International Journal of Technical Research and Applications e-ISSN: 2320-8163,
www.ijtra.com Volume 2, Issue 6 (Nov-Dec 2014), PP. 94-97

LITERATURE SURVEY: PEER TO PEER TRANSMISSION OF PASSWORD THROUGH SECURE SMS

V. Oviya, Dr. S. Kirubakaran
[1]PG Student, INFO Institute of Engineering, Coimbatore
[2]Assistant Professor, INFO Institute of Engineering, Coimbatore
Ovi Velusamy <oviya.vs@gmail.com>

Abstract: SMS(Short Message Service)plays vital role in day to day life. SMS used in many real world application like Transportation Information System, private health facilities using SMS, mobile banking, participation in elections through SMS, in Crime Scene Investigation and many more.The major problem facing in SMS is security ,while transferring message like account number or password from one user to another user it just taken as a plain text so there some type of attacks like man in the middle attack, disclosure, replay attack takes place and causing a huge risk. The traditional SMS service does not provide information security like confidentiality, integrity, authenticity. The attacker can alter SMS Information using weak encryption algorithm like A5/1 or A5/2.The existing protocol used for providing security in SMS is based on asymmetric and symmetric key. To provide secure end to end communication Easy SMS protocol is used which is completely based on symmetric key. On applying AES algorithm it may provide effective encryption for password. The expecting result on using Easy SMS protocol is to reduce bandwidth consumption and increasing the password or pass code strength through SMS.

Keywords: SMS Security, Cryptographic key, Encryption

I. INTRODUCTION

Short Message Service (SMS) mainly for mobile users to send and receive the messages to each other by using mobile phones and portable devices. The routing and delivery of SMS is managed by the Short Message Service Centre (SMSC), usually owned and run by a telecommunication operator.

A store-and-forward message mechanism is deployed, thereby storing the messages temporarily prior forwarding it to the recipient's phone. If the particular SMS recipient is not online, the SMSC will keep the stored SMS message for a period of time before deleting it from storage. When encryption is not applied to short message transmission then by default the messages could be intercepted and snooped during transmission. SMS messages are stored as plain text by the SMSC before they are successfully delivered to the intended recipient. These messages could be viewed by users in the SMSC who have access to the messaging system. SMS is a popular communication channel and are used for both personal and business communications. Some common examples are Alerts and notifications to customers by stock brokers and banks on stock transaction status. One-time passwords are being sent to the customers of banks or organizations via SMS messages for authorizing or confirming high-risk on-line transactions.

Two-way interactive text messaging is used by people for chatting and gossiping via their mobile phones. As these communications involves some confidential and personal information, it should be communicated effectively without any loss or misuse. But the traditional SMS service doesn't provide any encryption mechanisms for the secure transfer of data leading to security concerns as SMS disclosure, man-in-the-middle attack, replay attack and impersonation attack. Here comes the SMS security mechanism for protecting user's confidential and personal information that gets transmitted via mobile phones and other portable communicating devices. It is achieved by providing end-to-end security during the transmission of SMS over the network by implementing cipher algorithms and use of Symmetric keys while transmitting SMS.

The deployed Security mechanisms should provide lesser computation and communication overheads, effective use of bandwidth and reliable message transfer rate. SMS is now a very common communication tool. Security protection of SMS messages is not yet that sophisticated and difficult to implement in practice. With the increasing use of SMS for communication and information exchange, care should be taken when sensitive information is transmitted using SMS. Users should be aware that SMS messages might be subject to interception. The best solution is encrypted SMS should be considered if there is a need to send sensitive information via SMS.

Global System for Mobile Communications (GSM) is one of the popular mobile phone system in the today environment. GSM classified into three types mobile station(MS), base station(BS), network subsystem. The mobile station (MS) is a combination of mobile equipment and a Subscriber Identity Module (SIM)card.The mobile equipment personally identifies the International Mobile Equipment Identity (IMEI).The SIM card stores the high sensitive information such as the International Mobile Subscriber Identity (IMSI), Ki(a secret key for authentication), and other user information. All this information may be protected by personal identity number(PIN). The Base Station Subsystem contains two major parts are Base Transceiver Station (BTS) and the Base Station Controller (BSC). The Base Transceiver Station manages the radio transceivers that define a cell and handles the Radio-link protocols with the Mobile Station. The Base Station Controller managing the radio resources for one or more BTS. The major component of the Network Subsystem is the Mobile services Switching Center (MSC). The Home Location Register (HLR) and Visitor Location Register (VLR), along with the MSC, provide the Call-routing and roaming capabilities of GSM. (fig 1)

