SMS ENCRYPTION ON ANDROID MESSAGE APPLICATION

Varsha S. Bari[1],Nileema R. Ghuge[2],Chaitali C. Wagh[3],Sayali R. Sonawane [4],Mr.M.B. Gawali[5]

[1] *Student, Information Technology, Sanjivani College of Engineering Kopargaon, Maharashtra, India*
[1] *Student, Information Technology, Sanjivani College of Engineering Kopargaon, Maharashtra, India*
[1] *Student, Information Technology, Sanjivani College of Engineering Kopargaon , Maharashtra, India*
[1] *Student, Information Technology, Sanjivani College of Engineering Kopargaon , Maharashtra, India*

ABSTRACT

SMS messages are one of the popular ways of communication. Sending of any message is very easy. SMS is one of the easiest way of mobile phone. It is used for sending and receiving message. Sometime we can send and receive our confidential data during transmission of message when user sends any confidential data through message it is very difficult to protect it. also it is widely used in mobile banking. Security is the important thing in this but unluckily SMS does not provide a secure medium. SMS transmission GSM network is also not secure, so there is need to secure SMS by providing encryption process. Encryption is importance during transmission of SMS. There are so many type of encryption algorithms like AES, DES, RC4 are available. In this entire algorithm AES is most widely accepted suitable algorithm. We develop an application which is based on Android platform which useful for the user to encrypt the messages before it is transmitted over the network. The 3D-AES block cipher symmetric cryptography algorithm and used for secured transmission of message. In this system 3D AES block cipher symmetric algorithm is used for providing a secured medium by providing encryption. If message size is more than 256 bits then it required more time and size for sending that message In our system we will implement an SMS application or service which will decreased more time which required during SMS transmission

Keyword : - *Android, 3D-AES, SMS, block cipher, encryption, mobile application Cryptography, confidential data, Symmetric key, Asymmetric key Enciphering, Public key, Secrete key, and decryption.*

1. Introduction

Android is mobile Operating system based on the linux kernel and currently developed by google. Android is popular with technology companies which require ready-made, low cost customisable Operating system for hightech devices. It is the customisable, easy to use Operating system. Mobile phone users desire more secure and private communication in their daily usage of their mobiles. This is especially important in communications of secret nature such as that in military and governmental communication. Securing voice calls is a difficult task as calls may be tabbed in transmission through various means. On the other hand, securing communication through the popularly used means, namely text messages, can be helpful and useful in many cases. We are going to describe a secured text messages communication environment via SMS. For this purpose, we are going to develope a mobile-based application named Short Message Service (SSMS). It encrypts a text message before sending it and decrypts the message in the receiver's side. In this way, the message is unreadable while transmitted even if it is intercepted while transmitting it over the network. The proposed system can send encrypted messages via SMS and allow users to encrypt/decrypt messages for personal usage without sending them. The latter feature is desirable for those who want to ensure the privacy of their own information. SMS employs symmetric-key encryption. The same secret key is used for both encryption and decryption. Therefore, the secret key must be known by the sender and the receiver of the message. Key distribution remains a problem when using symmetric-key encryption, but we found that it is the best solution when considering time complexity, efficiency, and costs. SMS depends on secret key embedding, where the messages secret key is distributed inside the ciphertext after message encryption process. Secret key embedding is used for checking the correctness of a decryption key which is entered by the user. This schema saves time and space as there is no need for a database to store the secret key related to each message.

2. Literature Survey

1] SMS Encryption using 3D-AES Block Cipher on Android Message Application.

Author Name: Suriyani Arrifin et.al

Description:

SMS messages is one of the popular ways of communication. Sending any message is very easy. We can send and receive our confidential data at the time of transmission. During transmission of message through SMS is very difficult to protect it and also it is widely used in mobile banking. Security is the important thing in this but SMS does not provide a secure medium. SMS transmission through GSM network is also not secure, so there is need to secure SMS by providing encryption process. Encryption is important during transmission of SMS. There are so many type of encryption algorithms like AES, DES, RC4 are available. In this entire algorithm AES is most widely suitable algorithm. We develop an application which are based on Android platform which allows the user to encrypt the messages before it is transmitted over the network. The 3D-AES block cipher symmetric cryptography algorithm is used for secured transmission of message. In this system 3D AES block cipher symmetric algorithm is used for providing a secured medium by providing encryption. If message size is more than 256 bits then it required more time and size for sending that message.

2] SMS-A secure SMS messaging protocol for the m-payment systems.

Author Name: M. Toorani and A. A. B. Shirazi.

Description:

In this paper the GSM network with the greatest worldwide number of user that provide security. The short message service (SMS) is one of its superior and well-tried services with a global availability in the GSM networks. The main contribution of this paper is to introduce a new secure application layer protocol, called SSMS, to efficiently embedded the desired security attributes in the SMS messages to be used as a secure bearer in the m-payment systems. SSMS efficiently embeds the confidentiality, integrity, authentication, and non-repudiation in the SMS messages. It also provides an elliptic curve-based public key solution that uses public keys for the secret key establishment of a symmetric encryption and the attributes of public verification and forward secrecy. It efficiently makes the SMS messaging suitable for the m-payment applications where the security is the great concern.

