INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 5)
Available online at: www.ijariit.com

Security for mobile communication and M-commerce using signcryption– A detailed review

A. Renuga Devi
sekaradv@gmail.com
Madurai Kamaraj University College, Madurai, Tamil Nadu

Dr. K. Krishnaveni
kkveni-srnmc@yahoo.co.in
Sri S. Ramasamy Naidu Memorial College, Sattur, Tamil Nadu

Dr. M. Ramakrishnan
ramkrishod@gmail.com
Madurai Kamaraj University College, Madurai, Tamil Nadu

ABSTRACT

Mobile communication and Mobile Commerce is most famous nowadays as a result of the administration offered amid the portability. In any case, notwithstanding of its new headways, versatile correspondence has been confronting numerous security issues. This paper looked into different security systems dependent on the cryptographic methods. This paper mostly centers the Signcryption based cryptographic strategy, since Signcryption has been appeared to be valuable in different applications, for example, electronic trade, versatile correspondences, and smart cards. At last this paper gives the proposed research philosophy configuration to be executed in the future.

Keywords— *Mobile communication, Mobile security, Signcryption, Mobile commerce*

1.INTRODUCTION

Wireless and Mobile communications frameworks are extremely celebrated among the clients to the administrators and specialist co-ops [2]. In contrast to wired systems, the remote systems give anyplace and whenever access to clients. The Global System for Mobile Communications (GSM) possesses right around 70% of the remote market and is utilized by a huge number of endorsers on the planet [2]. In remote administrations, secure and mystery correspondence is alluring. It is the enthusiasm of both the clients and the specialist organizations. These gatherings could never need their assets and administrations to be utilized by unapproved clients. Versatile trade or M-Commerce is a business exchange brought through cell phones. It very well may be a procedure, frameworks or methodology that incorporates financial records balance, storing a change, purchasing and offering any item, every one of these things doing on mobiles.

The administrations like web-based saving money, e-installment, and m-trade are as of now utilizing the Internet [1]. The money related establishments like banks and different associations might want their clients to utilize online administrations through cell phones keeping the remote exchange as secure as conceivable from the security dangers. Savvy cards (e.g. SIM card) have been proposed for applications like secure access to administrations in GSM, to validate clients and secure installment utilizing Visa cards and MasterCard [10]. Remote exchanges are confronting a few security challenges because of some absence of security. Information sent through air confront nearly indistinguishable security dangers from the information over wired systems and significantly more. Notwithstanding, the confinements in remote transmission capacity, battery, computational power and memory of remote gadgets force encourage limitations to the security systems execution [9]. The utilization of portable correspondence in e/m-trade has expanded the significance of security. An effective remote correspondence foundation is required in each association for secure voice/information correspondence and client's confirmation. Among the fundamental destinations of a productive foundation is to diminish the flagging overhead and to lessen the quantity of HLR/AuC (Home-Location Register/Authentication Center) refreshes as the Mobile Station (MS) changes its area every now and again [7].

In numerous cryptographic calculations privacy, honesty, non-renouncement, and validation are the most vital necessities. A conventional way to deal with keep up these necessities is to sign-then-encryption. Signcryption is a cryptographic crude proposed by Zheng [5] to satisfy both the elements of advanced signature and open key encryption all the while at an expense fundamentally lower than that required by the conventional mark then-encryption approach.

Whatever is left of the paper is designed as: segment 1 manages general acquaintance related to the specific area, segment 2 talked about the related works of security in portable correspondence and M-Commerce. Area 3 talks about the Security Risks in Mobile Commerce Transaction. Area 4 manages the Security Requirements for Signcryption Scheme with the exploration hole and proposed to investigate the approach plan. The end is characterized as the following segment 5.

2. LITERATURE REVIEW

In 2015, Sumit Chakraborty [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 mobile communication trends and technologies. They discussed that the information residing in the mobiles, the 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 the 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.

3. SECURITY RISK IN MOBILE COMMERCE TRANSACTION

In, by and large, the absence of security arrangement made a hindrance against the selection of M-Commerce. The handheld gadgets have proportional registering capacity to the work area. While driving increasingly usefulness into a cell phone, the security dangers, for example, burglary, loss of information is additionally driving [11]. Some different dangers resemble wholesale fraud and Master card cheats. In the event that portable business has more huge significance than a customary E-Commerce as it is slip to listen stealthily into other's message with a base trouble in versatile condition.

