IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol.-7, Issue-8, Aug 2019 E-ISSN: 2347-2693

Comparative Study and evolution of Mobile Banking Security Solutions and Comparision between Various Solutions

Mubina Malik[1*], Shreya Banker[2]

[1,2]CMPICA, Charotar University of Science and Technology (CHARUSAT), Changa

Corresponding Author: mubina.a.malek@gmail.com, Tel.: +91 9879650192

DOI: https://doi.org/10.26438/ijcse/v7i8.227232 | Available online at: www.ijcseonline.org

Accepted: 12/Aug/2019, Published: 31/Aug/2019

***Abstract* —** Due to the rapidly increasing use of mobile phones, it is essential to provide a secure solution for mobile phones; with the evolution of mobile commerce, it is obvious to provide a secure and efficient solution for the mobile environment. Day by day usages of mobile devices is huge and consumers are getting familiar with the various purposes of devices such as mobile banking. This paper focuses and describes various types of mobile banking methods and their possible security solutions. In the first part mobile banking solutions using contactless technology – Near Field Communication (NFC) is discussed with its limitations in terms of security. In addition, we also address the security weaknesses of Wireless Application Protocol (WAP) and Wireless Transport Layer Security (WTLS). To overcome the above mention weaknesses, in the second part different solutions of mobile banking with Public Key Infrastructure such as MPKI, WPKI, ECC, LPKI are discussed with its limitations and possible solutions to overcome the limitations.

***Keywords* —** NFC, TSM, WAP, PKI, GSM, GPRS, SIM, SMS, Mobile PKI, Wireless PKI, Lightweight PKI.

I. INTRODUCTION

Due to the increased use of on-line commerce, Security in payment methods using mobile phones are becoming more challenging in today's era. Current payment methods that can be used for online transactions such as using the internet have a drawback in terms of usability, functionality costs and security. One of the widely used and reliably authorized ways of electronic payment transactions is with the digital signature in PKI framework.

Adopting Mobile banking technology and services is challenging in terms of the perception of insecurity. Author Federal Reserve surveyed a significant barrier to the use of mobile banking products and services. In the survey, he found 48% of the respondents cited they are concern about the security of mobile banking and because of that, they are not using mobile banking. In the same survey respondents were asked to rate, the security of protecting personal information using mobile banking and 32% response was very unsafe, while 34% respondent replies they were not sure of the security [1].

The main reasons for mobile operators of mobile penetration are to provide additional services such as mobile banking; GPRS based interactivity through applications and internet banking etc. This Howbeit requires a secure end to end robust solutions. Mobile banking or online transactions are more feasible because it is a convenient method to perform banking from anywhere at any time. But it brings lots of security concern in the actual implementation such as problems with GSM network, GPRS protocols, SMS, Security. In this paper, different methods and solution of mobile banking with its comparison is discussed. Majorly paper focused on end to end security framework using PKI as well as wireless protocol used for mobile banking. In Mobile Banking or Mobile payment different features of payment systems motivate diversity like Time of payment, Payment amount in micropayments, small payments or macro payments, anonymity issues – there are different degree of anonymity in many payment systems only partial or no anonymity can be provided, Security requirement – integrity, authentication, confidentiality, availability, authorization, reliability [2].

Section I contains the introduction of the need for security in mobile banking, Section II describes the types of mobile payment technology, Section III defines various mobile E-payment and banking solutions with its optimal solutions, Section VI gives a pictorial view with flow of evolution of technology and solutions to mobile banking security, Section V focuses comparison of various solutions with its limitations, Section VI concludes the research work and gives an idea of the best technology/solution for mobile banking security used currently.

II. MOBILE PAYMENT TYPES

Two different mobile payments are available that is through a mobile application- Mobile Wallet and through Contactless technology – NFC. Mobile Application includes Mobile Wallet through PayPal and Mobile Carrier Network.

According to Forrester Research by Daniel P. Hawley, LAPTOP Senior Writer stated that 50% of mobile users are attracted towards in-store mobile banking options still, the number is not good in terms of using mobile payments. Virtual wallets are going through serious problems in terms of conflicting formats and usability issues to security.