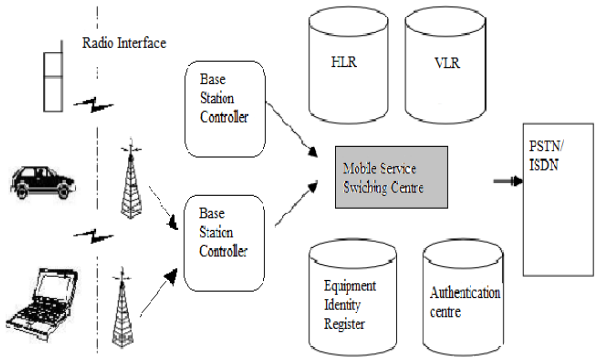

Fig 1: Overview structure of GSM network

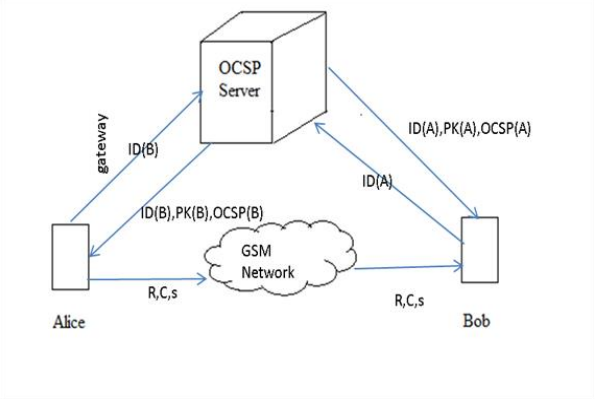

Fig 2: Basic Configuration of SSMS

II. PROBLEM STATEMENT

The traditional SMS(Short Message Service) service does not provide any information security of the message being sent over the network. SMS messages are transmitted as plaintext to the end user. While transmitting SMS to other user it first take place in the network operators system and they can easily retrieve the message. The implemented algorithm is not efficient, which means some algorithm consumes high bandwidth and there could be less computation overhead. The main aim is to secure the SMS by some encryption method and prevent it from the various attacks applied on SMS like replay attack, Man-in-Middle attack, cryptanalysis etc., so there takes some measures in data security like confidentiality, authentication, integrity and non-repudiation.

III. EXISTING SYSTEM

[1] SSMS, used to combine the desired security attributes in the SMS messages mainly to provide secure bearer in the m-payment systems. The SSMS protocol contains three phases are the initialization phase, the message exchange phase in which the participants exchange their secured short messages, and the judge verification phase that is used when any dispute occurs.(a) The initialization phase of the SSMS includes:(i)choose the domain parameters,(ii) Registering the user details into the system, generating the public/private keys, and issuing a certificate for the public key of each user,(iii) Installing the application software on the mobile phone. The elliptic curve *E* defined over the finite field *F* with the Weierstrass equation of the form $Y^2=X^3$ $+aX+b$.. (b)Message Exchange Phase: Alice as the sender wants to securely send her message *M* to *Bob***.** (fig 2) Her message in a payment order and *Bob* may be service provider. (c)Judge Verification Phase: If the Delegated Validation(DV) server can saves the transmitted messages, the judge as an additional proof may query the DV server to confirm that Alice has sent a message which containing(R,C,s) to Bob. SSMS perform by the Online Certificate Status Protocol (OCSP).The OCSP server in the SSMS should checking the status and verifying public key and certifying the good status. It performs under J2ME(Java Mobile Edition) platform. SSMS great advantages to be used in the real m-payment applications and the secure SMS messaging is important. It provide most feasible security services.

[2] A Secure Extensible and Efficient SMS (SEESMS) mainly to transmit secure SMS it main goal is to support several cryptosystems through a modular architecture. SEESMS performs at the application level and can be used for exchanging secure SMS in the P2P(peer to peer). SMS based communication channel as bearer service to exchange encrypted, non-reputable and tamperproof messages. SEESMS performs a secure SMS messages exchange by using binary SMS messages instead of using a traditional messages. Each binary SMS message can hold 140 bytes(equivalent to the 160 7-bit characters used for textual messages). SEESMS allows two peers to exchange encrypted communication between peers by using public key cryptography. Three cryptosystems are RSA(Rivest Shamir Adleman), DSA(Digital Signature Algorithm) and ECDSA(elliptic Curve Digital Signature Algorithm). The RSA cryptosystem is the mostly used for public key based cryptosystem. It include Integer Factorization Problem (IFP) for improving security. The Digital Signature Algorithm (DSA) is the first digital signature scheme based on one to one relationship. The security depends on the Discrete Logarithm Problem (DLP) that to be as hard as the IFP. The Elliptic Curve Digital Signature Algorithm (ECDSA) has been proposed as an ANSI X9.62 standard.Comparing to key-management mechanisms like PGP, SEESMS uses a centralized and light weighted implementation in which only a central authority can distribute signed public-keys. The message is signed by using SH4 hash algorithm and signing the result depends on anyone supported algorithm. It performs under java platform. The results seem to show that RSA and DSA cryptosystems perform generally better than ECDSA, except when using very large key.

