RESEARCHERID
THOMSON REUTERS

[Devi, 6(4): April 2019] ISSN 2348 – 8034
DOI- 10.5281/zenodo.2652558 Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

SECURITY FOR MOBILE COMMUNICATION AND M-COMMERCE USING SIGNCRYPTION – A DETAILED REVIEW

A. Renuga Devi[*1] & Dr.K.Krishnaveni[2]

[*1] Research Scholar, Madurai Kamaraj university – Madurai

[2]Associate Professor and Head, Department of Computer Science, Sri S. Ramasamy Naidu Memorial College – Sattur

ABSTRACT

Mobile communication and Mobile Commerce is most popular now-a-days because of the service offered during the mobility. However, despite of its new advancements, mobile communication has been facing many security problems. This paper reviewed various security mechanisms based on the cryptographic techniques. This paper mainly focuses the Signcryption based cryptographic technique, because Signcryption has been shown to be useful in various applications, such as electronic commerce, mobile communications and smartcards. Finally this paper provides the proposed research methodology design to be implemented in future.

Keywords: *Mobile Communication, Mobile Security, Signcryption, Mobile Commerce*.

I. INTRODUCTION

- Wireless and mobile communication systems are very famous among the customers as well the operators and service providers [2]. Unlike wired networks, the wireless networks provide anywhere and anytime access to users. The Global System for Mobile Communications (GSM) occupies almost 70% of the wireless market and is used by millions of subscribers in the world [2]. In wireless services, secure and secret communication is desirable. It is the interest of both the customers and the service providers. These parties would never want their resources and services to be used by unauthorized users. Mobile commerce or M-Commerce is a commercial transaction carried through mobile phones. It can be a process, systems or procedure that includes checking account balance, depositing a change, buying and selling any product, all these things doing on mobiles.
- The services like online banking, e-payment, and m-commerce are already using the Internet [1]. The financial institutions like banks and other organizations would like their customers to use online services through mobile devices keeping the wireless transaction as secure as possible from the security threats. Smart cards (e.g. SIM card) have been proposed for applications like secure access to services in GSM, to authenticate users and secure payment using Visa cards and MasterCard [10]. Wireless transactions are facing several security challenges due to some lack of security. Data sent through air face almost the same security threats as the data over wired networks and even more. However, the limitations in wireless bandwidth, battery, computational power and memory of wireless devices impose further restrictions to the security mechanisms implementation [9]. The use of mobile communication in e/m-commerce has increased the importance of security. An efficient wireless communication infrastructure is required in every organization for secure voice/data communication and users authentication. Among the main objectives of an efficient infrastructure is to reduce the signaling overhead and to reduce the number of HLR/AuC (Home-Location Register/Authentication Center) updates as the Mobile Station (MS) changes its location frequently [7].
- In many cryptographic algorithms confidentiality, integrity, non-repudiation and authentication are the most important requirements. A traditional approach to maintain these requirements is to sign-then-encryption. Signcryption is a cryptographic primitive proposed by Zheng [5] to fulfill both the functions of digital signature and public key encryption simultaneously at a cost significantly lower than that required by the traditional signature-then-encryption approach.

- The rest of the paper is formatted as: section 1 deals with general introduction related to the particular domain, section 2 discussed the related works of security in mobile communication and M-Commerce. Section 3 discusses the Security Risks in Mobile Commerce Transaction. Section 4 deals with the Security Requirements for Signcryption Scheme with the research gap and proposed research methodology design. The conclusion is defined as the next section 5.

II. LITERATURE REVIEW

- In 2015, Sumit Chakra borty[12]constructs an efficient and secure mechanism for mobile commerce applying the concept of financial cryptography and secure multi-party computation. The author said that the mechanism (MCM) is defined by various types of elements: a group of agents or players, actions, a finite set of inputs of each agent, a finite set of outcomes as defined by output function, a set of objective functions and constraints, payment function, a strategy profile, dominant strategy and revelation principle.
- In 2015, Krishna Prakash and Balachandra [8] surveyed various papers to discuss the mobile communication trends and technologies. They discussed that the information residing in the mobiles, integrity of the information and security of the information during its journey over the air security of the information within the wireless network has to be given much importance.
- In 2014, Hassan M. Elkamchouchi et al., [6] proposed a new communication protocol used in GSM using tripartite signcryption scheme without using bilinear pairings that proposed in [13]. The authors said that the proposed scheme is used to reduce the signaling overhead in the authentication step in mobile communication systems and combats the denial of service attack.
- In 2013, Eman F. Abu Elkhair et al., [3] examines the benefits of using signcryption rather than signature-then-encryption in the SET protocol. Using identity-based signcryption in the SET protocol reduces the number of encryption and decryption operations. Moreover, signcryption is less time consuming than signature-then-encryption.
- In 2013, Fagen Li and Tsuyoshi Takagi [4] proposed an attack to show that Zhang's scheme does not have the IND-CCA2 property (not even chosen plaintext attacks (IND-CPA)). We present a fully secure IBSC scheme in the standard model. We prove that our scheme has the IND-CCA2 property under the decisional bilinear Diffie–Hellman assumption and has the EUF-CMA property under the computational Diffie–Hellman assumption.

