Volume No:1, Issue No:11 (April-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

Protected Communication of SMS by Using Altered AES and Hash Techniques

P.Anusha
Assistant Professor
Vignan Institute of Information Technology,
Duvvada, Visakhapatnam.

B.S.Vamsi Krishna
Sr. Assistant Professor,
M.V.G.R College of Engineering,
Chintalavalasa, Viziaganaram.

ABSTRACT:

Short Message Service (SMS) has become one among the quickest and powerful communication channels to transmit the data across the world. Sometimes, we have a tendency to send the information like transaction ids, pass code, banking details and personal identity to our friends, members of the family and retail suppliers through the SMS. SMS messages are transmitted as plaintext between mobile user (MS) and also the SMS centre (SMSC), exploitation wireless network. SMS contents are kept within the systems of network operators and might be browse by their personnel which violets user information security. Since, the SMS is distributed as plaintext; therefore network operators will simply access the content of SMS throughout the transmission at SMSC. The ancient SMS service offered by numerous mobile operators surprisingly doesn't offer data security of the message being sent over the network. So as to guard such wind, it's seriously needed to produce finish-to-end secure communication between the users. Now this top needs are accomplished by proposing a protocol known as Cipher-SMS that provides end-to-end security throughout the transmission of SMS over the network. The Cipher-SMS protocol achieved by exploitation of scientific discipline algorithms of AES and MD5.The Cipher-SMS protocol prevents the SMS data from numerous attacks together with SMS revelation, over the air (OTA) modification, replay attack, man-in-the-middle attack, and impersonation attack. Planned SMS primarily 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 regular key cryptography of AES and hash cryptography of MD5 for cellular networks.

KEYWORDS:

SMSC, OTA, AES, MD5.

INTRODUCTION:

Short Message Service (SMS) has become one in every of the fastest and powerful communication channels to transmit the information across the globe. Sometimes, we've an inclination to send the wind like identification, pass code, banking details and private identity to our friends, members of the family and retail suppliers through an SMS. SMS messages or units transmitted as plaintext between mobile users (MS)in the SMS centre (SMSC) and mistreatment wireless networks. SMS content units keep inside the systems of network operators and should be scan by their personnel for his or her personal usage. Since, the SMS is distributed as plaintext, therefore network operators can merely access the content of SMS throughout the transmission at SMSC. the traditional SMS service offered by varied mobile operators astonishingly does not provide data security of the message being sent over the network. therefore on safeguard such wind, it's powerfully required to provide finish-to-end secure communication between finish users. the upper than a necessity is accomplished by proposing a protocol referred to as Cipher-SMS that has end-to-end security throughout the transmission of SMS over the network. The Cipher-SMS protocol achieved by mistreatment science algorithms of AES and MD5.The Cipher-SMS protocol prevents the SMS data from varied attacks along side SMS revelation, over the air (OTA) modification, replay attack, man-in-the-middle attack, and impersonation attack. Planned SMS based totally framework provides a low-bandwidth, reliable, economical and worth effective resolution for SMS Transmission. Cipher-SMS is that the primary protocol completely supported the symmetric key cryptography of AES and hash cryptography of MD5 for cellular networks. simple SMS that has finish-to-end secure communication through SMS between finish users. simple SMS is dead that creates out there the centro-symmetrical bilateral shared key between every MS then ciphering of message takes place using a symmetric key rule.

Volume No:1, Issue No:11 (April-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

The in operation of the protocol is given by considering 2 all completely different eventualities referred to as SMS Sec and PK-SIM protocols. SMS Sec protocol is works supported Java's Wireless transmission API, that provides SMS security. PK-SIM protocol proposes a typical SIM card with any PKI utility. every protocols square measure supported client-server paradigm. In simple SMS protocol, a science secret writing rule AES/MAES is maintained, to provide end-to-end confidentiality to the transmitted SMS inside the network. simple SMS provide SMS security with symmetric key cryptography, this protocol is completely supported symmetric key cryptography. The transmission of symmetric key to the mobile users is efficiently managed by the protocol. Security loses can happens once hacking key transmitted between Mobile Stations. The Cipher-SMS provides end-to-end security throughout the transmission of SMS over the network. The Cipher-SMS protocol achieved by mistreatment science algorithms of AES and MD5.The Cipher-SMS protocol prevents the SMS from varied attacks along side SMS revelation, over the air (OTA) modification, replay attack, man-in-the-middle attack, and impersonation attack.

