A Review of Differenet Encryption Algorithems for Security of Mobile- Banking

Leili Nosrati, Amir Massoud Bidgoli

***Abstract*— Bank account hacking has caused millions money losses around the world. In addition, there is lots of obvious weakness in the banking system. It is important to achieve how the security aspects in a banking system can influence great lost to the financial institution. This paper reports on the aiming at identifying and classifying Mobile banking payment security challenges. First, different methods of online banking specially, mobile banking have been discussed. In addition, we tried to gather all different protocols of mobile banking system which are used till now, also different security problems which reported. Then, different encryption algorithms were compared. Moreover, our method which has two layers of security has been presented.**

***Index Terms*— online banking, mobile banking, privacy in mobile banking, mobile banking vulnerabilities, security of mobile banking, Privacy in mobile banking**

I. INTRODUCTION

Electronic banking has lots of advantages for both banks and people who use online banking. Such as: it is easy, fast, cost saving and convenience to use. It has changed traditional banking industry. In addition, it is the most sensitive tasks which happened through the internet. Internet-banking, Mobile-banking, and SMS-banking are different parts of online banking .However, in this paper Mobile banking has been introduced.

A. 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 smartphons 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 [1].

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 [2].

Bank management technologies are among the major changes in internal banking systems that also have exercised a positive influence on banking achievement and propriety[3].We provide an overview of the-state-of-the-art of mobile banking security challenges, and a key for reading and interpreting them. In addition, this paper presents a number of interesting findings, including mobile banking challenges of payment security and application of mobile banking.

One of the new challenges of mobile banking is online threats, mobile user always active on online downloading various applications, song and official mail or other personal files over internet.

B. Benefits of mobile banking

With mobile banking, customers can do their banking activities anytime, anywhere, and cheaper [4]. 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

C. Vulnerabilities of mobile banking

1) Distributed Denial of service (DDOS) Attack

DDOS attack is ranked as third highest threat as FBI said. DDOS is the most common attack of banking system. DDOS attack orbit the attack to target system. Before an attack is happen, attacker will be attack network by scanning open ports [5].

2) Malware

Malware is the term for maliciously crafted software code. Moreover, it is possible to perform the following operations for this type of malicious software Account information theft [6]:

- Fake web site substitution
- Account hijacking

3) TCP/IP Spoofing

Here, an attacker gains unauthorized access to a mobile device or a network by making it show up that a malicious message has come from a trusted machine by "spoofing" the IP address of that machine [7].

4) Backdoors

Access to a mobile program that avoided security mechanisms is backdoor. A programmer may sometimes install a back door so that the program can be accessed for troubleshooting or other purposes. Anyhow, back doors have been used by attackers to install themselves, as chunk of an exploit [8].

5) Tamperring

Tampering is an intentional modification of products in a way that would make them harmful to the consumer [9].

6) Exploits

Exploit is a piece of software, or a data which acts as a bug or vulnerability in order to matter surprising behavior to exist on computer software, or hardware [10].

7) Social Engineering and Trojans

Trojans act as no authorized programs. Can delete, block, modify, and copy data. However, Trojan is not like a viruses and worms, it is not able to self-replicate [11].

D. Risks in wireless application protocol

- Eavesdropper attacker
- Unencrypted data during switching between protocols
- Attacker can contact to unencrypted data [12]

E. Risks in servers

- System may crash
- Server may be failed
- Virus may be attack

To prevent vulnerabilities of mobile banking, risks of mobile devices, risks in servers, also risks of protocols there are some security jobs which can done to have a secure mobile transactions such as; secure architecture, secure protocols, also some secure algorithms for encryption.

F. Security needed in mobile commerce

- Transaction privacy
- Authentication of parties
- Proof of transaction authorization by user
- Impossibility of unauthorized payments [13]

G. 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 [14].

Furthermore, 4 security services which are listed in below are critical and necessary for mobile transactions.

- Mobile registration and identity management
- Mobile public key interface (PKY)
- Mobile authentication and authorization
- Secure messaging

Because of the variety of mobile devices and platforms, preparing the security on mobile banking is not easy at all [15].

31% of mobile banking customers are ready to pay for added security features, 63% are eager to switch accounts for better security features, the 71% of the rest are ready to switch accounts for guarantees losses.

Four step-mobile banking risk assessment methods, has been chosen as below [16].

