ISSN 2347 - 3983

**International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 85- 88 (2015)**
*Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati*
***http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp17.pdf***

# Cipher SMS: A Protocol for End-to-End Secure

**K.Masthanamma[1], G.Rajeswarappa[2]**
[1]M.Tech CSE Student, S.V.Engineering College for Women, Tirupati, AP, India
Shahi.vahi@gmail.com
[2]Assistant Professor, Dept. of CSE, S.V.Engineering College for Women, Tirupati, AP, India,
rajeswarappag @gmail.com

## ABSTRACT

Short Message Service (SMS) has become one amongst the quickest and potent communiqué channels to broadcast the information diagonally the worldwide. Every so often, we have a propensity to send the information like transaction ids, pass code, banking details and personal identity to our friends, members of the family and repair suppliers through associate SMS. SMS messages are transmit as plaintext stuck between mobile user (MS) and also the SMS center (SMSC), exploitation wireless network. SMS contents are keep within the systems of network operators and might be browse by their personnel. In view of the fact that, the SMS is disseminated as plaintext, for that reason network operators will cleanly admittance the content of SMS all through the transmission at SMSC. That the ancient SMS service presented by numerous mobile operators amazingly doesn't offer data security of the message being sent over the network. so as to guard such wind, it's powerfully needed to produce finish-to-end secure communiqué amid end users. The on top of needs are regularly consummate through proposing a protocol well-known as Cipher-SMS. It provides end-to-end safekeeping all the way through the communication of SMS over the network. This protocol can be performed via exploitation scientific restraint algorithms of AES and MD5. This protocol prohibits the data of Short Message Service (SMS) from plentiful attacks together with SMS revelation, modification of over the air (OTA), playback attack, impersonation attack, and man-in-the-middle attack. Planned SMS primarily based framework provides a low-bandwidth, reliable, economical and value effectual answer for SMS Transmission. Cipher-SMS is that the 1st protocol fully supported the habitual key and hash cryptography of AES and MD5 for cellular network.

**Key words**: SMSC, OTA, AES, MD5.

## 1. INTRODUCTION

There are many quickest and powerful communication channels in world to transmit the knowledge across the global wide. One among them is Short Message Service (SMS). Sometimes, we have a tendency to send the wind like positive identification, pass code, banking details and personal identity to our friends, members of the family and repair suppliers through an SMS.

SMS messages area unit transmitted as plaintext between mobile user (MS) and therefore the SMS center (SMSC), victimisation wireless network. SMS contents area unit keep within the systems of network operators and may be scan by their personnel. Since, the SMS is distributed as plaintext, so network operators will simply access the content of SMS throughout the transmission at SMSC.That the ancient SMS service offered by varied mobile operators amazingly doesn't give info security of the message being sent over the network. So as to defend such wind, it\'s powerfully needed to supply finish-to-end secure communication amid end users. The higher than a necessity is consummate through proposing a protocol well-known as Cipher-SMS. It provides end-to-end safekeeping all the way through the communication of SMS over the network. The Cipher-SMS can be performed via victimisation science algorithms of AES and MD5.This protocol prohibits the information of data SMS from varied attacks together with SMS revelation, modification of over the air (OTA), playback attack, impersonation attack and man-in-the-middle attack . Intended SMS primarily based framework provides a low-bandwidth, reliable, economical and price effectual resolution for SMS Transmission. Cipher-SMS is that the 1st protocol utterly supported the cruciform key and hash cryptography of AES and MD5. EasySMS provides secure communication from finish-to-end between end users through SMS. EasySMS is dead that makes out there the symmetrical bilateral shared key amid each MS then ciphering of message takes place employing a symmetric key algorithmic program. The operating of the protocol is conferred by considering 2 totally different eventualities area unit SMSSec and PK-SIM protocols. SMSSec protocol is accustomed secure an SMS communication sent by Java's Wireless electronic communication API whereas the PK-SIM protocol proposes a emblematic SIM card with further PKI practicality. Each protocols area unit supported client-server paradigm. In EasySMS protocol, a science undisclosed script algorithmic program AES/MAES is maintained to give end-to-end secrecy to the transmitted SMS within the network. EasySMS give SMS security with cruciform key cryptography, the in attendance protocol is utterly supported cruciform key cryptography. Cruciform key is transmitted to the mobile users with competence and managed by the protocol. Security loses once hacking key conduction

