International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 4 (2015) pp. 10323-10331

http://www.ripublication.com

Efficient Cipher - SMS Communication Using Cryptographic Algorithms

B.Bala Abirami[1]

College and Dept: S.A Engineering College, Department of CSE
Postal Address: 3/772, Kamarajar street, Arunachalam Nagar, Chennerkuppam, Chennai-600056
Email ID: bala.bami@gmail.com

Dr.G.Umarani Srikanth[2]

College and Dept: S.A Engineering College, Department of CSE
Email ID: gmurani@yahoo.com

J.Sunitha[3]

College and Dept: S.A Engineering College, Department of CSE
Email ID:sunithaj04@gmail.com

U. Narmatha[4]

College and Dept: S.A Engineering College, Department of CSE
Email ID:narmi84@gmail.com

Abstract

SMS has become one of the quickest and robust communication channels to transmit the information across worldwide. Confidential information can also be send through SMS. Sometimes there is a tendency to hack the secure information by the persons at SMS Center (SMSC) if it is transmitted as plaintext. The traditional SMS service offered by various mobile operators surprisingly does not provide information security of the message being sent over the network. It is recommended to apply the cryptographic techniques such as encryption and decryption to protect such information. It uses a centralized Authenticated Server to store all the details of legitimate users. This paper uses Cipher-SMS protocol to guard the confidential messages.

Keywords— AES, Authentication Server, Decryption, Encryption, MD5, SMSC.

I. INTRODUCTION

Nowadays SMS plays a vital role in our day to day life because of its mobile - friendly, direct, simple, and cost-effective nature. In the recent few years, mobile devices such as laptops, palmtops and smart phone have been very popular. Smartphone users worldwide will total 1.75 billion in 2014.Because of its rapid growth it is widely used in business areas such as mobile commerce, mobile banking, governance, medical field and so on. In all these applications SMS plays a very big role, the user can get their SMS anywhere in the world.

A. Research Problem

We can send personal, business, confidential information through SMS. Online bank transactions, OTP send by banks or organizations via SMS messages for authorizing or confirming high-risk on-line transactions.

There are some issues associated with the open functionality of SMS, because the messages are transmitted as a plain text among the sender and receiver across the network. There is a chance for the hackers to read the message.

B. Key Contribution

In this paper Cipher-SMS model is proposed. It uses an efficient encryption and decryption technique for SMS communication. The process of transforming plain text to cipher for data security is also proposed. The above problem can be accomplished by this protocol.

C. Organization

This paper has organized into VI sections. Introduction is given in section I. Section II gives the model of proposed work. Section III deals with the system implementation. Section IV illustrates the suitable algorithm for proposing this paper. Conclusion is given in section V. Finally, section VI gives the future work.

II. PROPOSED SYSTEM

This section focuses on the system design specification that deals with the design aspects of the proposed system. The design models overall relates how the user creates the confidential message and the process of forwarding and authenticating. The main aim of this work is to send the messages confidentially and to avoid various attacks. The end-to-end security in mobile communication is provided by this approach. This work involves a new component, an Android mobile phone which is used to transmit authentication messages.

Android is an efficient Operating System supporting a large number of applications in smart phones. These applications make life more convenient and advanced for the mobile phone users. Some of its features are:

(i) Android is built on the open Linux Kernel and it is easy to implement in smart phones. It breaks down the hindrance in building new and innovative applications.

(ii) Fast & easy application development-It has a wide range of useful libraries, which is used to build rich applications

The Cipher-SMS protocol is implemented in application layer. The Android OS application framework provides this additional functionality. It is based on java language. Android is an open source for developers to develop applications The Android SDK includes a variety of custom tools that help you develop mobile applications on the Android platform. In the existing method, the message size is limited to 160 characters because it is implemented in normal mobile phones. The message size in Cipher-SMS is unlimited.

Fig.1 depicts the overall view of this work, when exchanging the SMS between sender and receiver. It is the pictorial representation of the entire work which is to be carried out. This architecture consists of four phases. Each phase is listed separately and described in detail in the later part.

