SMS Security: Highlighting Its Vulnerabilities & Techniques Towards Developing a Solution

Ikechukwu Ibekwe, Salem Aljareh
School of Engineering
University of Portsmouth
E-mail: ikechukwu.ibekwe@port.ac.uk

Abstract— **SMS has become an indispensible communication tool used by banking, government and other agencies. However, the SMS is not a secure service to be used to transport sensitive data, as its current security mechanism cannot guarantee protection from modification, eavesdropping and man-in-the-middle attacks.**
This paper examines existing security mechanisms; vulnerabilities and contributions put forward by researchers in enhancing SMS security features. Their proposals are criticized with a view to finding gaps and developing a comprehensive solution.

***Index Terms*—GSM, SMS Security, PKI, UMTS.**

I. INTRODUCTION

THE past two decades have seen an exponential increase in mobile communication usage. One of the reasons for this has been because of the increased functionality and services offered. Some of these include international roaming capability, cost effectiveness and new services (call waiting, call forwarding) and the Short Message Service (SMS). Of all services provided by mobile telephony, the SMS has become extremely popular.

The SMS is a service that provides text-messaging capability over a mobile network. The service is unique as it has a maximum message length of 160 characters, requires low bandwidth & provides assurance in message delivery within a specified period. This popularity of the SMS has made entities such as commercial, government take leverage of this platform to communicate with individuals and businesses. For example it is not uncommon for bank transaction or voting to be made via SMS, prompting acronyms such as m-banking and e-voting. In as much as SMS provides such a wide reach and convenience, is its platform secure? Is there assurance on the origin of the message or mechanism to protect data from eavesdroppers?

This paper aims to provide an overview of SMS security and provide a framework for which a comprehensive solution may be adopted. Section II describes the GSM network architecture that the SMS operates on. Message flow within the network is also described. Section III describes current security mechanisms service provides adopted with respect to protecting the SMS from modification, eavesdropping and unauthorized access to content. Vulnerabilities associated with the mechanisms are also discussed. Section III describes research work done to enhance SMS security and finally Section IV looks at the different elements that will be studied in view of enhancing SMS security. It should however be noted that this is in its design phase and results will be published subsequently.

II. SMS NETWORK ARCHITECTURE

This section discusses SMS traversing a GSM platform (figure 1.0). For delivery, messages must undergo three processes[1]: submission, routing and transportation medium.

Initiation of a text message is achieved through a mobile devices or *External Short Messaging Entities (ESMEs).* For ESMSs to deliver SMS, they must be connected to the mobile platforms through the SMS *Interworking Mobile Switching Centre (SMS-IMSC)[1]* . Operators offering SMS service usually have one or more servers known as the *Short Messaging Service Center (SMSC).* These servers are designed to operate in a store and forward fashion[2]. This is to enforce correct SMS message format and provide storage facility if the recipient is not available at time of delivery. Once the message is in SMS format, it is ready for routing to its destination.

Before routing can occur, the SMSC queries the *Home Location Register (HLR),* a permanent repository that stores information about subscribers, about the routing information of the recipient. Other information the HLR stores are the visitor location register number, service restrictions (e.g. roaming limitations), subscription data[3]. Depending on the result of the query, the SMSC either stores the message for later delivery or receives information about the *Mobile Switching Center (MSC)* where the intending recipient is being served. The MSC handles traffic routing, authentication, location updates and handover procedure on a mobile network and as such can route messages to its destination[3]. With the aid of the *Visitor Location Register (VLR),* a database for temporary storage of information about the subscribers being serviced by an MSC, the MSC obtains device information if its HLR is not local. With knowledge of device location, the MSC forwards the message to the *Base Station (BS)* in communication with the device for transmission over the air medium to the device.

The BS on receiving the message from the MSC needs to forward the content to the recipient (mobile equipment) via

