hameed Ullah Khan, "E-banking: Online Transactions and Security Measure", Research Journal of Applied sciences, Engineering and technology 7(19): 4056-4063, (2014)

[23] G. Bella, F. Massacci, and L. C. Paulson,"The verification of an industrial payment protocol: The SET purchase phase" In V. Atluri, editor, 9th ACM Conference on Computer and Communications Security, pages 12–20. ACM Press, (2002).

[24] Haiyong Xie, Li Zhou, and Laxmi Bhuyan, "Architectural Analysis of Cryptographic Applications for Network Processors", Department of Computer Science & Engineering, University of California.

[25] Leili Nosrati, Amir Massoud Bidgoli ," A Review of Differenet Encryption Algorithems for Security of Mobile- Banking"- International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869 (O) 2454-4698 (P), Volume-5, Issue-3, July 2016

[26] ElBahlul ElFgee, Ahmed ARARA, "Technical Requirements of New Framework for GPRS Security Protocol Mobile Banking Application", International workshop on intelligent techniques in distributed systems (ITDS), Procedia Computer Science 37, (2014).

[27] Stallings, W. Network Security Essentials Applications and Standards, international second ed. Prentice Hall, 2003.

[28] "ATM User Manual," in Oracle FLEXCUBE ATM User Manual. [Online].Available:https://docs.oracle.com/cd/E52129_01/PDF/UserManual/AT M%20User%20Manual.pdf. Accessed: Mar. 12, 2016.

[29] Bhawani, "How to transfer your files & pictures on NFC enabled Android phones," in Tips for Mobiles, Android Advices, 2011. [Online].Available: http://androidadvices.com/how-to-transfer-your-files-pictures-on-nfc-enabled-android-phones/# 7avwAtoqigtOsD5r.99. Accessed: Mar. 12, 2016.