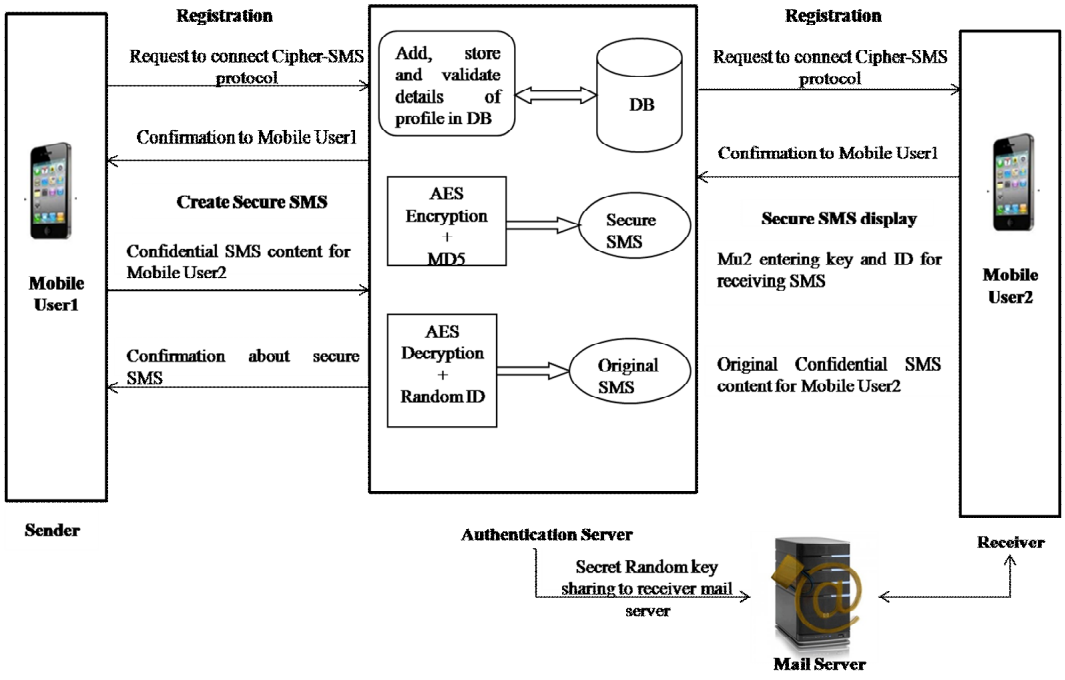

Fig: 1 Structure of Cipher-SMS protocol

A. Proposed Protocol: Cipher-SMS

There are four major components in Cipher-SMS protocol. They are Mobile User1 (Mu1), Authentication Server (AS), Mobile user2 (Mu2) and Mail Server. The Mobile user1 at sender side has to register their details and this will send as a request signal to Authentication Server .The new user details will be moved to AS database. The server

will send a conformation request to the Mu1.The Mobile user1 send the SMS content for Mobile user2.The Authentication Server checks for valid user through its database. Then it encrypts the message using AES and generates secure SMS. The Random number is generated using MD5, both these are accumulated in Authentication Server.

In Receiver side, the Mu2 also performs registration with AS for authentication in the communication. The user requests random ID for Decryption. The Authentication Server sends the secret key only to the authenticated user. The secret key is sent to the Mu2 mail server. It sends the secret key to the receiver side AS, it will perform decryption to the Cipher SMS and send the original SMS to the Mu2.

B. System and communication model

This subsection depicts the working model of communication system using the Cipher-SMS. It is broadly classified into four phases.

(i) *Registration phase:* The Mu1 sends a service request to the AS. Along with other details the AS creates a user profile using the user IMSI number and mail_id. User details are handled in a common database. The user login or logon is the process by which individual access to the service is controlled by identifying and authenticating the user referring to credentials presented by the user. A user can log in to a system to obtain access and can then log out or log off when the access is no longer needed. After validation the AS sends a conformation request to the validated Mobile user1.

(ii) *Create Secure SMS:* The Mu1 creates SMS for Mu2 and it is sent to the AS. It checks for validity, if it is from valid user, the AS will perform symmetric key encryption. It will encrypt the message using AES algorithm.

(iii) *Random key generation:* The AS generates a Random ID using MD5 algorithm for the cipher format SMS. The encrypted message travel through the base station and Mu2 receives the message in secure inbox. Now the receiver wants to decrypts the message. The server generated random number is sent to Mu2 valid mail server.