ISBN: 978-1-902560-26-7

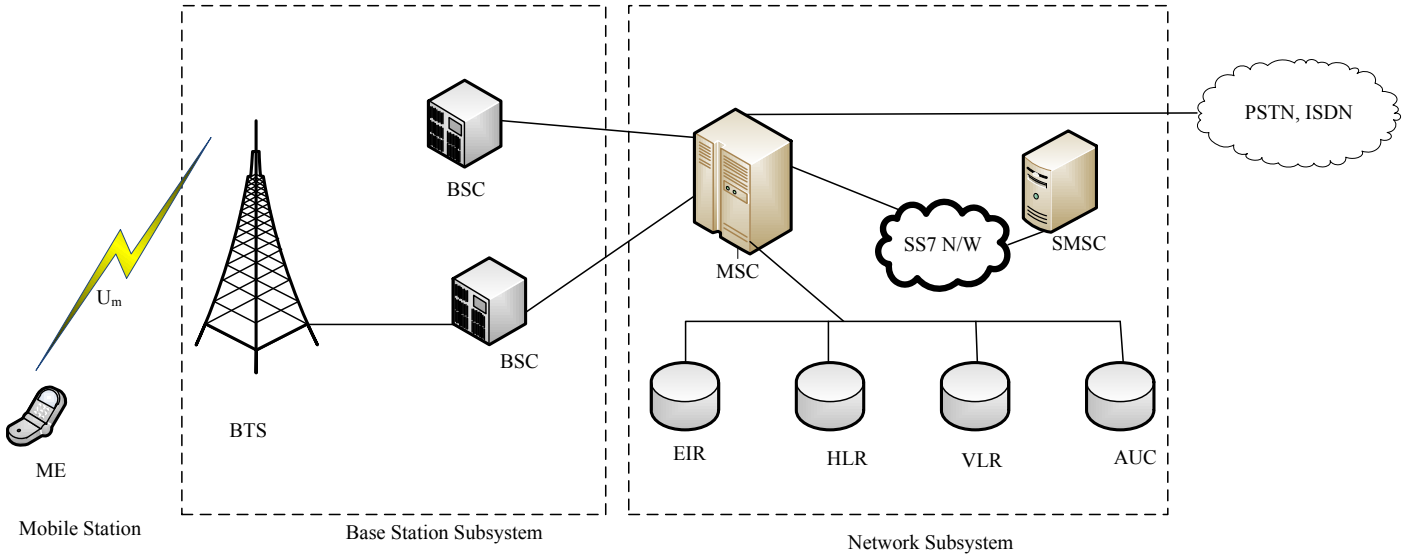

Figure 1.0: GSM Network Architecture [2]

the air. The medium comprises of the *Control Channels (CCH)* and *traffic Channels (TCH)[3]*. The base station uses the CCH to deliver SMS to mobile devices as mobile devices are designed to listen to this channel for SMS traffic. CCH is subdivided into the *Random Access Channel (RACH)* and *Paging Channel (PCH)*. The BS uses the PCH to send a message with the *Temporary Mobile Subscriber ID (TMSI)* alerting the ME of an intending SMS. When the ME hears its TMSI, it contacts the BS via the RACH and confirms availability to receive SMS. The BS then instructs the ME to listen to a particular *Standalone Dedicated Control Channel (SDCCH)*. With the SDCCH, the BS is able to perform encryption, authentication procedures and deliver the SMS message[3].

A. SMS SECURITY MECHANISMS

The resilience of SMS messages from alteration, replay and SMS spoofing attacks is subject to the platform the SMS transverses. As described the previous section, SMS can be transmitted via mobile networks (GSM, GPRS, UMTS and CDMA) and ESMEs. In this section a case study of security mechanisms deplored by two different network platforms will be examined.

CASE I: Global System for Mobile Communication (GSM)

GSM incorporates security mechanisms to ensure confidentiality and integrity of services. These mechanisms are embedded within the ME and the operator network. In order to ensure secrecy, GSM operators deplore the A5 algorithm. The ME initiates encryption at the request of the network; it uses an algorithm A8 to generate a ciphering key K_c with RAND gotten from the HLR. The key K_c is then used with the A5 algorithm to encrypt data[4]. Figure 2.0 depicts procedure.

The legitimacy of the user is determined by the network issuing a challenge to the intending user (ME). The HLR is assigned to send a 128bit random number (RAND), generated by AUC, to the ME. The ME uses an authentication algorithm (A3) and key K_i to compute a *Signed Response (SRES)*. The network also computes this challenge and compares it with that of the ME. Authentication is deemed successful if SRES from the Network corresponds to that sent to the Network [4].

VULNERABILITY ANALYSIS

In ensuring non-disclosure of data GSM utilizes the A5 algorithm; however it has been demonstrated to be weak and liable to cryptanalysis as demonstrated in [5] who found the secret key in minutes. Although higher variants of this algorithm have being developed it is still not resistant to attacks.