III. SECURITY RISK IN MOBILE COMMERCE TRANSACTION

In Generally, The Lack Of Security Provision Created A Barrier Against The Adoption Of M-Commerce. The Handheld Devices Have Equivalent Computing Power To The Desktop. While Driving More And More Functionality Into Mobile Device, The Security Risks Such As Theft, Loss Of Data Is Also Driving [11]. Some Other Risks Are Like Identity Theft And Credit Card Frauds. If Mobile Commerce Has More Significant Importance Than A Traditional E-Commerce As It Is Ease To Eavesdrop Into Other's Message With A Minimum Difficulty In Mobile Environment.

ISSN 2348 – 8034
Impact Factor- 5.070

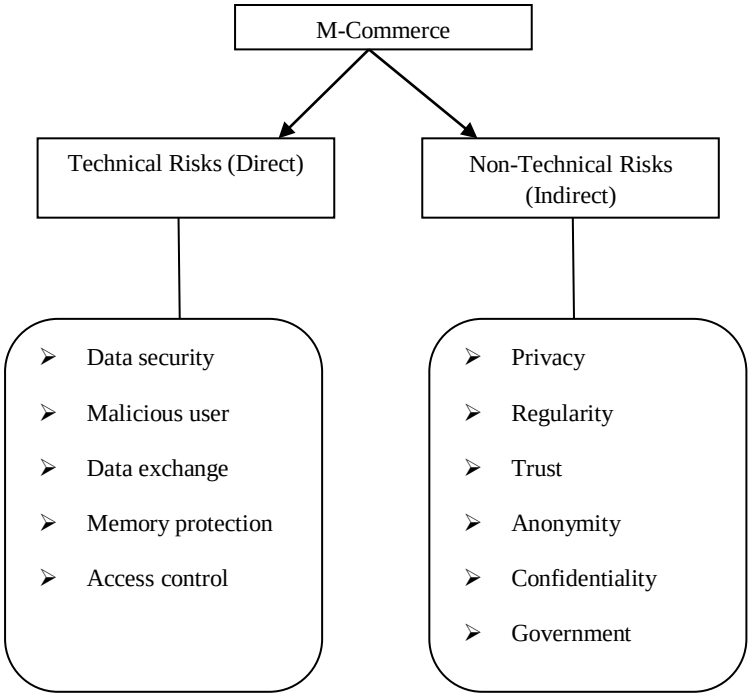

Figure 1. Type DEs Of M-Commerce

In M-Commerce Security Risks Is Categorized As Two Types, Such As

i) Technical Or Direct Risk
ii) Non-Technical Or Indirect Risk

The Identification Integrity Refers To The Signature Element Found In Message To Infer From Where The Message Is Originating The Message Integrity Point To Detail To Establish That, No Third Party Opened, Modify Or Alter The Content [13]. The Technical Risks Have More Concern Of Sender And Service. The Risk Of Theft Or Misuses Of Personal Information And Repudiation Of Transaction Are Major Issues For Both. Data In M-Commerce Is Secured By Using Encryption Technology Which Is Vulnerable To Attack. Therefore The Word Complete Security Is Obsolete. The Technical Security Risks Can Also Be Seen Into Impact Data In A Mobile Commerce Transaction Platform To Facilitate Data Communication And Necessary Protocol And Software For This Communication.

IV. SECURITY REQUIREMENTS FOR SIGNCRYPTION SCHEME

Here, the Security Requirements [14] For the Signcryption Scheme Are Provided,

Confidentiality

It Means That Only The Intended Recipient Of A Signcrypted Message Should Be Able To Read Its Contents. That Is, Upon Seeing A Signcrypted Message, An Attacker Should Learn Nothing About The Original Message, Other Than Perhaps Its Length.

Unforgeability

It Refers To The Inability Of Any Entity To Produce A Valid Message-Signature Pair Except The Designated Signer.

Public Verifiability
It Means That Any Third Party Or Judge Can Verify That The Signcrypted Text Is Valid Or Not, Without Any Need For The Private Key Of The Sender Or The Recipient.

Non-Repudiation
The Sender Of A Message Cannot Later Deny Having Sent The Message. That Is, The Recipient Of A Message Can Prove To A Third Party That The Sender Indeed Sent The Message.