ISSN 2347 - 3983

**International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 85- 88 (2015)**
*Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati*
***http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp17.pdf***

between Mobile Station. Cipher-SMS provides the security throughout the transmission of SMS between end-to-end users over the network. This protocol can be performed by victimisation science algorithms of AES and MD5. This protocol prohibits the data of Short Message Service (SMS) from plentiful attacks together with SMS revelation, modification of over the air (OTA), playback attack, impersonation attack, and man-in-the-middle attack. Planned Short Message Service (SMS) primarily based framework provides a low-bandwidth, reliable, economical and price effective resolution for SMS Transmission. Cipher-SMS is that the 1st protocol utterly supported the cruciform key and hash cryptography of AES and MD5 algorithms are used for cellular network. This protocol sends transmitted bits with less range , it provides computation overhead is less, and less damage of information measure and message changed as compare to existing protocols. It provides less communication and computation overheads, exploit information measure with efficiency, and reduces message changed throughout authentication than EasySMS (existing) protocols. Here most all the rage a cruciform key algorithmic program of AES with MD5 as a result of these algorithms area unit a thousand times quicker than the uneven algorithms and improve the potency of the system. Achieved a lot of security than EasySMS by victimisation AES with MD5 algorithms. No use once Hacking AES key between Mobile Station, as a result of MD5 generates wholly special key ID of every transmission. The Cipher-SMS protocol generates minimum communication and computation outlay as compare to existing.

**2. Secure SMS through Encryption based channel coding algorithm**

SMS contains a variety of benefits and drawbacks for M-Commerce purpose. the benefits are it's simple to use, a typical transmission tool among customers, works across all wireless operators, low value for mobile users, no specific software package is required for installation, permits banks and cash institutions to provide amount of your time knowledge to shoppers and staff and hold on messages is accessed whereas not a network affiliation. Most important disadvantage of SMS is that it does not offer a secure setting for confidential data throughout transmission and there is no procedure to certify the SMS sender. There is a want for associate end to complete SMS secret writing with excellent message transmission therefore on offer a secure with error free data transmission for communication. These a pair of factors unit of measurement important for SMS throughout this paper, we have got analyzed concerning primarily JCCC and Soft Input secret writing (SID). We've got a bent to planned a novel in theory theme NTRU Sign rule throughout this paper. We've got a bent to stand live expect that it\'ll improve this security level speed and provide reliable message at receiver end.

**2. PDA PUSH Service by Implementing Security Message Protocols**

In this paper, we've got a bent to propose and implement a service model to transfer messages safely for personal digital assistant on CDMA wireless networks and a secure message transfer protocol that considers characteristics of personal digital assistant. The planned PUSH service uses SMS (short message service) to connect Associate in Nursing offline client device with the wired network for transmission. Once receiving SMS message, client device methodology the SMS message and creates a data channel thought RAS (remote access service), then the information of the server are pushed to client. The enforced securing protocol can offer safe data transmission on each communication thought two manner channels of SMS and data. This protocol can cut back kind of transmissions for exchanging a secure session key by victimization security gift table. As a result, intensity of cryptography are hyperbolic.

**4. SMS through High Security Communication Protocol**

Now a days, short message service (SMS) is faced with abundant refuge threats. Thus, the fields of soaring confidentiality (e.g., mobile E-commerce) need a better level of safety measures protection on SMS. Secure communication in unimaginable mobile network has vital significance. This paper presents a high security communication protocol for SMS. Through authentication, coding and integrity protection, it establishes Associate in Nursing end-to-end secure channel between server-side and mobile terminal. Through analyzed it by svo logic, this protocol is proved to craft sure confidentiality, integrity and non-repudiation of SMS messages.