- Assessment method
- Classification of information
- Identify threats and vulnerabilities
- Measure risk and communicate risk

Online threats– challenge of mobile banking is shown in table1 [17].

There are different technologies for authenticating the customer. Such as customer passwords, personal identification numbers (PINs), digital certificates using a public key infrastructure (PKI), physical devices, one time passwords (OPTs), USB plug in or other tokens, transaction profile scripts, biometric identification. As the selection and use of authentication technologies should depend upon the results of risk assessment process, the level of risk protection afforded by each of these techniques are a lot and different.

Crime of finance industry involved various type of common attacks such as tampering (physical), brute force (hacking), and spyware (malware) [18].

TABLE1 Online threats of mobile banking

Broad threats	Phone threats	Online threats
Unauthorized access Malicious hacking Malware, Mobile Viruses	Memory cards, Downloads, Various, Application, Mobile Browsers, Smart cards	Mobile E-mail, SMS, Mobile IM, Voice, Online Games, Gateway

H. Differnet protocols of mobile

a) 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 transaction steps which are property request, authorization of Payment, and Payment grab [19].

b) 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 [21].

c) 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.

d) 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 to the 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 [22].

I. *Review of Encryption Algorithm*

a) DES

DES is symmetric key algorithm based on the backbone concept of Feistel Structure. It is a block cipher that uses a 64 bit plain text with 16 rounds and a Key Length of 56-bit, originally the key is of 64 bits, one bit has been selected as ‘parity’. It was initially considered as a strong algorithm. However, because of large amount of data and short key length it is not used for encryption nowadays [23]. It is highly vulnerable to linear cryptanalysis attacks, Weak keys is also a great issue. DES is also exposed to brute force attack.

b) Triple-DES

Triple-DES was much more complicated version of DES achieving high level of security by encrypting the data using DES three times using with three different irrelevant keys [28]. It uses a 64 bit plain text with a Key Length of 168-bits permuted into 16 sub- keys each of 48- bit length 3DES is exposed to differential and related-key attacks. It is also susceptible to certain variation of man-in-the-middle attack [29].

c) Blowfish

Blowfish is invulnerable against differential related-key attacks, by reason of every bit of the master key holds many round keys that are very much independent, making such attacks very complicated or infeasible [24].
Four rounds of blowfish are exposed to 2nd order differential attacks. So, reliability of Blowfish is questionable due to the large no. of weak keys [25].

d) IDEA

IDEA is symmetric key algorithm based on the concept of Substitution-Permutation Structure. It is a block cipher that uses a 64 bit plain text with 8 rounds and a Key Length of 128-bit permuted into 52 sub- keys. It does not contain S- boxes and same algorithm is used in reversed for decryption. It is also defined to collision. IDEA contains 8 rounds that first 3 rounds appears to highly exposed to key attacks such as key-schedule attacks and related-key differential timing attacks [26] .

e) TEA

TEA is a block cipher that uses a 64 bit plain text with 64 rounds and a Key Length of 128-bit with variable rounds having 32 cycles. It does not contain S- boxes and same algorithm is used in reversed for decryption. TEA algorithm offers the same security level as that of IDEA, it also consist of a 128 bit key size and is known for its simple structure and easy implementation. The major problem with TEA algorithm is Equivalent keys in which each key is equivalent to three others reducing the effective key size to a minimum of 126 bits. Further it is also exposed to related key attack involving 223 chosen plain texts under a related-key pair, with complexity of 232 [27].

f) CASTS5

CAST is symmetric key algorithm based on the backbone concept of Feistel Structure [28]. The CAST is a block cipher that uses a 64 bit plain text with 12 or 16 rounds and a variable Key Length of 40 to128-bit. It also contains 4 S- boxes and same algorithm is used in reversed for decryption in cryptography, CAST-128 (CAST 5) is a block cipher used for different applications. CAST makes use of variable key size operation to increase its security strength, the security of CAST is great and it disobedient against linear and differential attacks [29].

g) AES(Rigndael)

AES can be well adapted to a wide range of modern processors. Generally speaking, AES is the name of the standard, and Rijndael is the name of algorithm anyhow, in practice the algorithm is also referred to as "AES". Security of Rijndael depends on its variable nature key size allowing up to a key size of 256-bit, to provide resistance against certain future attacks. It was observed that a mathematical property of the cipher might be vulnerable into an attack. Furthermore, the inverse cipher implementation is inappropriate on a smart card than the cipher itself [30].