Integrity
This Means That The Recipient Should Be Able To Verify That The Received Message Is The Original One That Was Sent By The Sender And It Has Not Been Tampered With During Transmission.

Authentication
It Involves Confirming The Identity Of A System User. Authentication Often Involves Verifying The Validity Of At Least One Form Of Identification. Also, It Allows the Legitimate Recipient Alone to Be Convinced That theCipher text And the Signed Message It Contains Were Crafted by the Same Entity.

Forward Secrecy
It Refers To The Inability Of An Attacker To Read Signcrypted Messages, Even With Access To The Sender's Private Key. That Is, The Confidentiality Of Signcrypted Messages Is Protected, Even If The Sender's Private Key Is Compromised.

4.1 Research gap
The Reviewed Existing Methods In This Paper Have Some Certain Restrictions And Problems Because It Has Neglected Many Of The Points Some Of Them Are:
1. The Existing Security Model Developed Do Not Enhanced The Security Of Mobile Communication; Because The Existing Cryptographic Techniques In Mobile Networks Are Easily Hack Able.
2. The Majority Of The Existing Techniques Are Limited To Development Of The Encryption Algorithm And Code To Encrypt The Transactional Data.

4.2 Proposed Research Methodology
1. Identified Different Security Risk Management Techniques In M-Commerce
2. Examined The Challenges And Barriers In Penetration Of M-Commerce
3. Proposed A Signcryption Based Standard Cryptographic Mechanism To Secure The Mobile Communication And M-Commerce.
4. Designed A Control Mechanism To Increase The Security Level During Transactions In M-Commerce.

REFERENCES

1. *D. Boneh and M. Franklin, Identity-Based Encryption From The Weil Pairing, In: Advances In Cryptology-CRYPTO 2001, In: Vol. LNCS, 2139, Springer-Verlag, 2001, pp. 213–229.*
2. *R. Borgohain et al., " TSET: Token Based Secure Electronic Transaction"; International Journal of Computer Applications, May 2012, ISBN: 978-93-80866-55-8, DOI: 10.5120/5056-7374.*
3. *Eman F. Abu Elkhair, "An Improvement to the SET Protocol Based On Signcryption", International Journal on Cryptography and Information Security (IJCIS), Vol.3, No. 2, June 2013, pp 1-13.*
4. *Fagen Li and Tsuyoshi Takagi, "Secure identity-based signcryption in the standard model", Mathematical and Computer Modelling, Volume 57, 2013, pp. 2685–2694.*
5. *H.Gupta and V. K. Sharma," Role of Multiple Encryption in Secure Electronic Transaction", International Journal of Network Security & Its Applications (IJNSA), Vol.3, No.6, November 2011.*
6. *Hassan M. Elkamchouchi et al., "An Improved Authentication Protocol for Mobile Communication based on Tripartite Signcryption", International Journal of Computer Applications, ISSN 0975 – 8887, Volume 92 – No.14, April 2014, pp. 13-18.*

7. *Z. Jin et al., An Improved Semantically-Secure Identity-Based Signcryption Scheme In The Standard Model, Computers & Electrical Engineering, 36 (3), 2010, pp. 545–552.*
8. *Krishna Prakash and Balachandra, "Security Issues and Challenges in Mobile Computing and M-Commerce", International Journal of Computer Science & Engineering Survey (IJCSES) Vol.6, No.2, April 2015, pp 29-45.*
9. *F. Li et al., Analysis Of An Identity-Based Signcryption Scheme In The Standard Model, IEICE Transactions On Fundamentals Of Electronics, Communications And Computer Sciences E94-A (1), 2011, pp. 268–269.*
10. *B. Libert and J.J. Quisquater, "A New Identity Based Signcryption Schemes", In: 2003 IEEE Information Theory Workshop, Paris, France, 2003, pp. 155–158.*
11. *Mahmoud Elkhodr Et Al., "A Proposal To Improve The Security Of Mobile Banking Applications", IEEE International Conference On ICT And Knowledge Engineering, 2012.*
12. *Sumit Chakraborty, "Mobile Commerce: Secure Multi-party Computation & Financial Cryptography", Technical Report / MCSMCFC/ V1.0 15082015, 2015, pp. 1-13.*
13. *P.Subhasri and Dr.A.Padmapriya., "Enhancing the Security Of Dicom Content Using Modified Vigenere Cipher", International Journal of Applied Engineering Research, Volume: 10(55), January 2015, pp. 1951-1956.*
14. *B. Zhang, "Cryptanalysis of an Identity Based Signcryption Scheme without Random Oracles", Journal of Computational Information Systems 6 (6), 2010, pp. 1923–1931.*