**5. Implementing Performance evaluation for mobile banking system on end-to-end security architecture**

The advantage of mobile penetration permits mobile operators to contribute appeal further service like secured mobile banking, mobile commerce and supply increased security for web banking. Mobile banking is enticing as a result of it\'s a convenient come close to execute banking from anyplace any time, nevertheless there are security considerations within the accomplishment, that embrace issues with GSM, network, SMS, GPRS protocols. During this paper Associate in Nursing end-to-end security framework victimization PKI for mobile banking is planned. Recital of the premeditated model is conferred during this paper**.**

**6. Implementing a Secure Information Transmission Scheme Based on Polar Coding with a Secret Key**

In this letter, a replacement secure data transmission theme supported polar codes with a pre-shared secret secret's

ISSN 2347 - 3983

**International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 85- 88 (2015)**
*Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati*
***http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp17.pdf***

planned. In polar codes, when the channel polarization is iatrogenic, sensible split channels square measure accustomed transmit the user message and dangerous channels square measure used to support the reconstruction of the message by sharing fastened data. If the fastened data in dangerous channels is secret, Associate in Nursing antagonist gets issue in reconstructing the user message in sensible channels while not information of the fastened data. From this observation, we tend to construct a secure data transmission theme. By appending pre-/post-processing that imposes a dependency between the transmitted message sub-blocks, the adversary's issue may be modified to trait, since solely partial data may be decidable by attackers. a replacement category of secret key theme is developed in such some way.

## 7. CIPHER-SMS

The Cipher-SMS provides end-to-end security all the way throughout the transmission of SMS in excess of the network. This protocol can be performed by mistreatment cryptanalytic algorithms of AES and MD5. This protocol avoids the data of SMS from various number of attacks as well as SMS revealing, modification of over-the-air(OTA), playback attack, man-in-the-middle attack, and impersonation attack. Proposed SMS first and foremost based framework provides a low-bandwidth, reliable, economical and value effective answer for SMS Transmission. Cipher-SMS is that the 1st protocol fully supported the bilateral key and hash cryptography of AES and MD5 algorithms. This Cipher-SMS sends slighter range of transmitted bits, generates with a reduction of computation visual projection, and reduces information gauge consumption and message misrepresented as judge against to existing protocols.

## 8. SYSTEM ARCHITECHTURE

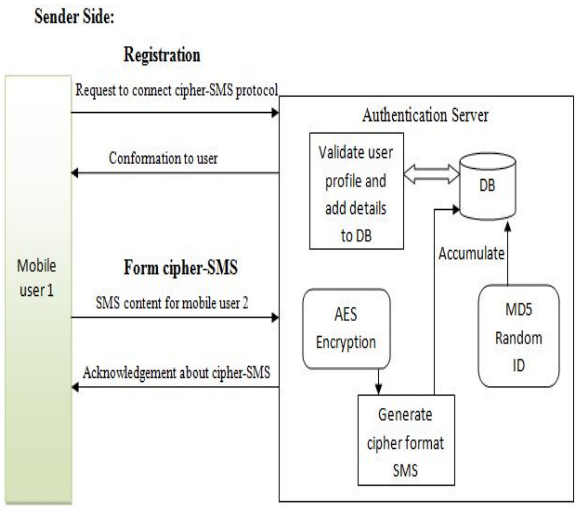


Fig 1: Sender Side of Cipher-SMS

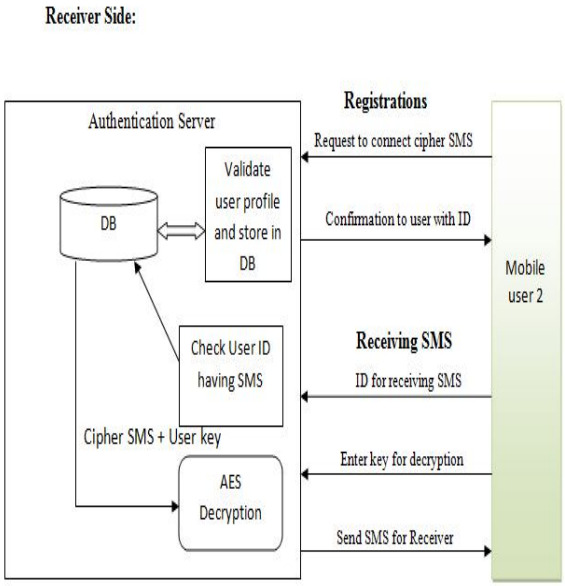


Fig 2: Receiver Side of Cipher-SMS

### 8.1 User Profile Module:

The mobile device that recognizes the authenticated user by receiving the user details with some parameters. This restricts the non-owner users to see information about the SMS we send. However, any mobile device can using this services to getting some additional profile examination. It can be handled with some unique parameters. Throughout this utility, the mobile device can allow to access the data and secured SMS can be send to others with authenticated profile owner.