3] SMS encryption for mobile communication.

Author Name: D. Lisonek and M. Drahansky

Description:

This paper deals with an SMS encryption for mobile communication. The SMS transmission in GSM network is not secure, therefore it is desirable to secure SMS by additional encryption. In SMS, there are compared differences in the use of symmetric and asymmetric cryptography for SMS transfer securing. In the next part, there is the description of design and implementation of the application for mobile phones, which encrypts and signs SMS using an asymmetric RSA cipher. At the end, there are described attacks on secured SMS and future extension of the application.

4] Trusted SMS communication on mobile devices.

Author Name: J. P. Albuja and E. V. Carrera

Description:

In this paper author has introduced the higher growth of the Short Message Service (SMS) use has transformed this service in a widespread tool for social and commerce messaging. However, security concerns have been raised as applications become more critical and complex. Thus, this paper introduces an SMS security framework, which allows programmers and users to exchange confidential, non-reputable and digitally signed text messages. This framework can fit in many development scenarios, such as commercial transactions or bureaucratic delegations. In addition, the proposed framework is highly flexible and efficient, since programmers can choose among several encryption algorithms according to the computational power and battery usage of each mobile device.

5] Building secure user-to user messaging in mobile telecommunication networks.

Author Name: Zhao, A. Aggarwal and S. Liu

Description:

In this paper author explained that Short Message Service (SMS) and Multimedia Message Service (MMS) are popularly used and will be more popular in the future. However, the security of SMS(Short message service) and MMS(Multimedia message service) messages is still a problem. There is no end-to-end security (including integrity, confidentiality, authentication, and non- repudiation) in these services. This hinders service providers to provide some services that require communication of high-level security. There have been some solutions proposed for this

issue in literature, but these are not suitable for user-to-user communication. In this paper, we review existing solutions and analyze their weaknesses.

6] Secure SMSPay: secure SMS mobile payment model.

Author Name: H. Harb, H. Farahat, M. Ezz .

Description:

In this paper a secure mobile payment model suitable for transactions that consist of cost, simplicity, security, and performance of transaction, which contain minimum number of cryptography key usages, and less encryption/decryption operations as compared to other models. This model can use for symmetric and asymmetric cryptography. And there is no need of trusted 3rd parties or even PKI complexity. Now a days it is based on SMS as a transport channel which provides the capability to send transactions to payer not to payee; as usually done in most current payment transaction models. The payer receives a secured SMS message waiting his/her confirmation that is yes or no. Each things in the payment system payer/payee trusts only his/her bank respectively, so the transaction will always go through trusted nodes. The payer/payee can also use any bank payment instrument like credit card, debit card, or even current account without revealing confidential data during the payment. This model can be used for any payment application e.g. e-check, money transfer, e-commerce, and even normal EFTPOS transactions with leverage infrastructure supporting the above mentioned payment applications.

7] Mobile sms banking security using elliptic curve Cryptosystem.

Author Name: R. Soram

Description:

In this paper Mobile devices have many differences in their capabilities, computational powers and security requirements. Mobile devices can be used as the enabling technology for accessing Internet based services, as well as for personal communication needs in networking environments. Mobile services are spread throughout the wireless network and are one of the crucial components needed for various applications and services. However, the security of mobile communication has topped the list of concerns for mobile phone users. Confidentiality, Authentication, Integrity and Non-repudiation are required security services for mobile communication. Currently available network security mechanisms are inadequate; hence there is a greater demand to provide a more flexible, reconfigurable, and scalable security mechanism. This project provides effective security solution using Public key cryptography. The implementation of this project is divided into two parts first, design of API for ECC (Elliptic Curve Cryptography) which generates shared secret key required for secure communication and secondly, a web service is created which distributes this key to validate mobile user.

8] A proposal for enhancing the security system of short message services in GSM.

Author Name: M. A. Hossain, S. Jahan, M. M. Hussain, M.R. Amin, and S.H. S Newaz

Description:

In this paper author introduced, Short message service will play a very important role in the future business areas which is popularly known as m-commerce, mobile banking etc. In future commerce, SMS could make a mobile device in a business tool as it has the availability and the effectiveness. SMS is not free from the eavesdropping, but security is the main thing for any business company such as banks who will provide these mobile banking. Now a days there is no such scheme which can give the complete SMS security. In this paper, we have proposed a security scheme for improving the SMS security. At first plaintext of SMS would be made as cipher text with the help of GSM encryption technology, then this cipher text would be digitally signed .It can be signed with the help of public key signature. These have to be made compatible to existing infrastructure of GSM security. The proposed system will give total authenticity, data integrity, confidentiality, authorization and non-repudiation which are the most essential and common issues in m-commerce or mobile banking and in securing any messaging.

9]Secure asynchronous communication for mobile devices.