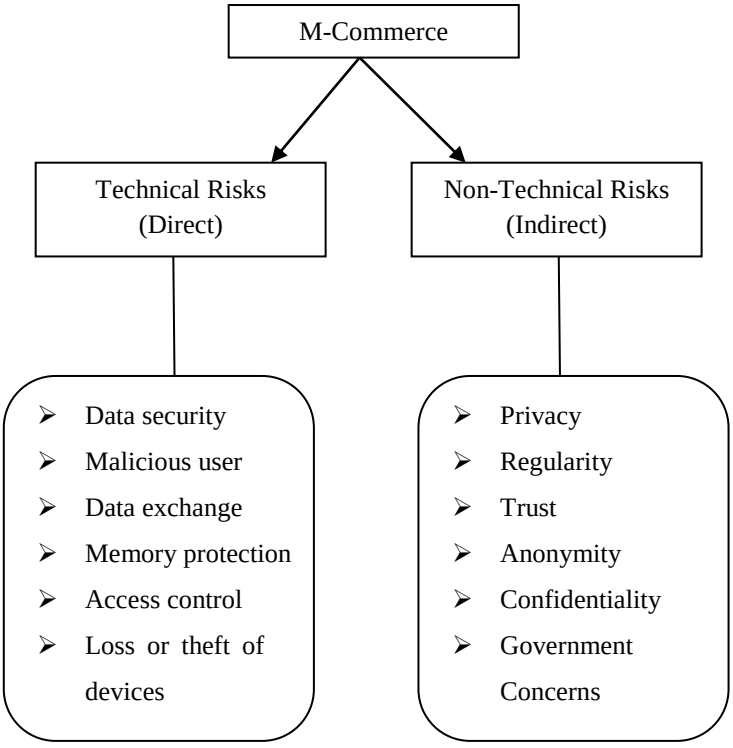

Fig. 1: Types of M-Commerce

In M-Commerce security risks are categorized into two types, such as:

i) Technical or Direct Risk
ii) Non Technical or Indirect Risk

The identification proof uprightness alludes to the mark component found in a message to construe from where the message is starting the message respectability point to detail to build up that, no outsider opened, adjust or change the substance [13]. The specialized dangers have more worry about sender and administration. The danger of robbery or abuses of individual data and denial of exchange are significant issues for both. Information in M-Commerce is anchored by utilizing encryption innovation which is powerless against assault. Hence the word finish security is out of date. The specialized security dangers can likewise be

seen into effect information in a portable trade exchange stage to encourage information correspondence and important convention and programming for this correspondence.

4. SECURITY REQUIREMENTS FOR SIGNCRYPTION SCHEME

Here, the security requirements [14] for the signcryption scheme are provided:

4.1 Confidentiality

It implies that just the expected beneficiary of a signcrypted message ought to have the capacity to peruse its substance. That is, after observing a signcrypted message, an aggressor ought to get the hang of nothing about the first message, other than maybe its length.

4.2 Unforgeability

It mentions that the inability of any entity to produce the valid message-signature pair except the designated signer.

4.3 Public Verifiability

It means that any of the third party or judge can authenticate that the signcrypted text is valid or not, without any need for the private key of the sender or the recipient.

4.4 Non-Repudiation

The sender cannot deny the message having sent the message. That is, the recipient of a message can provide to the third party that the sender indeed sent the message.

4.5 Integrity

This means that the receiver should be able to confirm that the received information's is the original message that was sent by the sender and it has not been tampered with during transmission.

4.6 Authentication

It includes affirming the personality of a framework client. Verification frequently includes confirming the legitimacy of somewhere around one type of recognizable proof. Additionally, it permits the real beneficiary alone to be persuaded that the ciphertext and the marked message it contains were made by a similar substance.

4.7 Forward Secrecy

It alludes to the powerlessness of an assailant to peruse signcrypted messages, even with access to the sender's private key. That is, the secrecy of signcrypted messages is ensured, regardless of whether the sender's private key is endangered.

5. RESEARCH GAP

The check on existing strategies in this paper have some specific confinements and issues since it has ignored huge numbers of the focuses some of them are:

- The existing security show created don't improve the security of portable correspondence; in light of the fact that the current cryptographic methods in versatile systems are effortlessly hacked capable.
- Most of the current strategies are constrained to the improvement of the encryption calculation and code to encode the value-based information.

6. PROPOSED RESEARCH METHODOLOGY

- Acknowledged different security risk management methods in M-Commerce.
- Observed the challenges and barriers in penetration of M-Commerce.
- The current Signcryption based standard Cryptographic mechanism to secure the mobile communication and M-Commerce.
- Designed the control mechanism for increasing the security level during transactions in M-Commerce.

7. CONCLUSION

In this survey, the paper introduces an assessment to anchor the versatile correspondence and M-Commerce by utilizing cryptographic strategies. Many existing versatile correspondence security techniques are investigated in this paper. The exploration hole is finding and the proposed arrangement is outlined in this paper. In future, this work is actualized a novel technique to accomplish the better security contemplations in portable correspondence and M-Commerce with the assistance of cryptographic systems.

8. 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.