As shown in table2, after analyzing the most popular algorithms for encryption AES was found the most secure, faster and better among the entire existing algorithm with no serious weaknesses, there are some flaws in these algorithms. For example; keys are weak, insecure transmission of secret key, speed, flexibility, authentication and reliability. However, it can be decrypted. Hence, the new method have been presented in this paper which is supported by java language also cannot decrypted since we use SHA algorithm for encryption.

TABLE 2. Comparison of Encryption Algorithms

Algorithm name	**Algorithm structure**	**Plain text length**	**Speed**	**Security**	**Attack**	**Flexibility**	**No. of rounds**	**No. S boxes**	**Key size**
DES	Festial Structure	64 bits	Low	Proven land equate	Brute force	No	16	8	56
TDES	Festial Structure	64 bits	Moderate	Insecure	Man-in-the-middle	Yes	48	168	168
CAST	Festial Structure	64 bits	Moderate	Secure for both linear & differential attacks	One related key	Yes	16	4	40, 128
Blowfish	Festial Structure	64 bits	High	Secure	Differential attacks	Yes	16	4	128,148
IDEA	Substitution-permutation structure	64 bits	Low	Secure	Key-schedule attack, Related-key differential attack	No	8	N/A	128
TEA	Festial Structure	64 bits	Low	Secure	Related key attack	No	64	N/A	128
AES (Rijindael)	Festial Structure	128 bits	Moderate	Secure	Side channel attack, Square attack, Reversed key schedule attack	Yes	10, 12, 14	1	128, 192, 256
SHA	MD5 Structure	512 bits	High	The most Secure	Collision attack, Birthday attack, Brute force attack, Side channel attack	Yes	80	64	160

J. *Proposed Method*

a) Channel Manager

In our method Channel Manager which is middle-ware software to integrate Internet Banking, and Mobile Banking to core banking solution has been selected. Channel Manager provides an API in form of web services to handle transactions or queries expected from Internet Banking, and Mobile Banking.

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.

In Channel manager there is two security layers:

- Authentication
- Authorization

b) *Authentication*

As Authentication of each request we chose following attributes:

- User name
- Vendor name
- Password
- Secret key

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.

As shown in fig.1, the Authentication server is an application which manages the OTP (One Time Password) and E-Sign of the transactions of the other application (e.g. Internet Banking,).

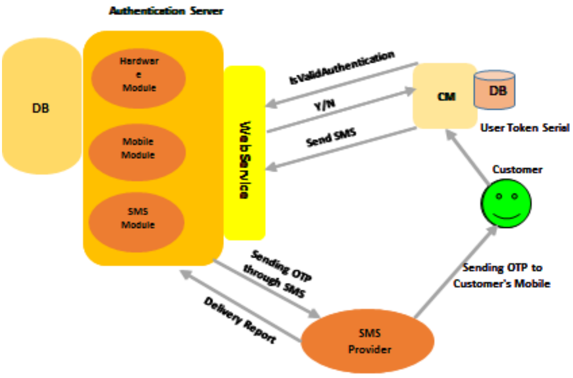

Fig. 1. Authentication Server Architecture

c) *Authorization*

For Authorization of request the following attributes have been selected.

- User name
- Vender name
- Action name
- Password
- Check sum
- Secret Key

Channel Manger validates the check sum and timestamp for the authorization. Check sum is encrypted with 'SHA-256' (Message Digest) with shared secret key. If check sum validates successfully, channel manager will validate the time stamp of the service, Requested service should be within the specified time (Parameterized Value).

d. Message format

For Network security Layer, Channel Manager Authorize the Message format with Check sum, which is encrypted with 'SHA-256' format.
Checksum Format is including six different parts.

- Secret Key
- Vendor
- User name
- Action name
- Password
- Input Parameters/Attributer

Each parameter are speared by # and concatenated one by one sequentially, after successful authorization process the business logic and return the response with Common Response Parameters, which includes error code, error message, and status of the service.

II. 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.
In this paper, we tried to gather all different kinds of online banking systems. However, we focus on mobile banking, the benefits of mobile banking, its architecture, all vulnerabilities which found till now, and different protocols of mobile banking. Moreover, different algorithms of encryption which used in mobile banking have been compared. At last we proposed our own method which is more secure for mobile banking system. Our method has two security layers which are Authentication and Authorization. In addition, for preparing the security of the Network Layer, our method will authorize the Message format, which is encrypted with 'SHA-256' format. Our findings ring a bell to the research community.