Planned SMS based totally framework provides a low-bandwidth, reliable, economical and worth effective resolution for SMS Transmission. Cipher-SMS is that the first protocol completely supported the symmetric key cryptography of AES and hash cryptography of MD5 for cellular network. This Cipher-SMS sends lesser vary of transmitted bits, generates less computation overhead, and reduces metric consumption and message modified as compare to existing protocols. This protocol produces lesser communication and computation overheads, utilizes metric efficiently, and reduces message modified throughout authentication than simple SMS (existing) protocols. Here preferred a symmetric key rule of AES with MD5 as a results of these algorithms square measure 1000 times faster than the uneven algorithms and improve the efficiency of the system. Achieved plenty of security than simple SMS by mistreatment AES with MD5 algorithms. No use once hacking the AES key between Mobile Station, as a results of MD5 generates all completely different key ID of each transmission. The Cipher-SMS protocol generates minimum communication and computation overheads as compare to existing.

LITERATURE SURVEY:

1.Encryption based channel coding algorithm for secure SMS

SMS contains a form of advantages and disadvantages for M-Commerce purpose. the advantages are it is straightforward to use, a typical transmission tool among customers, works across all wireless operators, low cost for mobile users, no specific software package needed for installation, permits banks and money establishments to supply period of time data to shoppers and workers and hold on messages is accessed while not a network affiliation. Most vital disadvantage of SMS is that it doesn't supply a secure setting for confidential knowledge throughout transmission and there's no operating procedure to certify the SMS sender. There's a desire for finish to finish SMS secret writing with perfect message transmission so as to supply a secure with error free knowledge transmission for communication. These 2 factors square measure vital for SMS. During this paper, we analysed regarding primarily JCCC and Soft Input coding (SID). We have a tendency to plan a unique theory in theme NTRU Sign rule during this paper. We have a tendency to square measure expect that it will improve this security level speed and supply reliable message at receiver finish.

2. The Implementation of Security Message Protocol for PDA PUSH Service:

In this paper, we have a tendency to propose and implement a service model to transfer messages safely for PDA on CDMA wireless networks and a secure message transfer protocol that considers characteristics of PDA. The planned PUSH service uses SMS (short message service) to attach Associate in nursing offline consumer device with the wired network for electronic communication. Once receiving SMS message, consumer device method the SMS message and creates a knowledge channel through RAS (remote access service), then the information of the server will be pushed to consumer. The enforced securing protocol will give safe information transmission on every communication channels of SMS and information. This protocol will scale back variety of transmissions for exchanging a secure session key by victimisation security present table. As a result, intensity of cryptography will be increased.

Volume No:1, Issue No:11 (April-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

3. High Security Communication Protocol for SMS:

Nowadays, short message service (SMS) is facing with numerous security threats. Thus, the fields of high confidentiality (e.g., mobile E-commerce) need a better level of security 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. Though analysed it by svo logic, this protocol is proved to make sure confidentiality, integrity and non-repudiation of SMS messages.

4. Performance evaluation on end-to-end security architecture for mobile banking system:

The advantage of mobile penetration permits mobile operators to supply worth more service like secured mobile banking, mobile commerce and supply increased security for web banking. Mobile banking is enticing as a result of its a convenient approach to perform banking from anyplace any time, however there are security considerations within the implementation, 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. Performance of the planned model is conferred during this paper.

5. A Secure Information Transmission Scheme with a Secret Key Based on Polar Coding:

In this letter, a new secure information transmission scheme based on polar codes with a pre-shared secret key is proposed. In polar codes, after the channel polarization is induced, good split channels are used to transmit the user message and bad channels are utilized to support the reconstruction of the message by sharing fixed information. If the fixed information in bad channels is secret, an adversary gets difficulty in reconstructing the user message in good channels without knowledge of the fixed information. From this observation, we construct a secure information transmission scheme.

By appending pre-post-processing that imposes a dependency between the transmitted message sub-blocks, the adversary's difficulty can be changed to intractability, since only partial information can be decidable by attackers. A new class of secret key scheme is developed in such a way.

EXISTING SYSTEM:

•Easy SMS that provides finish-to-end secure communication through SMS between end users. Easy SMS is dead that makes accessible the isobilateral shared key between each MS then ciphering of message takes place employing a symmetric key rule. The operating of the protocol is conferred by considering 2 totally different situations square measure SMS Sec and PK-SIM protocols.
•SMS Sec protocol will be accustomed secure associate SMS communication sent by Java's Wireless electronic communication API whereas the PK-SIM protocol proposes a regular SIM card with extra PKI practicality. Each protocols square measure supported client-server paradigm.
•In Easy SMS protocol, a science secret writing rule AES/MAES is maintained to give end-to-end confidentiality to the transmitted SMS within the network.