(iv) *Secure SMS display:* The AS checks for the valid user request from mobile user2 by its IMSI number and mail_id. It checks in its database. It will reject the unauthorized user request. The receiver sends the secret key to AS for decryption. It will check for the userID in its database. The AS will decrypt the message along with the secret key and random ID. Then the decrypted message is send to the receiver for display.

III. SYSTEM IMPLEMENTATION

In this subsection, we propose a new protocol named Cipher-SMS with two different scenarios which provide end-to-end secure transmission of information in the cellular networks. It deals with sending messages from Mobile user1 (Mu1) to Mobile user2 (Mu2). There are two main entities in the proposed protocol one is the Authentication Server (AS), and the other is Certified Authority/Registration Authority (CA/RA) [8].

AS is one of the most fundamental building blocks for providing communication security. It provides an efficient key sharing framework designed to provide authentication service for mobile networks. Second entity CA/RA stores all the information related to the mobile subscribers. Every subscriber has to register his/her mobile number with CA/RA entity and only after the verification of identity, the user can send message. Thus, this is responsible to authenticate the identity of the subscribers.

Scenario-1 when both MS belong to the same AS:

In this scenario, the Mu1 wants to send an SMS to the Mu2, who is in the same AS that is in the same HLR (Home Location Register). It works as follows,

(1) The Mu1sends a service request to the Mu2.The initial service request comprises of International Mobile Subscriber Identity (IMSI) number of Mu1, a service request number RNo, a Timestamp T1.

$$Mu1 \longrightarrow Mu2: ServiceReq\ (IMSI1, RNo, T1).$$

The AS gets the service request checks in its CA/RA and sends a conformation request to Mu1.

(2) On receiving conformation request, Mu1send the SMS content to AS. It will perform encryption using ak (which will be described in next section) and generate a cipher format SMS.

$$Mu1 \overset{ak}{\longleftrightarrow} AS$$

(3) In the meanwhile, the AS sends a Random ID to Mu2 mail server.

$$AS \overset{RID}{\longleftrightarrow} Mu2$$

(4) The Mu2 must also perform registration with the AS, the message is send only to the authenticated user by the AS. This authentication is performed by CA/RA.

$$Mu2 \longleftrightarrow AS: ServiceReq\ (IMSI2, RNo, T1).$$

Scenario-2 when both MS belong to the different AS:

In this scenario, the Mu1 wants to send an SMS to the Mu2, who is in different AS that is in the different HLR (Home Location Register). It works as follows,

(1) The Mu1 composes a message to Mu2.It is send to the nearest SMSC, then it is send to the AS that is within the same HLR. The AS gets the service request checks in its CA/RA.
(2) The AS checks for the (receiver) Mu2's SMSC, whether it is in same HLR or not. If it is different, the AS sends its encrypted message to SMSC2 (different network).
(3) Then the message is received by the receiver AS and the process works as stated in scenarion1.

The main difference in scenario 1 and 2 is the message communication takes place among AS of different network.

IV. ALGORITHM USED

This section focuses on two cryptographic algorithms, which are AES and MD5 for providing higher security to the SMS transmission. Block cipher based symmetric key algorithm is efficient than the stream cipher. The performance of block cipher algorithm relies on key size and block size. It takes large chunk of data in one cycle and it speeds up the execution. The security depends on the number of rounds. A large number of rounds make the process more secure.Existing methods include DES, Triple-DES with 2 keys, RSA, Elliptic Curve Cryptography. DES used 56-bit key to 64-bit data block. Its security has become weak, because it is insecure [17]. Triple-DES with 2 keys takes more computation time and it is slow [6].By using RSA in [9] the encrypted message size is large. The elliptic curve cryptography involves complicated group operations and pre-computed tables. These drawbacks can be rectified in Cipher-SMS protocol by combining AES-128 and MD5.It is highly secured, fast and doesn't include more tedious computations. The following subsections demonstrate the working model of AES and MD5.

A. AES

AES algorithm can accept can accept a block size of 128 bits and with a choice of three keys-128,192,256 bits. Cipher-SMS uses 128 bit keys, [5] to improve the performance of the protocol. Various steps of AES-128 are as follows:

(1) Key generation: In cipher-SMs protocol, 128 bit key of ak is generated at the Mu1 and AS which is used as a cipher key for AES.
(2) Initial round: Add Round Key:-bit-by-bit XOR is done with an expanded key.
(3) Rounds:
(i) Substitute Bytes: byte-by-byte substitution using a 16 x 16 matrix of bytes.
(ii) Shift Rows: a permutation, which cyclically shifts the last three rows in the state
(iii) Mix Columns: a substitution that uses GF (2^8) arithmetic
(iv) AddRoundKey.