In the field of mobile payments use of Near Field Communications (NFC) payments are growing. End to end communication-using NFC enabled point of sale using radio frequency identification. In NFC mobile phones need not have to touch each other or point of sale to transfer data. Examples of NFC enabled payment system are Google Wallet, ISIS, PayPal. In Google Wallet and ISIS user can able to set the password PIN to complete the transaction which makes hacking difficult. NFC signal in Google Wallet and ISIS have a very short range and hackers can take data from NFC device by rubbing NFC reader, but hacker has to be very close to users during payment app are running and open. The use of NFC is governed by ISO 18092 standards and it has some limitations such as data transfer rate is limited to 424 kbps, it supports communication up to 0.2 meters and it does not offer native encryption [1]. Due to NFC communication enabled automatically where two compatible devices are within a short-range and no native encryption implemented NFC must be defined with cryptography module in mobile devices to bring more security.

III. MOBILE E-PAYMENT/BANKING SOLUTIONS

A. TSM –Architecture in NFC

Trusted Service Manager is introduced in the NFC as a trusted third party which is used to manage the deployment of mobile applications.

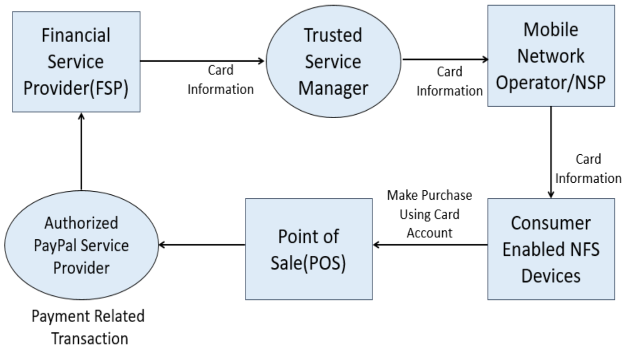
Financial Service Provider(FSP)
Card Information
Trusted Service Manager
Card Information
Mobile Network Operator/NSP
Card Information
Make Purchase Using Card Account
Authorized PayPal Service Provider
Point of Sale(POS)
Consumer Enabled NFS Devices
Payment Related Transaction

Figure 1. Trusted Service Manager Architecture

TSM sends secure data through the mobile network to the secure element in mobile phone, it also handles the life cycle of a mobile device and deactivates the NFC chip in case of any theft. Only individual organization consideration is not sufficient and needs a strong inter-organization relationship. Card information is stored inside SIM card and that can be possible user are moving card from one device to another device that is not controlled by bank and because of this reason, it requires to ensure true distribution of payment card information and some SIM controlling mechanism. A possible solution for mobile threats at system level is TSM (Trusted Service Manager) Architecture that is a combination of technical as well as business boundaries to provide secure mobile environment [3].

B. WAP protocol

The wireless approach is used for the communication between devices after NFC. A consumer can realize more functionality using Wireless Application Protocol (WAP). In Wireless approach customer are more concern about how the information is transfer. WAP uses the encryption process for secure data transmission between the bank and the users but the challenging problem is protection and protection process. As bank transactions have sensitive data encryption process required more powerful computing methods and high storage capacity. Internet banking uses a powerful computer system and complex encryption system to ensure the security but our focus is on mobile banking that uses mobile devices which have very low computational capacity and therefore it fails to apply complex cryptographic methods. WAP uses a wireless identity module (WIM) perform digital signature using private keys and certificate verification using public keys which is difficult for hackers to get keys which are stored on mobile devices. The WIM can be compared to the SIM of the GSM. WAP is part of an open mobile alliance and it's a protocol stack which is equivalent as an internet protocol stack (TCP/IP). This architecture mainly focuses on a mobile phone, internet, and WAP gateway. The communication between mobile devices and WAP Gateway is secured with WTLS whereas the communication between WAP Gateway and the internet is secured with SSL/TLS. In this architecture WAP Gateway first decrypts the encrypted WTLS (Wireless Transport Layer Security) and has to encrypt it again using SSL/TLS. Advantage of WAP is bearer independent that is GSM, PDA or mobile phones.