[3] SMS is a part of GSM networks that allows the alphanumeric message up to 160 characters to be sent and received.The message generated from External Short Messaging Entity (ESME) is just in plain text which can be easier to read and modified before it reaches to the short message service center(SMSC). To exploit the popularity of SMS in M-commerce and mobile banking, it is necessary to provide the proper security to SMS so that it could reach to the receiver's mobile safely to provide data confidentiality, integrity, authentication, and non-repudiation. The main aim of this method is do the ciphering on SMS first, and then the digital signature are implemented. The plaintext of SMS would be made as cipher text with the help of GSM encryption technology, then this cipher text digitally signed with the help of public key signature. It provides secure end-to-end communications because it is required that SMS must

be secured even from the network operator. The signed encrypted SMS is finally transmitted. The digest algorithm SHA-1 is used for the message digest algorithm and encryption algorithms. This technique implemented in J2ME platform. The asymmetric encryption major advantage is in its functionality. Asymmetric cryptography is used for encryption. This technique prevent from substitution of fake SMS also.[4] SMS communication is not properly secure and not trustworthy. SMSSec is a protocol it mainly depends on both asymmetric and symmetric key cryptography and two-factor authentication process. The end to end encryption is widely performed in this section as shown(fig).the encryption algorithm on this method should possess three attributes,(i)The encrypted message should be in the form of ciphertext, (ii)The encryption algorithm cannot alter the size of the message, no padding mechanism,(iii)The encryption algorithm should be simple and computationally inexpensive. In SMS sec secret keys are not transporting and not share user's personal identification number (PIN) on any computing environment like GSM network. symmetric cipher it choice to use the AES for encryption and decryption, asymmetric cipher use the RSAES. Asymmetric cryptography the authentication is for both public and private key management. It performs under java platform. The public and private key are generated from server where the private key are secure under storage mechanism.

DISADVANTAGES

- The SSMS generate shared key for each session but also generate huge overheads and not suitable for the real world applications.
- Weak and Broken stream cipher algorithm is implemented.
- Implementation of SEESMS framework not much suitable for the resource constraints devices such as mobile phones.
- Asymmetric encryption is slower than symmetric encryption because they require more computational processing power.
- Less Energy Expensive.
- Improve Feasibility, Scalability for the existing protocol

IV. PROPOSED SYSTEM

Easy SMS which may provides end-to-end security during the transmission of SMS in the network. Symmetric Cryptography is the main technique for encryption used to provide end-to-end security to Easy SMS messages. This protocol well suited for mobile devices due to their limited resources, i.e., limited power/energy, insufficient memory and less processing power.

Easy SMS service provides encryption to the information before its transmission. Key distribution mechanism remains secure because encryption key based on SIM card used. Easy SMS protocol is able to prevent from attackers and intruders for SMS while transmitting to the other user through the network. In this technique the cryptographic functions are not publically available, it maintain secret where the network operators cannot identify the message. The snapshot of any secret key SK is not possible because no secret key has been transmitted in any phase of the proposed protocol and always a delegation key DK1 is being transferred in the cipher mode whenever is required. Secret keys are not publically available and are secret. AES is a symmetric key block cipher. The key can be based on three rounds 128 bits (16 bytes), 192 bits (24 bytes), or 256 bits (32 bytes) in length. AES using the same key for both encryption and decryption is called a symmetric encryption algorithm. In AES each round is based on four type of transformation are

i. Sub-Byte-It is predefined mainly used for encryption and decryption,
ii. Shift-Row-Shifting row from one round to another,
iii. Mix-Column-Constant Square Matrix are predefined,
iv. Adding Round key-keeping Round Constant, it mainly used for key expansion.

Easy SMS is the first protocol which is completely based on the symmetric key cryptography. It retains original architecture of cellular network and Mutual Authentication between MS and AS. It may provide Efficient Key Management comparing to existing protocol. AES with 128-bit key may be an efficient algorithm to encrypt the SMS. The Architecture design for proposed scheme is figure below(fig 3).,