ESMEs communicate with the SMSC is done through *Short Message Peer to Peer protocol (SMPP)[3]*. The SMPP protocol does not encrypt its content making SMS originating via ESMEs susceptible to man in the middle attack. Besides the weak encryption the GSM network utilizes, the network does not provide end-to-end security. This exposes plaintext messages at certain points within the infrastructure thereby making those areas vulnerable to man-in-the-middle attack.

Replay attacks are possible with the authentication mechanism the GSM operates. GSM infrastructure lacks mutual authentication [6]. As a result there is a possibility where an attacker deplores an authentication request or response to be replayed. Impersonation and false transaction could be executed thereby compromising existing authentication mechanisms. Moreover the GSM does not provide non-repudiation mechanisms. This greatly compromises the SMS in its ability to provide information assurance.

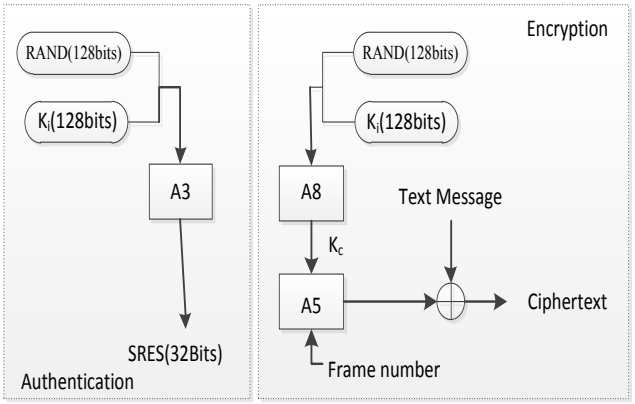

Figure 2.0: Security mechanism in mobile equipment [4]

CASE II: Universal Mobile Telecommunication System (UMTS)

UMTS security mechanism was designed to eliminate the security flaws of its predecessor, the GSM. The security mechanisms can be classified into five distinct features; network domain security, network access security, application domain security, user domain security and visibility and configurability of security [7, 8]. Of the above mentioned security features, the network access security is a primary component as it is tasked with providing confidentiality, integrity protection of signaling data and authentication [7].

Unlike its predecessor, the UMTS incorporates mutual authentication between *Serving Network (SE) and ME*. In order to achieve mutual authentication, authentication vectors consisting of *Encryption Key* (CK), *user challenge* (RAND), *expected user response* (XRES), *the integrity key* (IK) and the *authentication token for network authentication* (AUTN) are used [9].

Authentication is initiated in the VLR and mutual authentication is successful when VLRs XRES matches the received RES. Figure 3.0 depicts the process involved in mutual authentication. Exchange of CK and IK to their entities are then permissible to perform integrity protection. When authentication is complete, *Message Authentication Code* (MAC) function is applied on the link with CK and IK derived from the authentication process to preserve integrity.

VULNERABILITY ANALYSIS

UMTS design allows for interoperability with the GSM network. Interoperability between UMTS and GSM was necessary for easy transition to UMTS networks[8]. Moreover GSM had a wider coverage, it was necessary for UMTS subscribers to roam in areas with GSM only coverage and vice-versa. But lack of mutual authentication in GSM means a man-in-the-middle attack could still occur as shown in [10].

The failure of a mobile station to authenticate the serving network means that a variant of false base station attack could still occur. This was demonstrated in [11] where a redirection of traffic to a different network with weak encryption algorithm was possible.

In all, vulnerabilities in underlying networks could enable attacks on SMS possible. Contributions on eliminating these vulnerabilities are examined in the following section.

III. RELATED WORK

Several proposals have been put forward towards securing SMS services; contributions have being centered on either modifying network infrastructure or providing end-to-end security at the application layer. Hossain *et al.* in [12] suggested modifying the GSM infrastructure at the transport layer to enhance confidentiality. His proposal could strengthen confidentiality however the encryption process proposed is subject to operators' encryption scheme and therefore requires their consent for implementation. Most researchers don't concentrate effort at the transport layer due to the limitation mentioned.

