Volume No:2, Issue No:3 (August-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

Secure Communication of Group SMS

G.Saritha Devi
Student of M.Tech,
Dept of CSE,
Jawaharlal Nehru institute of Technology,
Ibrahimpatnam, Hyderabad, Telangana, India.

V.Jhansi Lakshmi
Associate. Professor,
Dept of CSE,
Jawaharlal Nehru institute of Technology,
Ibrahimpatnam, Hyderabad, Telangana, India.

ABSTRACT:

Short Message Service (SMS) has become one amongst the quickest and powerful communication channels to transmit the data across the worldwide. Sometimes, we have a tendency to send the wind like Arcanum, pass code, banking details and personal identity to our friends, members of the family and repair suppliers through associate SMS. SMS messages are transmitted as plaintext between mobile user (MS) and also the SMS centre (SMSC), exploitation wireless network. SMS contents are keeps within the systems of network operators and might be browse by their personnel. Since, the SMS is distributed as plaintext; therefore network operators will simply access the content of SMS throughout the transmission at SMSC. So as to guard such wind, it's powerfully needed to produce finish-to-end secure communication between end users. The on top of needs is often 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 scientific discipline algorithms of AES, 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 reliable, economical and value effective answer for SMS Transmission. Cipher-SMS is that the 1st protocol fully supported the regular key cryptography of AES.

Keywords : AES, android ADT.

1. Introduction:

Short Message Service (SMS) has become one amongst the quickest and powerful communication channels to transmit the knowledge across the worldwide. 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 centre (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. So as to safeguard such wind, it\'s powerfully needed to supply finish-to-end secure communication between end users. The higher than a necessity is 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 victimisation science algorithms of AES and MD5, The Cipher-SMS protocol prevents the SMS info from varied 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 price effective resolution for SMS Transmission. Cipher-SMS is that the 1st protocol utterly supported the cruciform key cryptography of AES and hash cryptography of MD5 for cellular network. EasySMS that provides finish-to-end secure communication through SMS between end users. EasySMS is dead that makes out there the symmetrical bilateral shared key between 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. SMSSec is accustomed secure AN SMS communication sent by Java's Wireless electronic communication API whereas the PK-SIM protocol proposes a typical SIM card with further PKI practicality. . Each protocols area unit supported client-server paradigm.

In EasySMS protocol, a science secret writing algorithmic program AES is maintained to give end-to-end confidentiality to the transmitted SMS within the network. EasySMS give SMS security with cruciform key cryptography, the present protocol is totally supported cruciform key cryptography. The transmission of cruciform key to the mobile users is with efficiency managed by the protocol. Security loses once hacking key transmission between Mobile Station. The Cipher-SMS provides end-to-end security throughout the transmission of SMS over the network. The Cipher-SMS achieved by victimisation science algorithms of AES. The Cipher-SMS protocol prevents the SMS info from varied 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 reliable, economical and price effective resolution for SMS Transmission. Cipher-SMS is that the 1st protocol utterly supported the cruciform key cryptography of AES. 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 this protocol produces lesser communication and computation overheads, utilizes information measure with efficiency, and reduces message changed throughout authentication than EasySMS (existing) protocols. Here most well-liked a cruciform key algorithmic program of AES. Achieved a lot of security than EasySMS by victimisation AES. The Cipher-SMS protocol generates minimum communication and computation overheads as compare to existing.

2. Literature survey:

a. Encryption based channel coding algorithm for secure SMS:

SMS contains a form of advantages and disadvantages for M-Commerce purpose. the advantages are its 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 AN 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’ve got analyzed regarding primarily JCCC and Soft Input coding (SID). We have a tendency to plan a unique in theory theme NTRU Sign rule during this paper. We have a tendency to square measure expect that it’ll improve this security level speed and supply reliable message at receiver finish.

b. 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 thought RAS (remote access service), then the info of the server will be pushed to consumer. The enforced securing protocol will give safe information transmission on every communicating thought 2 manner 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 . b. High Security Communication Protocol for SMS:Nowadays, short message service (SMS) is faced 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. Through analyzed it by svo logic, this protocol is proved to make sure confidentiality, integrity and non-repudiation of SMS messages.

c. 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 it\'s 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.

d. 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.