LIMITATIONS:

•Easy SMS offer SMS security with stellate key cryptography, the prevailing protocol is totally supported stellate key cryptography.
•The transmission of stellate key to the mobile users is expeditiously managed by the protocol.
•Security loses once hacking key transmission between Mobile Station.

PROPOSED SYSTEM:

•The Cipher-SMS provides end-to-end security throughout the transmission of SMS over the network. The Cipher-SMS protocol achieved by cryptanalytic algorithms of AES and MD5.
•The Cipher-SMS protocol prevents the SMS data from numerous attacks as well as SMS revealing, over the air (OTA) modification, replay attack, man-in-the-middle attack, and impersonation attack.

Volume No:1, Issue No:11 (April-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

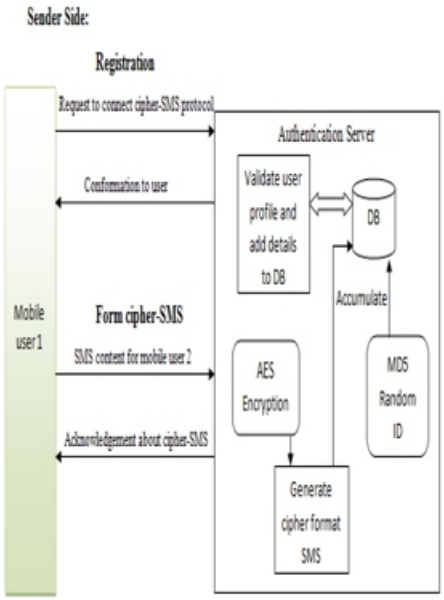
•Proposed SMS protocol primarily based framework provides a low-bandwidth, reliable, economical and value effective answer for SMS Transmission. Cipher-SMS is that the 1st protocol fully supported the bilateral key cryptography of AES and hash cryptography of MD5.

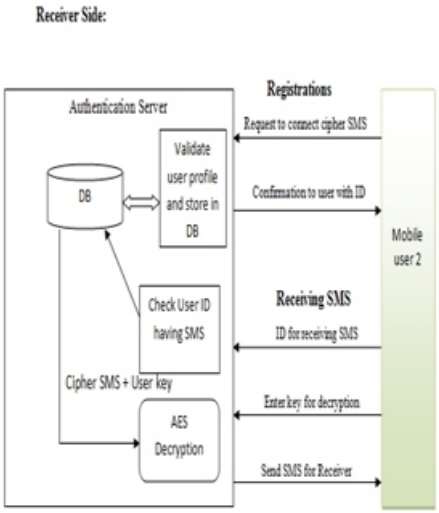
•This Cipher-SMS sends lesser range of transmitted bits, generates less computation overhead, and reduces information measure consumption and message changed as compare to existing protocols.

ADVANTAGES:

•This protocol produces lesser communication and computation overheads, utilizes bandwidth efficiently, and reduces message exchanged during authentication than Easy SMS (existing) protocols.
•Here preferred a symmetric key algorithm of AES with MD5 because these algorithms are 1000 times faster than the asymmetric algorithms and improve the efficiency of the system.
•Achieved more security than Easy SMS by using AES with MD5 algorithms.
•No use when Hacking AES key between Mobile Station, because MD5 generates different key ID of each transmission.

SYSTEM ARCHITECHTURE:

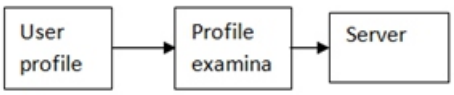




MODULES:

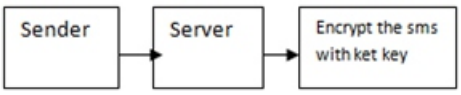
User Profile Module:

The mobile device that receive the user details with some parameters, that recognize the authenticate user. This restricts the non-owner users to see information about the SMS we send. However, any mobile device using this service can get some additional profile examination has to be handled with some unique parameter. Through this function, the mobile device can allow authenticated profile owner to access the data and send secure SMS to others.



SMS Communication:

The Authenticated mobile user can send the SMS with some key to the server. The mobile who wants to send SMS must be registered with server. The mobile sends the SMS with certain key to server. The server can encrypt the original message using AES algorithm and the send SMS to receiver through base station and mobile station.

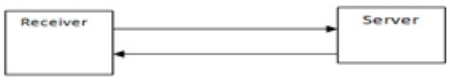


Authentication Server:

The Encrypted message can travel through base station. Receiver receives the message in secure inbox.