The second category of research is concentrated on is the application layer. It appeals to researchers and developers because implementation can be achieved without the service providers' consent. However, providing security platforms at this layer is subject to the capability and capacity of the mobile equipment[13]. Therefore in developing security

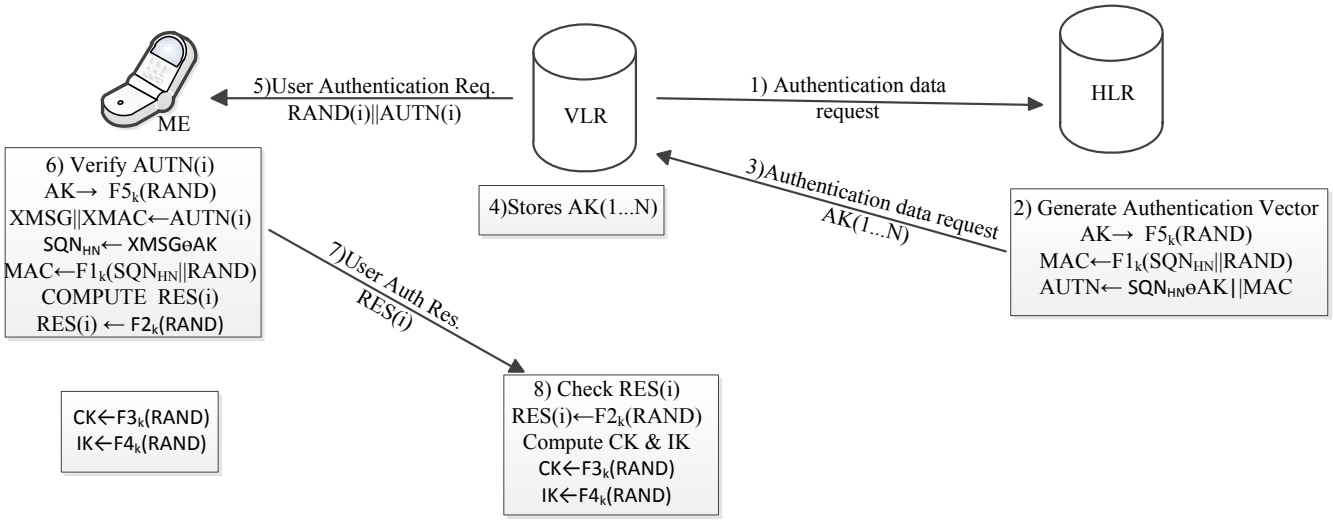

Figure 3.0: Process of authentication in a UMTS Network

mechanisms, encryption schemes, consideration of key management, energy consumption and speed must be considered.

Due to the limitation of mobile equipment, symmetric encryption techniques would be ideal as its encryption process is fast and uses shorter keys when compared to asymmetric encryption. However, key distribution is a problem when deploying symmetric encryption and the number of keys needed for communication is approximate to the square of number of senders [14]. Another drawback is its limitation to ensure confidentiality of data.

Ratshinanga introduced a hybrid scheme by proposing the use of asymmetric key encryption for key distribution process [15]. This ensured key protection and integrity of SMS service. However, the computational process is too high due to incorporation of asymmetric encryption scheme in encrypting the SMS distribution and key agreement. Researches tend to combine asymmetric cryptography and symmetric cryptography to achieve fast processing speed and safe key agreement. The schemes described above can be does not incorporate authentication mechanisms.

The *Public Key Infrastructure* (PKI) provides a framework of providing assurance that the parties communicating are authentic. It involves obtaining certificate and extracting public key before encryption can be applied. The PKI scheme is high computationally intensive due to large key generations; it cannot be directly imbedded on a mobile device [16]. Many researchers in adopting this framework attempt to segment the high computational part to a dedicated server or third party. Others adopt the symmetric key cryptography to reduce the asymmetric cryptography overhead. Table I shows different schemes of PKI framework.

Although the PKI framework can be used to enhance SMS security, it is beneficial to large organizations such as banks or governmental usage. This is due to the large cost of maintaining servers or third party license cost. The PKI framework is also fraught with lots of complexities such as Service provider approval, certificate standardization and will require technical support.

IV. PROPOSAL FOR ENHANCING SMS SECURITY

Providing efficient end-to-end cryptographic solution is the most effective method of enhancing SMS security. This approach provides a single point of decryption (at the receiving node) thus ending numerous cycles of encryption-decryption processes currently experienced at different nodes of the mobile network. This approach will also reduce the number of attack nodes. End-to-End security can be applied at the application layer on the mobile equipment device and is software driven subject to:

a) Processing capabilities of mobile phone.
b) Memory capacity of the mobile phone or SIM card.
c) Processing capabilities of a crypto-processor that is embedded in the ME.