It was identified that security is the vulnerability in WAP, which is safe for the data to be sent from the gateway to the end-users but due to data available for a short time on a gateway, it may be possible for the hackers to attack and access the information [4]. It was identified that because of the unreliable connection, low speed and high-cost users are not using mobile banking over WAP.

C. PKI (Public Key Infrastructure)

Deploying PKI in mobile banking is quite challenging. It was noted that two keys are an important one for encryption which is a public key and one for decryption which is a private key. PKI in mobile banking woks as follow - each mobile user is register with his/her public key and listed in public directory. If mobile users want to send data to the bank server then banks server gives public key from the directory to the mobile users for encrypting the data and that encrypted data is sent to the bank application server. Now only the bank server has the private key to decrypt the data. Moreover, mobile users have their private key to digitally sign the data by encrypting the hash. Although everyone can access public key directories they must be protected from misrepresentation and abuse. PKI pair key is generated for a user which is called asymmetric key cryptography, the public is derived from the private key so it is not feasible to derive private key from public key. Sender send the message/data using the public key of receiver then the sender can be sure that secure data can only be decrypted by correct recipient and not by the other. Therefore, there is a need to implement appropriate infrastructure called PKI.

D. Mobile PKI (MPKI)

Mobile PKI is the appropriate solution for this because of the listed reasons: 1) Ensure inter-operability for operationalized on any channel (GPRS, SMS, WAP based), 2) Customer protection to ensure a standard authentication form across all channels. 3) Valid Identification can be associated with a user validation by trying DSC issuance 4) Data Protection through PKI Technology and recognize at the best form of security. 5) Authentication is the Key pair concept ensures that authenticity of the sender/device can be ascertained.

PKI has various solutions in terms of security that is traditional PKI, ECC Based PKI, WPKI and LPKI in this paper various PKI solutions as well as its comparison is discussed.

E. Wireless PKI (WPKI)

WAP is used for mobile security but that has some disadvantages 1) WAP does not provide end to end security because the data passes through the gateway 2) WAP does not support Proof Of Possession (POP) function in its certificate request message. To remove this problem Y. Lee et al. proposed a wireless CMP suitable for wireless PKI in 2007 and 2008 [5]. In wireless PKI mobile users can request a public key certificate to CA. Then CA performs the authentication and verifies the POP function that will generate the valid private key corresponding to the public key. If verification is done, then it published the certificate/certificate URL on the web or in its directory. Wireless PKI includes some of the limitations for mobile security 1) It requires an out of band user identification to collect ID and password for certificate 2) Issues in certificate request message because of low storage and low computational power.

F. Elliptic Curve Cryptography

Wireless PKI is limited to out of band user identification at CA level. Also, mobile device generates certificate request message itself, which is not possible for all devices which have less storage and low computational power. To remove this limitation Sangram Ray and G.P Biswas proposed Mobile Home Agent (MHA) based mobile –PKI using Elliptic Curve Cryptography (ECC) to perform a number of operations for mobile devices [6].

ECC is encryption techniques based on elliptic curve theory which is used to perform more efficient smaller and faster cryptographic keys. It is not oval shape but it represents a looping line intersecting two axes. ECC generates public keys through elliptic curve equation properties, which is derived from mathematical groups that are a set of values. Mathematical operation can be performed on any two members of the group and generate the third member which is derived from points where the line intersects the axes. That curve point multiplies by a number and produces another number on the curve but it's very difficult to find out that number even if you know the original number. So, the outcome of that ECC based equations is easy to perform but very difficult to reverse in a cryptosystem. Compared with RSA algorithm ECC has less processing time and smaller size key, RSA using 1024-bit size whereas in ECC 160 bit. ECC techniques operate to store all the information of mobile phone and to get a certificate from CA. this scheme also considers the RA to reduce the workload of CA, RA performs user authentication and POP verification. CA will generate ECC based public key certificate on mobile user request with a sign and also send certificate URL to Mobile phones via MHA. This solution is appropriate but it has computational cost.

G. WPKI with ECC based solution

A mobile phone lacks the computing capabilities of PKI services. Because of the technical limitation in processing certificate management protocol (CMP) of wireless environment downloading CRL and verify certificate become very hard. Some of the requirements listed below must be satisfied in wireless internet in compare with wired internet which does not [4].