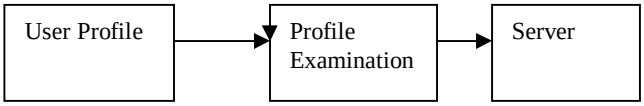


Fig 3: User profile module of Cipher-SMS

### 8.2 SMS (Shortest Mobile Service) Communication:

The genuine mobile user be capable of send the SMS with some key to the server. The mobile user must be registered with server who wants to send the SMS and again the mobile user can sends the SMS to server with certain key. The server can encrypted the original message by using AES algorithm and then send the SMS to receiver through base station and mobile station.

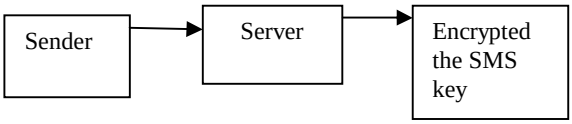


Fig 4: SMS Communication of Cipher-SMS

ISSN 2347 - 3983

**International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 85- 88 (2015)**
*Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati*
***http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp17.pdf***

**8.3 Authentication Server:**

The Encrypted message preserve voyage through base station. Receiver receives the message in secure inbox. Now the receiver wishes to decrypts the message. So receiver needs the key by means of random number initiator from server. Then servers generates the random number and send it to the receiver.

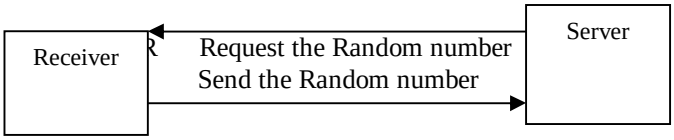


Fig 5: Authentication Server of Cipher-SMS

**8.4 Symmetric Key:**

Server recognizes the random number from receiver; from this server authenticate the endorsed receiver. Then server sends the symmetric key to receiver. After getting symmetric key, receiver decrypts the encrypted message and extracts the original message in secure inbox.

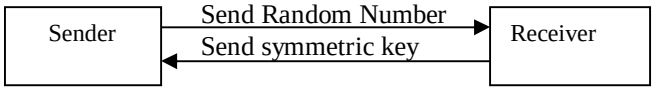


Fig 6: Symmetric Key of Cipher-SMS

**9. RESULTS**

This protocol produces less significant communication and computation overheads, utilizes bandwidth efficiently, and reduces message exchanged during substantiation than EasySMS (existing) protocols. Here favored a symmetric key algorithm of AES with MD5 for the reason that these algorithms are 1000 times faster than the asymmetric algorithms and progress the competence of the system. Achieved more security than EasySMS by using algorithms of AES and MD5. No use when Hacking AES key flanked by Mobile Station, for the reason that MD5 generates poles apart key ID of apiece transmission.

**10. CONCLUSION**

EasySMS protocol is with triumph premeditated so as to fabricate end-to-end protected communication all the way through SMS stuck between mobile users. The psychotherapy of the predictable protocol shows that the protocol is geared up to forestall numerous attacks. The transmission of parallel key to the mobile users is expeditiously managed by the protocol. This protocol produces lesser communication and computation overheads, utilizes information measure expeditiously, and reduces message changed throughout authentication than SMSSec and PK-SIM protocols.

**REFERENCES**

[1] Press Release. (2012, Dec. 3). Ericsson Celebrates 20 Years of SMS [Online]. Available:http://www.ericsson.com/ag/news/2012-12-03-smsen_3377875_c

[2] R. E. Anderson et al., “Experiences with a transportation information system that uses only GPS and SMS,” in Proc. IEEE ICTD, no. 4, Dec.2010.

[3] D. Risi and M. Teófilo, “MobileDeck: Turning SMS into a rich user experience,” in Proc. 6th MobiSys, no. 33, 2009.

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

[5] J. Chen, L. Subramanian, and E. Brewer, “SMS-based web search for low-end mobile devices,” in Proc. 16th MobiCom, 2010, pp. 125–135.

[6] B. DeRenzi et al., “Improving community health worker performance through automated SMS,” in *Proc. 5th ICTD*, 2012, pp. 25–34.