3. EXISTING SYSTEM

•EasySMS that provides finish-to-end secure communication through SMS between end users. EasySMS 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 SMSSec and PK-SIM protocols.

•SMSSec 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 EasySMS protocol, a science secret writing rule AES/ MAES is maintained to give end-to-end confidentiality to the transmitted SMS within the network.

4. LIMITATIONS:

•EasySMS 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

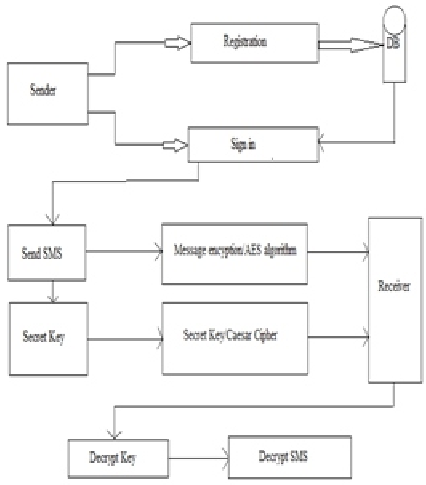
5. PROPOSED SYSTEM:

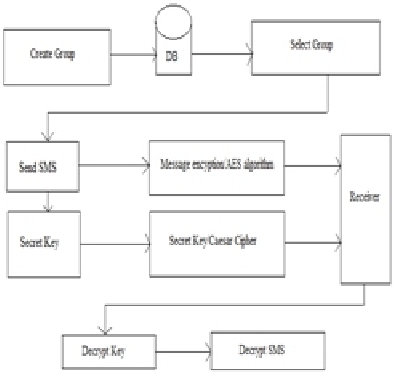
» Without network the Cipher-SMS provides end-to-end security during the transmission of SMS. The Cipher-SMS protocol achieved by using cryptographic algorithms of AES.
» Proposed SMS based framework provides a reliable, efficient and cost effective solution for SMS Transmission.
» This Cipher-SMS sends lesser number of transmitted bits, generates less computation overhead, and message exchanged as compare to existing protocols.
» The Cipher-SMS provide secure inbox on the receiver side and group way communication.

6. ADVANTAGES:

• This protocol produces group communication.
•We no need to depending on cellular network.
•Here preferred a symmetric key algorithm of AES because these algorithms are 1000 times faster than the asymmetric algorithms and improve the efficiency of the system.
•Achieved more security than EasySMS by using AES.
•The Cipher-SMS protocol generates group communication and computation overheads as compare to existing.

SYSTEM ARCHITECTURE:



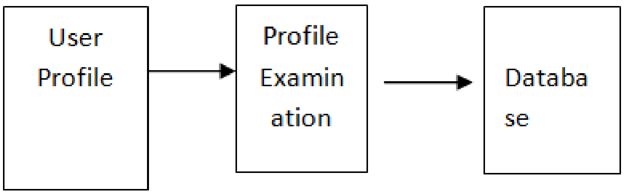


7. MODULES:

- User Profile
- Key Generation
- SMS Communication
- Group Creation

1.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.



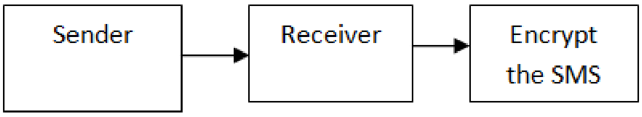
2.Key Generation:

Key generation is the process of generating keys in cryptography. A key is used to encrypt and decrypt whatever data is being encrypted and decrypted. Here, we are using AES algorithm and Caesar cipher for sending and receiving message. User will generate 16 digit secret key with encryption using Caesar cipher.

Sender
Encryption message
Receiver

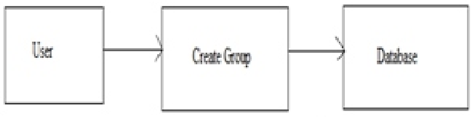
3.SMS Communication:

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 database. The mobile sends the SMS with certain key to receiver. The receiver can encrypt the original message using AES algorithm and the send SMS to receiver through base station and mobile station.



4.Group Creation:

User can create n number of groups. We can be able to create maximum five members for that group. This all group numbers are stored in database. We can send the SMS with encryption using AES algorithm And then receiver can receives the message in secure inbox.



8. Conclusion:

EasySMS 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.

9. References:

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

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

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

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

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

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