REFERENCES

[1] 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)

[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] 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)

[6] Elkhodr, M., Shahrestani, S., & Kourouche, K.," A pro-posal to improve the security of mobile banking applications", In ICT and Knowledge Engineering (ICT & Knowledge Engineer-ing), 2012 10th International Conference on (pp. 260-265). IEEE, (2012)

[7] He, W., "A Review of Social Media Security Risks and Mitigation Techniques", Journal of Systems and Information Technology, 14(2), 171-180, (2012)

[8] He, W. , "A Survey of Security Risks of Mobile Social Media through Blog Mining and an Extensive Literature Search", Information Management and Computer Security, 21(5), pp.381–400.

[9] Paul Judge and Mostafa Ammar, "Security Issues and Solutions in Multicast Content Distribution: A Survey ", IEEE Network,(2003)

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

[11] Rajpreet Kaur Jassal1, Ravinder Kumar Sehgal," Study of Online Banking Security Mechanism in India: Take ICICI Bank as an Example ", IOSR journal of computer engineering (IOSR-JCE), p-ISSN: 2278-8727 Volum13, Issue1 ,PP114-121,(2013),

[12] Jeong, B. K., & Yoon, T. E. , "An Empirical Investigation on Consumer Acceptance of Mobile Banking Services", Business and Management Research, 2(1), 31-40 , (2013)

[13] "Alternative Graphical Authentication for Online Banking Environments", Proceedings of the Eighth International Symposium on Human Aspects of Information Security & Assurance (2014)

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

[15] Vorugunti Chandra Sekhar, "A Secure Account-Based Mobile Payment Protocol with Public Key Cryptography", Mrudula Sarvabhatla, ACEEE Int. J. on Network Security, Vol. 03, No. 01, (2012)

[16] Jaak Tepandi, "Security Analysis of Mobile ID", Ordered by Department of State Information Systems, (2008)

[17] Yacine Challal, Hamida Seba, "Group Key Management Protocols: A Novel Taxonomy", International journal of information technology volume 2 number 2 ISSN 1305-239X ,(2005)

[18] Ibrahim M. Al-Jabri, M. Sadiq Sohail," Mobile banking adoption: Application of diffusion of innovation theory ", Journal of Electronic Commerce Research, VOL 13, NO 4,(2012)

[19] 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)

[20] M.Ebrahimi, S. Khan, Shujjat kahn, UMer Bin Khalid,"Symmetric Algorithm Survey: A Comparative Analysis", International Journal of Computer Applications (0975 – 8887) Volume 61– No.20,(2013)

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

[22] 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)

[23] Limor Elbaz & Hagai Bar-El, “Strength Assessment of Encryption Algorithms, (2000)

[24] Bruce Schneier, "The Blowfish encryption algorithm9", Dr. Dobb's Journal of Software Tools, 19(4), p. 38, 40, 98, 99, (1994)

[25] Jeong, B. K., & Yoon, T. E., "An Empirical Investigation on Consumer Acceptance of Mobile Banking Services",Business and Management Research, 2(1), 31-40, (2013)

[26] X. Lai and J. Massey. A proposal for a new block encryption standard. In Proceedings of the EUROCRYPT 90 Conference, pp. 3 89-404, (1990)

[27] Wheeler, D.J., & Needham, R.J., "TEA, a tiny encryption algorithm", In Fast Software Encryption– Proceedings of the 2nd International Workshop, 1008. (1994).

[28] Kelsey, John; Schneier, Bruce; Wagner, David "Related-key cryptanalysis of 3-WAY, Biham-DES, CAST, DES-X NewDES, RC2, and TEA", Lecture Notes in Computer Science 1334: 233–246. Doi: 10.1007/BFb0028479, (1997)

[29] Anjali Patil, Rajeshwari Goudar, "A Comparative Survey of Symmetric Encryption Techniques for Wireless Devices", International journal of scientific & technology research volume 2, ISSUE 8, (2013)

[30] James Nechvatal, Elaine Barker, Lawrence Bassham, William Burr, Morris Dworkin, James Foti, and Edward Roback, "Report on the Development of the Advanced Encryption Standard (AES)", Volume 106 Number 3 , (2001)