Volume No:1, Issue No:11 (April-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

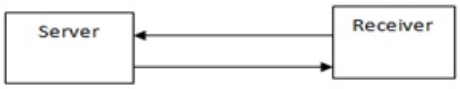
Now the receiver wants to decrypts the message. So receiver requests the key using random number generator from server. Then server generates the random number and sends it to the receiver.



Request random number

Symmetric Key:

Server recognizes the random number from receiver; from this server authenticate the authorized 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.



Send Random Number

RESULTS:

Fig shows the graph for comparison of encryption time for various algorithms against 10-50 milliseconds of simulation time where x-axis shows the simulation time (sec) and y-axis shows the encryption time (ms).

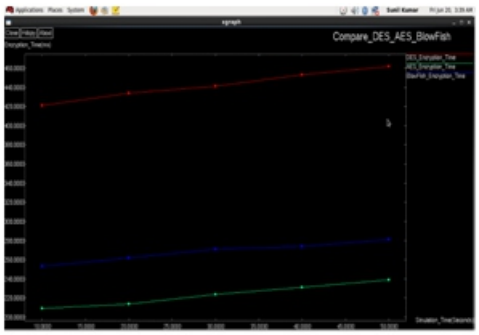


Fig: AES Encryption

Fig shows the graph for comparison of decryption time for various algorithms against 10-50 milliseconds of simulation time where x-axis shows the simulation time (sec) and y-axis shows the decryption time (ms).

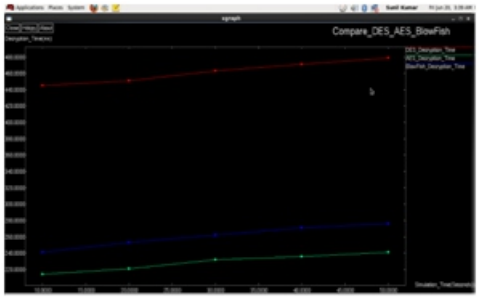


Fig: AES Decryption

Md5:

Secure hash functions actually have various applications. A very common case is verifying the integrity of data. When we send some data, we append a hash of that data. On the receiving end, we re-hash the received data and check that the computed hash equals to that sent. If any of the data has changed then (with overwhelming probability), the computed hash value will no longer match the original. Another case is where we need to authenticate some data, i.e. produce a kind of integrity check that only a party with a given private key could produce. (In this case, the general solution is to combine a hash code with encryption.)

Conclusion:

Easy SMS protocol is with success designed so as to produce end-to-end secure communication through SMS between mobile users. The analysis of the projected protocol shows that the protocol is ready 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:

•Press Release. (2012, Dec. 3). Ericsson Celebrates 20 Years of SMS.

• R. E. Anderson et al., “Experiences with Transportation Information System that Uses Only GPS and SMS,” IEEE ICTD, No. 4, 2010.

Volume No:1, Issue No:11 (April-2016)
ISSN No : 2454-423X (Online)
International Journal of Research in Advanced Computer Science Engineering
A Peer Reviewed Open Access International Journal
www.ijracse.com

• D. Risi, M. Teófilo, "MobileDeck: Turning SMS into a Rich User Experience," 6th MobiSys, No. 33, 2009.

•Kuldeep Yadav, "SMSAssassin: Crowdsourcing Driven Mobile-based System for SMS Spam Filtering," Workshop Hotmobile, 2011, pp. 1-6.

• J. Chen, L. Subramanian, E. Brewer, "SMS-Based Web Search for Low-end Mobile Devices," 16th MobiCom, 2010, pp. 125-135.

•B. DeRenzi, "Improving Community Health Worker Performance through Automated SMS," 5th ICTD, 2012, pp. 25-34.

•Y. Zeng, K. Shin, X. Hu, "Design of SMS Commanded-and-Controlled and P2P-Structured Mobile Botnets," WiSec, 2012, pp. 137-148.

•[K. Hamandi, "Android SMS Botnet: A New Perspective," 10th ACM MobiWac, 2012, pp. 125-129.

• J. Lo, J. Bishop, J. Eloff (2008). SMSSec: An End-to-end Protocol for Secure SMS. Computers & Security, 27(5-6), pp. 154–167.

• H. Rongyu, Z. Guolei, C. Chaowen, X. Hui. (2009). A PK-SIM Card based End-to-end Security Framework for SMS. Com. Standard & Interfaces, 31, pp. 629-641.

• M. Hassinen, "Java based Public Key Infrastructure for SMS Messaging," ICTTA, 2006, pp. 88-93.

• S. Wu, C. Tan, "A High Security Framework for SMS," BMEI, 2009, pp. 1-6.