Due to the limitations of mobile phones, a lightweight infrastructure is proposed. The cryptographic technique deployed would be hybrid (both symmetric and asymmetric encryption). Using both modes of encryption takes advantage of their cryptographic strength and enhances the overall security of the SMS service. The infrastructure will incorporate

1) Using Symmetric Encryption for encryption and decryption.
2) Using asymmetric cryptography for key distribution. The Elliptic Curve Cryptographic (ECC) technique will be deployed as it is efficient and uses lesser number of keys as opposed to other schemes.
3) Deploying a pair of private-public keys to each subscriber.

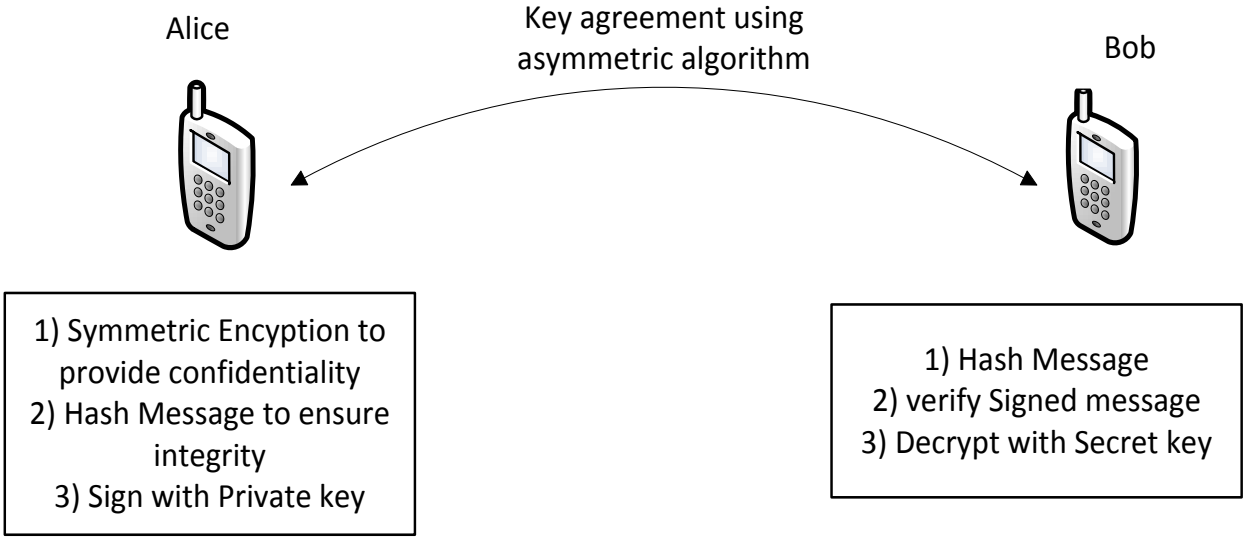

Figure 4.0: Proposed Solution Architecture

Integrity of the message will be achieved by hashing the message before it is sent to the recipient. Figure 4.0 shows the steps taken in achieving this process. On the receiver end, the message is first hashed and verified to ensure the integrity of the message.
The asymmetric encryption in the proposed architecture performs twos tasks: it ensures safe key exchange between the sender and the recipient, it also prevents the sender from denying not sending the message as the private key will be used sign the message.

Validation of the proposed solution will be done in two phases:

- Testing different encryption techniques using a suitable emulator to determine suitable option for mobile systems.
- Installing developed solution on multiple mobile phone devices to determine their performance on different processing capabilities.

V. CONCLUSION

SMS is one communication tool that will be used for a long time due its simplicity and low cost. Current security mechanisms cannot curb modification, replay and man-in-the-middle attacks. End-to End security is seen as a permanent solution in preserving user data. Challenges that need addressing include providing efficient yet lightweight cryptographic mechanisms, reliable key management and distribution system. This paper highlights the challenges with a view to get a framework where a solution can be obtained.

REFERENCES

[1] W. Enck, P. Traynor, P. McDaniel *et al.*, “Exploiting open functionality in SMS-capable cellular networks,” in Proceedings of the 12th ACM conference on Computer and communications security, Alexandria, VA, USA, 2005, pp. 393-404.

[2] G. Peersman, P. Griffiths, H. Spear *et al.*, “A tutorial overview of the short message service within GSM,” *Computing & Control Engineering Journal,* vol. 11, no. 2, pp. 79-89, 2000.