(4) Final round: It uses three rounds except Mix Columns.

B. MD5:

MD5-"Message Digest5" is a cryptographic hash function. It is used to make clear that the messages send between Mu1and Mu2 are similar or not. The perfect match of MD5 value ensures that the data integrity and security of the SMS has not been violated by someone else and also that it is the exact copy of the original message. It takes input of random length and produces a constant output. The input M can be of any size or length, but the output hash value is fixed.

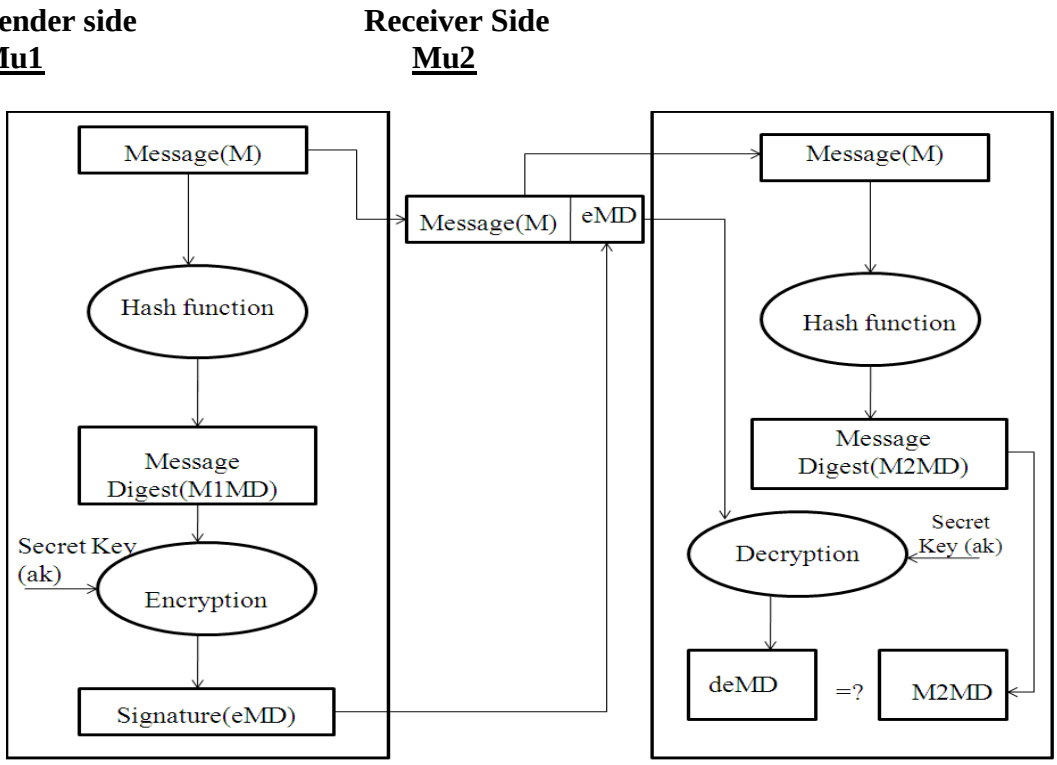

Fig. 2. Working of MD5 algorithm

The working of MD5 algorithm is shown in Fig.2.It is illustrated below as follows.

(1) Sender side: Mobile user1 creates an input message (M) and computes its message digest (M1MD). Then it uses its secret key (ak) and encrypts the message digest (eMD).

(2) Encrypted message digest (eMD) is attached to the input message (M) and the whole message (M-eMD) is sent to (receiver) Mu2.

(3) Receiver side: Mobile user2 gets the message (M-eMD) and extracts the encrypted message digest (eMD). Then it computes its own message digest (M2MD) of the received message (M).

(4) Mu2 also decodes received message digest (eMD) with secret key (ak) and gets decoded message digest deMD). Then he compares both message digests

(M2MD? = deMD). When both are equal, the message (M) was not altered during the data transmission.

C. Contention against attacks

In this section, we justify that Cipher-SMS can fight against various attacks in the message communication over the network. The cryptographic methods used in this paper are secret and not publicly known to any mobile user. It uses a secret key ak and Message digest eMD which provides high data security.