Author Name: P. H. Kuat, J. L. Lo and J. Bishopin

Description:

This paper As Short Message Service is now widely use as business tool, security of sms has become a major thing for any business organizations and customers. There is strong need for an end to end SMS Encryption to provide a secure medium for communication. This paper evaluates RSA, ELGamal and Elliptic curve encryption techniques using random SMS messages of various sizes for measure their encryption and decryption time. The results are presented to show the effectiveness of each algorithm and to choose the most suitable and good algorithm for SMS encryption.

Conclusion from Literature Survey:

From the given survey we found that there are so many encryption and decryption algorithm are available. Among all these algorithm we choose 3D-AES Algorithm.3-AES Algorithm is most secure and require less time for sending

the message. If the message size is more than 256 bits then it required more time and space for sending and receiving message. Because of all these problems we select 3D-AES Algorithm

3. Problem Statement

Now a days many people wants to connected with each other, for this purpose they are using many applications like messaging. But we can see that SMS transmission is not that much secure in the environment. To avoiding this kind of problems we are going to developing an Android Application, that will secure the SMS transmission.
In sms transmission service sends the text between cell phones. It contain sender and receiver. The SMS is work on the other computing devices such as laptops,tablet PC's as long as they can accept SIM card. It is needed because SMS service needs sms center client which is built on the SIM card. The BTS(Base Transciver Station)nis used for communication between user and network. MSC(Mobile Switching center) is used for routing the calls.SMSC (SMS Center)is act as temporary storage for SMS.

5. System Framework

5.1 System architecture

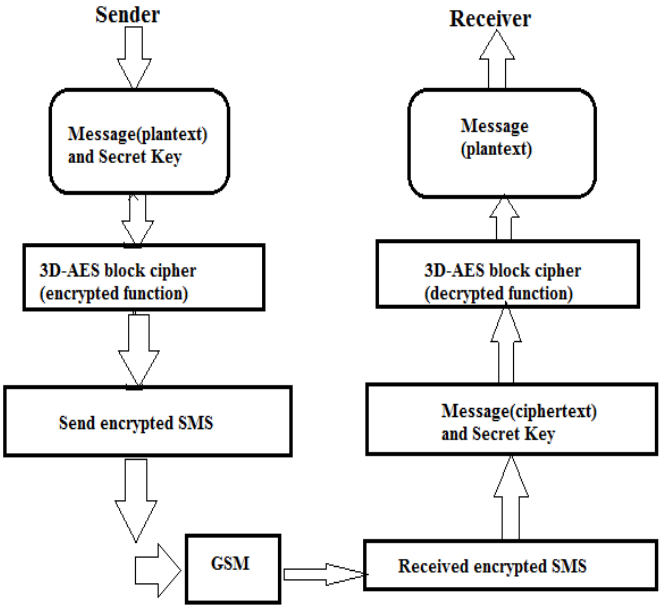

Fig: SMS Encryption

Fig -1: System Architecture

5.1.1 Sender:

This module is for sending message to the Receiver.

5.1.2 Encrypter:

In SMS Encryption it contain sender and receiver. the sender sends the messages which is called plaintext. Using 3D-AES block cipher algorithm the SMS is encrypted. Send this encrypted message and secrete key to the receiver through GSM .GSM is used for routing the calls etc. Receiver received this encrypted message and the secrete key. Decrypt this message. Receiver receive the plaintext message.

5.1.3 Decrypter:

SMS encryption is part of the Global System for mobile communication. We can sent any message via SMS. But this message is not directly delivered to it's destination. But this message is stored in SMSC(SMS Center) after passing through a mobile switching center which is use for message routing. The information provided by Home Location Register(HLR) and Visitor Location Register(VLR).The SMS Encryption contain three steps. It is encrypted in first step, digitally signed in second step and sent in last step.

6. CONCLUSIONS

SMS is a simple, straightforward and easy to use. where access control plays an important role. Thus, our application can be used to authenticate the sender of message. It is possible to detect if message is corrupted during transmission. The most important is the security of the encrypted data against various attacks. Hence this application can be used for secure transfer of data without any corrupted data segment.

7. REFERENCES

1. Suriyani Arrifin et.al ,"SMS Encryption using 3D-AES Block Cipher on Android Message Application." 2013 IEEE.
2. M. Toorani and A. A. B. Shirazi ,"SMS-A secure SMS messaging protocol for the m-payment systems.",March 2013.
3. D. Lisonek and M. Drahansky,"SMS encryption for mobile communication."
4. J. P. Albuja and E. V. Carrera, Trusted SMS communication on mobile devices.
5. Zhao, A. Aggarwal and S. Liu, Building secure user-to user messaging in mobile telecommunication networks.
6. H. Harb, H. Farahat, M. Ezz,"Secure SMSPay: secure SMS mobile payment model.",March 2013.
7. R. Soram ," Mobile sms banking security using elliptic curve Cryptosystem."
8. M. A. Hossain, S. Jahan, M. M. Hussain, M.R. Amin, and S.H. S Newaz, A proposal for enhancing the security system of short message services in GSM.
9. P. H. Kuat, J. L. Lo and J. Bishopin s, Secure asynchronous communication for mobile devices.