- Optimal digital signature in the mobile phone which carry shorter key.
- Optimal certificate
- Optimized CMP protocol
- Optimized certificate validation scheme.

To achieve the optimal solution for above requirements WPKI with ECC based solution is best. As discussed above WPKI and ECC solution have its own benefits. Only thing is left is how to verify the certificate? OCSP is the solution to achieve optimal certificate validation.

Process of verifying certificate using OCSP:

New mobile users request for the registration at CA. CA will generate random code specific for each wireless mobile device after that CA generate username and password and store the values along with the random code in the database. After this process mobile user can be authenticated via the credential and can generate public/private keys using a digital signature algorithm. Data is transfer to the authority/another user with username, password and public key. A message digest is generated using hash algorithm using that digest private key and digital signature is generated. A mobile user sends data with public key and digital signature to CA for verification. CA will decrypt digital sign using public key match the digest of user with digest generated by CA. If digital signature verified, then CA issues digital certificate for the user. Files are stored in CA directory and URL of the certificate is sent to the user for communication with other servers and reduces the load on wireless devices such as mobile phones. When mobile device and server interact with each other for transaction then server sends certificate to the mobile users and OCSP server. OCSP server downloads the CRL list and verifies the certificate validity. After verification OCSP server sends response to the mobile users which can be used for the future transactions also, thus reducing the burden for future transactions [7].

Table 1. Optimal solution for Wireless PKI

	Optimal Solution	Benefits
Digital Signature	Elliptic Curve Digital Signature Algorithm (ECDSA) and Data Encryption standards (DES)	Smaller key size
Certificate	X.509	Remove unnecessary data from the certificate an reduce the size of certificate
CMP protocol	Through Wireless bandwidth	Suited to wireless devices
Certificate verification	Through OCSP server	Reduce the load on wireless devices.

H. Lightweight public key infrastructure (LPKI)

Lightweight Public Key Infrastructure (LPKI) is introduced for a mobile environment that has considerably light computational costs because it is based on ECC and uses signcryption[8]. LPKI has several improvements over traditional and wireless PKI. Signencryption is the technique which is used instead of digital signature in LPKI with few steps and effectively decreases the computation cost and communication overheads. As discussed in the above schemes PKI, WPKI which uses digital signature and public-key encryption have two main problems that are low efficiency and high cost. The signencryption scheme is introduced by Zheng in 1997, Sheng also proposed ECC based signencryption that saves computational cost to 58% and communication cost to 40% in comparison with traditional PKI with ECC based implementation [9].

In LPKI method key generation is done at two entities 1) At KGS (Key Generation Server) and 2) at end entities (sender and receiver) [8]. As LPKI uses X.509v3 certificate format it is compatible with other infrastructure and system. In this approach issued certificates are stored in Certificate Repository (CR) which stores certificates in Lightweight Directory Access Protocol (LDAP) directory. LDAP is updated all the time if certificate issued or revoked [10]. LPKI uses AES algorithm for message encryption in which secret key is generated using public-private keys of the involved entities. Any authenticated key exchange protocol can be deployed in LPKI but LPKI can implement EC based and improved version of HMQV key exchange protocol [11]. For both encryption and digital signature LPKI uses single pair of public-private keys. Certificate Validation is performed through CRL, Delta CRL or OCSP in order to obtain revocation status. In LPKI information retrieval and message exchange can be predicted by two modes: 1) Both the sender and receiver individually perform certificate and public key validation. 2) VA gets signencrypted messages through communication link and performs required validation for both sender and receiver.