[3] P. Traynor, W. Enck, P. McDaniel *et al.*, “Mitigating attacks on open functionality in SMS-capable cellular networks,” *IEEE/ACM Trans. Netw.,* vol. 17, no. 1, pp. 40-53, 2009.

[4] M. Toorani, and A. A. Beheshti Shirazi, "Solutions to the GSM Security Weaknesses." pp. 576-581.

[5] A. Biryukov, A. Shamir, and D. Wagner, “Real Time Cryptanalysis of A5/1 on a PC,” in Proceedings of the 7th International Workshop on Fast Software Encryption, 2001, pp. 1-18.

[6] A. Fanian, M. Berenjkoub, and T. A. Gulliver, "A new mutual authentication protocol for GSM networks." pp. 798-803.

[7] A. Bais, W. T. Penzhorn, and P. Palensky, "Evaluation of UMTS security architecture and services." pp. 570-575.

[8] L. Min, B. Hai, and F. Zhengjin, "Security architecture and mechanism of third generation mobile communication." pp. 813-816 vol.2.

[9] H. Chung-Ming, and L. Jian-Wei, "Authentication and key agreement protocol for UMTS with low bandwidth consumption." pp. 392-397 vol.1.

[10] U. Meyer, and S. Wetzel, “A man-in-the-middle attack on UMTS,” in Proceedings of the 3rd ACM workshop on Wireless security, Philadelphia, PA, USA, 2004, pp. 90-97.

[11] Z. Muxiang, and F. Yuguang, “Security analysis and enhancements of 3GPP authentication and key agreement protocol,” *Wireless Communications, IEEE Transactions on,* vol. 4, no. 2, pp. 734-742, 2005.

[12] A. Hossain, S. Jahan, M. M. Hussain *et al.*, "A proposal for enhancing the security system of short message service in GSM." pp. 235-240.

[13] A. Nicholson, I. Smith, J. Hughes *et al.*, "LoKey: Leveraging the SMS Network in Decentralized, End-to-End Trust Establishment Pervasive Computing," Lecture Notes in Computer Science K. Fishkin, B. Schiele, P. Nixon *et al.*, eds., pp. 202-219: Springer Berlin / Heidelberg, 2006.

[14] M. Abomhara, O. Kalifa, O. Zakaria *et al.*, “Suitability of Using Symmetric Key to Secure Multimedia Data: An Overview,” *Journal of Applied Sciences,* vol. 10, no. 15, pp. 1656-1661, 2010.

[15] R. Prasad, S. M, and P. Maruthi, “Secure SMS with Identity Based Cryptography in Mobile Telecommunication Network,” *International Journal of Computer Science & Technology* vol. 2, no. 4, pp. 166-169, 2011.

[16] J. Dankers, T. Garefalakis, R. Schaffelhofer *et al.*, “Public key infrastructure in mobile systems,” *Electronics & Communication Engineering Journal,* vol. 14, no. 5, pp. 180-190, 2002.

[17] S. T. Chanson, and T.-W. Cheung, “Design and Implementation of a PKI-Based End-to-End Secure Infrastructure for Mobile E-Commerce,” *World Wide Web,* vol. 4, no. 4, pp. 235-253, 2001.

[18] M. Hassinen, "Java based Public Key Infrastructure for SMS Messaging." pp. 88-93.

[19] M. Hassinen, "SafeSMS - end-to-end encryption for SMS." pp. 359-365.

[20] C. N. J., and O. M. S, “Using an approximated one-time pad to secure Short Message Service (SMS),” *Information and Computer Security Architectures (ICSA) Research Group*, 2004.

[21] C. Kelvin, C. Ming, A. Alapan *et al.*, “Security of Mobile Banking,” *Data Network Architecture Group*, 2003.

[22] M. Toorani, and A. A. B. Shirazi, "LPKI - a Lightweight Public Key Infrastructure for the mobile environments." pp. 162-166.

[23] H. Harb, H. Farahat, and M. Ezz, "SecureSMSPay: Secure SMS Mobile Payment model." pp. 11-17.

[24] Z. Shushan, A. Aggarwal, and L. Shuping, "Building secure user-to-user messaging in mobile telecommunication networks." pp. 151-157.

[25] N. B. Anuar, L. N. Kuen, O. Zakaria *et al.*, “GSM mobile SMS/MMS using public key infrastructure: m-PKI,” *W. Trans. on Comp.,* vol. 7, no. 8, pp. 1219-1229, 2008.