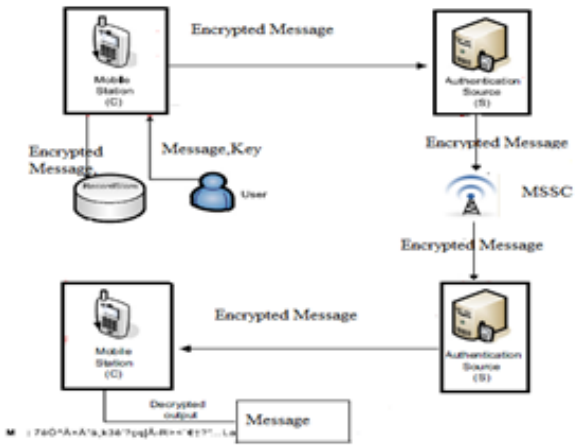

Fig 3: Architectural Design

SNO	STEPS	ENCRYPTION ALOGORITHM	DECRYPTION ALGORITHM
1	STEPS	1)Sub Byte 2)Shift Row 3)Mix Column 4)Add Round Key	1)Add Round Key 2)Inv Mix Column 3)Inv Shift Row 4)Inv Sub Bytes
2	INPUT	Password in unrecognized format	Variable Length Message
3	KEY	+91 and Receiver Phone Number	RECEIVER SIM CARD
4	ALGORITHM	AES Encryption Algorithm	AES DECRYPTION Algorithm
5	OUTPUT	Unintelligible Format	Password in Recognized format.
6	INPUT SIZE	Maximum 10 Character	Variable Length Message.
7	KEY SIZE	15 DIGITS(13+2 for Digital Signature)	13 DIGITS.
8	OUTPUT SIZE	Variable Length Message	Maximum 10 Character

AES Algorithm Step by Step Procedures for Proposed Method

ADVANTAGES

- Mutual Authentication Between MS and AS
- Efficient Key Management
- Reduce Computation Overhead Comparing to existing protocol
- Communication Overhead
- Increasing Bandwidth Utilization
- Resistance to Attacks(SMS Disclosure, Replay Attack, Man-in-the-middle Attack, OTA Modification in SMS Transmission, Impersonation Attack)
- Speed up encryption and decryption process.

V. CONCLUSION

The expecting result of the proposed protocol is to prevent from various attacks. The transmission of symmetric key to the mobile users is may efficiently managed by the protocol.On overview of the existing method is motivate to deeper analysis of the algorithm and implement it properly. This protocol may expected to produces lesser communication and computation overheads, utilizes bandwidth efficiently, and reduces message exchanged ratio comparing to existing protocol. It may improve password or account details can be send securely to authenticated user.

REFERENCES

[1] M.Toorani and A. Shirazi, "SSMS—A secure SMS messaging protocol for the m-payment systems," in *Proc. IEEE ISCC*, Jul. 2008, pp. 700–705.

[2] A.De Santis, A. Castiglione, G. Cattaneo, M. Cembalo, F. Petagna, and U. F. Petrillo, "An extensible framework for efficient secure SMS," in *Proc. Int. Conf. CISIS*, 2010, pp. 843–850.

[3] Neetesh Saxena "Enhancing Security System of Short Message Service for M-Commerce in GSM", IJCSET, ISSN: 2229-3345 Vol. 2 No. 4.

[4] J. L.-C. Lo, J. Bishop, and J. H. P. Eloff , "SMSSec: An end-to end protocol for secure SMS," *Comput. Security, vol. 27, nos. 5–6*, pp. 154–167, 2008.

[5] Neetesh Saxena, *Member, IEEE*, and Narendra S. Chaudhari, *Senior Member, IEEE* "EasySMS: A Protocol for End-to-End Secure Transmission of SMS", IEEE Transactions on Information Forensics and Security, Vol. 9, No. 7, July 2014.

[6] E.Biham, "Design tradeoffs of the AES candidates," in *Asiacrypt* (Lecture Notes in Computer Science). New York, NY, USA: Springer- Verlag, 1998.

[7] M. Hassinen, "Java based public key infrastructure for SMS messaging," in Proc. 2nd ICTTA, 2006, pp. 88–93. [20] S. Wu and C. Tan, "A high security framework for SMS," in Proc. 2nd Int. Conf. BMEI, 2009, pp. 1–6.

[8] S.Kirubakaran,C.Manoharan,"Performance Study on Handoff Delay and Packet Loss in Heterogeneous Mobile Wireless Network", European Journal of Scientific Research, ISSN 1450-216X Vol.77 No.3 (2012), pp.373-385.

[9] Ruth E. Anderson, Waylon Brunette, Erica Johnson, Caitlin Lustig, Anthony Poon, Cynthia Putnam, Odina Salihbaeva, Beth E.
Kolko, Gaetano Borriello,"Experiences with a Transportation Information System that Uses Only GPS and SMS".

[10] Jay Chen, Lakshmi Subramanian, Eric Brewer" SMS-Based Web Search for Low-end Mobile Devices.

[11] Patrick Traynor, William Enck, Patrick McDaniel, and Thomas La Porta"Mitigating Attacks on Open Functionality in SMSCapable Cellular Networks".