IV. FLOW OF EVOLUTION OF TECHNOLOGY AND SOLUTIONS TO MOBILE BANKING SECURITY

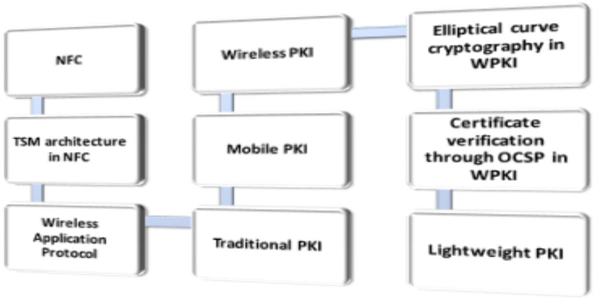
NFC
TSM architecture in NFC
Wireless Application Protocol
Wireless PKI
Mobile PKI
Traditional PKI
Elliptical curve cryptography in WPKI
Certificate verification through OCSP in WPKI
Lightweight PKI

Figure 2. Flow of evolution of technology and solutions to mobile banking security

V. COMPARISON OF MOBILE BANKING SOLUTIONS

NFC	• NFC phones communicate with each other and with NFC enabled points of sale, using radio frequency identification • NFC Enabled Payment System uses PIN password to complete the banking transaction which makes hacking difficult. **Limitations:** • Data transfer rate is limited to 424

	kbps. • Supports communication up to 0.2 meter. • Communication enabled automatically where two compatible devices are within a short-range and no native encryption.
TSM Architecture in NFC	• TSM send the secure data through the mobile network to the secure element in mobile phone and deactivate NFC in case of any theft. • TSM Architecture that is a combination of technical as well as business boundaries to provide secure mobile environment. • Good solution for Mobile threat at System Level (for the users who are not changing their mobile phone) **Limitations:** • It requires to ensure true distribution of payment card information and some SIM controlling mechanism because users are changing SIM and Mobile device frequently
WAP	• WAP devices use a Wireless Identity Module (WIM) which performs digital signatures and certificate verification using public private keys. • Difficult for the hackers to find out the keys which are stored in mobile device. • Good solution for Internet banking but not for Mobile banking. **Limitations:** • Low speed and limited bandwidth • Storage capacity and complex encryption are challenging for mobile device using this solution. • Unreliable connection - data passed through intermediate gateway • Does not support POP function • There are no cookies available to hold session together.
Traditional PKI	• PKI implementation is good solution for internet banking but in terms of security sender cannot be sure that data is decrypted by correct users and need appropriate infrastructure. **Limitations:** • Mobile devices Lacks computing capabilities of PKI services.
Mobile PKI	Overcome the limitation of tradition PKI and suited for mobile.
Wireless PKI	Wireless CMP used for wireless PKI and eliminate the limitation of WAP Approach, Mobile phone generates certificate request itself. **Limitations:** • It requires an out of band user identification to collect ID and password for certificate. • Issues in certificate request message because of low storage and low computational power.
MPKI with ECC based approach	MHA based mobile-PKI using Elliptic Curve Cryptography (ECC) which eliminate limitation of Wireless PKI and perform number of operations for mobile devices [6]. • Less Processing time. • Faster and smaller size key. • Efficient cryptography and difficult to reverse. • Great computation on constrained platforms. **Limitation:** • Computational cost
WPKI with ECC based approach	ECC approach with wireless PKI is the optimal solution for mobile devices. • Smaller Key size used for encryption and digital signature. • Reduce the size of the certificate. • Wireless CMP through wireless bandwidth • Certificate verification through OCSP to reduce the load on wireless devices as well as reduce the burden of future transactions. **Limitation:** • Computational cost
LPKI	LPKI eliminate the limitation of ECC based approach in MPKI and WPKI and efficiently decrease the computational cost and communication overhead for mobile devices and resource-constrained platforms. • Private/public key generation using Elliptic curve • Uses Signencryption EC-based Sign that eliminates the traditional signature problem of low efficiency and high cost. • Eliminate Signature then encrypt scheme that is for tradition approach.