(i) *SMS Disclosure:* In the Cipher-SMS protocol, the highly secured cryptographic algorithm of AES and MD5 is used. It provides an end-to-end confidentiality to the message and it cannot be disclosed by the mobile operators at SMSC.

(ii) *OTA Modification:* OTA Modification is an attack in which the hackers modify the SMS content, which is sent by OTA gateway. In this the operator's back-end system sends service requests to an OTA Gateway which transforms the requests into Short Messages and sends them onto a Short Message Service Centre (SMSC) which transmits them to one or several SIM cards in the field. Thus, Over-The-Air (OTA) is a technology that updates and changes data in the SIM card. The strong encryption algorithm of AES provides security to the OTA interface and thus it avoids this attack than the exiting algorithms of A5/1 and A5/2

(iii) *Play back attack:* Each message uses a timestamp, the unique timestamp value T1 used in message communication prevents this attack.

(iv) *MITM attack:* A Man-in-the-Middle attack allows a wicked user to intercept, send, and receive message for someone else. In normal flow there are no intruders to hack the message, whereas in MITM the confidential message is hacked by the man-in-the-middle. The hacker notifies the communication and performs data hacking. The server thought that it is from normal client. . Man-in-the-Middle attacks can be denoted in any of the following form such as, MITM, MitM, MiM, or MIM. The Authentication server keenly notifies the communication and it maintains the entire user login in its database and thus it avoids MITM

(v) *Masquerade:* A masquerade takes place when one entity pretends to be a different entity. It is a form of active attack. The Cipher-SMS uses IMSI number of each mobile users and this it avoid this attack

V. CONCLUSION

As smart phones are getting more prevailing, they are subjected to various attacks. In this paper the symmetric key cryptography of AES and hash cryptography of MD5 is introduced using Cipher-SMS. It is an application layer protocol that provides a high degree of data integrity, confidentiality and user authentication to the transmitted messages. The scalability and efficiency for secured web authentication using a personal device has been found out to be extremely essential. It shows that the protocol is able to avoid many attacks. The transmission of symmetric key to the

mobile users is efficiently managed by the protocol. This Cipher-SMS protocol provides higher security than EasySMS because it uses AES and MD5. Proposed SMS based framework provides a reliable, low cost and effective solution for SMS Transmission.

VI. FUTURE ENHANCEMENTS

For the future work this can be implemented with Multimedia Message Service such as image, Audio, Video and needs to use high compression technique. It has become one of the fastest and strong communication channels to transmit the information.

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] Y. Zeng, K. Shin, and X. Hu, "Design of SMS commanded-and controlled and P2P-structured mobile botnets," in Proc.5th WiSec, 2012, pp. 137–148.

[3] K. Yadav, "SMSAssassin: Crowdsourcing driven mobile-based system for SMS spam filtering," in Proc. Workshop Hotmobile, 2011, pp. 1–6.

[4] I. Murynets and R. Jover, "Crime scene investigation: SMS spam data analysis," in Proc. IMC, 2012, pp. 441–452.

[5] C. H. Kim, "Improved differential fault analysis on AES key schedule," IEEE Trans. Inf. Forensics Security, vol. 7, no. 1, pp. 41–50, Feb. 2012.

[6] Neetesh Saxena and Narendra S. Chaudhari, "EasySMS: A Protocol for End-to-End Secure Transmission of SMS" IEEE Trans. Inf. Forensics and Security, vol. 9, no. 7, pp. 1157–1168, July. 2014

[7] P. Traynor, W. Enck, P. McDaniel, and T. La Porta, "Mitigating attacks on open functionality in SMS-capable cellular networks," IEEE/ACM Trans. Netw., vol. 17, no. 1, pp. 40–53, Feb. 2009.

[8] A. Medani, A. Gani, O. Zakaria, A. Zaidan and B. B. Zaidan "Review of mobile short message service security issues and techniques towards the solution" Scientific Research and Essays Vol. 6(6), pp. 1147-1165, 18 March, 2011.

[9] Manoj Patil, Prof. Vinay Sahu "A Survey of Compression and Encryption Techniques for SMS" International Journal of Advancements in Research & Technology, Volume 2, Issue 5, May-2013.

[10] 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.