VI. CONCLUSION

This paper is focused on the different solutions for mobile banking and its applications. Mobile banking systems growing very rapidly because of that security needs to be enhanced in mobile phones. Mobile banking security needs secure protocol, secure mobile payment system and secure approach of Public key infrastructure. In this paper, I focused on the evolution of mobile banking security solutions with its limitations and benefits. Concluding this paper NFC with TSM architecture provides system-level security and it is good solutions for the users who are not changing their mobile phones, WAP provides security using digital signature and certificate verification which is good for internet banking but not feasible for the mobile banking because of the low storage capacity and complex encryptions. Public Key Infrastructure is the good security solution for internet banking which requires more computing capabilities, so Mobile PKI and wireless PKI address the limitation of traditional PKI and suited for mobile devices but have some issues in certificate request message, low storage, and low computational power, hence MPKI and WPKI with Elliptic Curve Cryptography(ECC) uses smaller key size, x.509 certificate format and OCSP server and can be implemented for the mobile devices which have less processing power and storage capacity, it also eliminate the issues of certificate request message, in addition it increases the computational cost. Hence, in MPKI and WPKI the computational cost is too high it is not the best solution for mobile banking. Lightweight PKI is used to reduce the limitation of MPKI and WPKI. LPKI uses EC based signencryption which efficiently decrease the computational cost and communication overhead for mobile devices and resource constraint platform. From the above statements, it is concluded for mobile banking security requires ECC based signencryption – single pair keys for digital signature and encryption, OCSP to verify the certificate validity and Lightweight public key infrastructure, which provide confidentiality, integrity, unforgeability, non-repudiation and forward secrecy.

REFERENCES

[1] Venessa Pegueros : “Security of mobile banking and payments” : GIAC (GSEC) Gold certificate, 2012.

[2] S. Schwiderski- Grosch and H. Knopse : “ Secure Mobile commerce”, Electronic And communication engineering journal , Vol. 14, Issue 5, pp-228-238,2002.

[3] Nikolaos Zacharopoulos, An ISACA Emerging Technology White paper: “Mobile Payments, risks Security and assurance issues”, November 2011.

[4] Balachandra Muniyal,Krishna Prakash, Shashank Sharma : “wireless public key infrastructure for mobile phones”: International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.6, pp. 111-118, 2012.

[5] Yong lee, Jaeil Lee, JooSeok Song, "Design and Implementation of wireless PKI technology suitable for mobile phone in mobile commerce”,Science Direct, Computer communication 30, pp.893-902, 2007.

[6] Sangram Ray, G. P. Biswas, “design of mobile public key infrastructure (m-PKI) using elliptic curve cryptography”, International Journal on Cryptography and Information Security (IJCIS), Vol.3, No.1, pp. 25-37, 2013.

[7] Ke Gu,Na Wu,Yongzhi Liu,Fei Yu and Bo Yin : “WPKI Certificate Verification Scheme Based on Certificate Digest Signature-Online Certificate Status Protocol” :Mathematical Problems in Engineering, Volume 2018, Article ID 7379364, 19 pages.

[8] M. Toorani and A. Beheshti, "LPKI - A lightweight public key Infrastructure for the mobile environments," 11th IEEE Singapore International Conference on Communication Systems, Guangzhou, , pp. 162-166, 2008.

[9] Y. Zheng : “Digital signcryption or how to achieve Cost (Signature & Encryption) << Cost (Signature) + Cost (Encryption),” Advances in Cryptology–CRYPTO'97, LNCS 1294, Springer-Verlag, pp.165-179, 1997.

[10] K. Zeilenga,“Lightweight Directory Access Protocol (LDAP): Schema Definitions for X.509 Certificates”, RFC 4523, 2006.

[11] H. Krawczyk : “HMQV: A high-performance secure Diffie-Hellman protocol (Extended Abstract)” : Advances in Cryptology – CRYPTO'05, LNCS 3621, Springer-Verlag, pp.546-566, 2005.

Authors Profile

Mubina Malik in pursed Master of Computer Applications from Sardar Patel University,Gujarat,India in year 2009. She is currently working as an Assistant Professor in Charotar University of Science and Technology since 2013. She has published 2 research papers in reputed international journals including IJETAE, IJIST and it’s also available online. Her paper total citation is 23 and her main research work focuses on Cryptography algorithms, data security, network security, machine learning in cyber security.She has 10 years of teaching experience.

Shreya Banker in pursed Master of Computer Applications from Sardar Patel University, Gujarat,India in year 2010. She is currently working as an Assistant Professor in Charotar University of Science and Technology since 2013.She has published 5 research papers in reputed international journals including Ijist, ijarcsse and ijares and it’s also available online. Her paper total citation is 6 and her main research work focuses on Machine Learning, Big Data Analytics, Data Mining. She has 7 years of teaching experience.