ISSN: 2321-7782 (Online)

Volume 2, Issue 11, November 2014

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Secured Mobile Messaging for Android application

Namrata A. Kale[1]
Department of Computer Engineering
Vishwabharati Academy' College of Engineering
Ahmednagar, India

Prof. S. B. Natikar[2]
Department of Computer Engineering
Vishwabharati Academy' College of Engineering
Ahmednagar, India

S.M. Karande[3]
Department of Computer Engineering
Vishwabharati Academy' College of Engineering
Ahmednagar, India

Abstract: Today the age of information technology has transformed the ways we communicate with each other. We send emails, send SMS, send message using social networking sites and many more. The uses of computers, smart phones and clouds have become an integral part of our life for sharing information with each other. Thus introduction of all these means have also given rise to misuse of information by third party which can steal our private information. Thus we are thinking of using cryptography for securing our information. Today there are many cryptographic algorithms available for securing data but those are common from AES to RSA. So we are thinking of enhancing the security by using an advanced version of AES called as 3D-AES which generates a symmetric key by shuffling the original key array three times and making the key better each time it is shuffled. Thus the final output key will be more strong then a normal AES key. It will help secure the data more accurately than the normal one. The studies should reflect a lower encryption time and more security then the normal one. The other technique is used PGP for encryption and Compress the encrypted message to reduce its length, using Shannon fano algorithm technique.

Keywords: 3D-AES; Encryption; Block cipher; Security; Compression; Message

I. Introduction

SMS stands for Short Message Service. It is a technology that enables the sending and receiving of messages between mobile phones. Adding text messaging functionality to mobile devices began in the early 1980s. The first action plan of the CEPT Group GSM was approved in December 1982, requesting that, "The services and facilities offered in the public switched telephone networks and public data networks, should be available in the mobile system." This plan included the exchange of text messages either directly between mobile stations, or transmitted via message handling systems in use at that time. The SMS concept was developed in the Franco-German GSM cooperation in 1984 by Friedhelm Hillebrand and Bernard Ghillebaert. The GSM is optimized for telephony, since this was identified as its main application. The key idea for SMS was to use this telephone-optimized system, and to transport messages on the signaling paths needed to control the telephone traffic during periods when no signalling traffic existed. In this way, unused resources in the system could be used to transport messages at minimal cost. However, it was compulsory to limit the length of the messages to 128 bytes (later improved to 160 seven-bit characters) so that the messages could fit into the existing signaling formats. SMS could be applied in every mobile station by updating its software. Hence, a large base of SMS capable terminals and networks existed when people began to use SMS. SMS first performed in Europe in 1992. Later it was ported to wireless technologies like CDMA and TDMA. The GSM and SMS standards were originally developed by ETSI. ETSI is the abbreviation for European Telecommunications Standards Institute.[1] Now the 3GPP (Third Generation Partnership Project) is responsible for the development and maintenance of the GSM and SMS standards. The rapid development in mobile communication has transformed SMS as common tool for business and public messaging. SMS services are growing day by day. With SMS, people can easily share personal and official messages in a cost effective way. SMS enables the transmission of up to 1120 bits alphanumeric messages between mobile phones and external systems. It uses SMS center (SMS-C) for its routing operation in a network and can be transmitted into another network through the SMS gateway.[2] SMS usage is weak with security concerns, such as eavesdropping, interception and modification. SMS messages are transmitted as plaintext between the mobile stations and the SMS center using the wireless network. SMS content are stored in the systems of the network operators and can easily be read by their personnel. The A5 algorithm, which is the GSM standard for encrypting transmitted information, can easily be compromised. Therefore, there is a need to provide an additional encryption on the transmitted messages. As suggested by the name Short Message Service, the data that can be held by an SMS message is very limited. One SMS message can contain at most 140 bytes (1120 bits) of data, so one SMS message can contain up to:

- » 160 characters if 7-bit character encoding is used.
- » 70 characters if 16-bit Unicode UCS2 (2-byte Universal Character Set) character encoding is used.

SMS text messaging supports languages internationally. It works fine with all languages supported by Unicode, including Arabic, Chinese, Japanese and Korean. SMS is a communication service standardized in the GSM mobile communication systems; it can be sent and received simultaneously with GSM voice, data and fax calls [3]. This is possible because whereas voice, data and fax calls take over a dedicated radio channel for the duration of the call, short messages travel over and above the radio channel using the signaling path. Using communications protocols such as Short Message Peer-to-Peer (SMPP) allow the interchange of short text messages between mobile telephone devices as shown in Fig. 1 that describe traveling of SMS between parties.

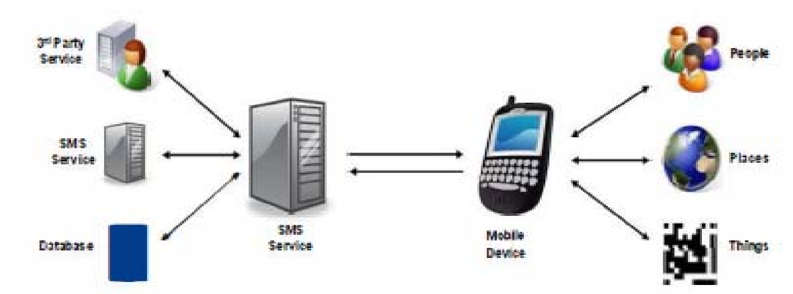

Fig.1 Basic traveling of SMS

SMS messages do not require the mobile phone to be active and within range, as they will be held for a number of days until the phone is active and within range. SMS are transmitted within the same cell or to anyone with roaming skill. The SMS is a store and forward service, and is not sent directly but delivered via an SMS Center (SMSC). SMSC is a network element in the mobile telephone network, in which SMS is stored until the destination device becomes available. Each mobile telephone network that supports SMS has one or more messaging centers to handle and manage the short messages.

II. Short Message Service Architecture

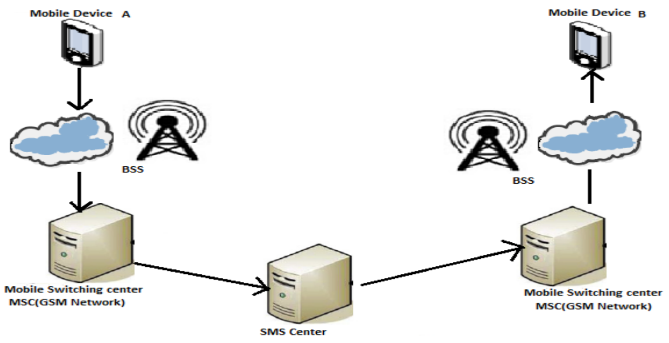

Fig.2 GSM short message service network architecture

The network architecture of short message service in GSM is illustrated in Fig 2. In this architecture, the short message is first delivered from the Mobile Device A to a short message service center (SM-SC) through the base station system (BSS), the mobile switching center (MSC). The SM-SC then forwards the message to the GSM network through a specific GSM MSC called the short message service gateway MSC (SMS GMSC). The SM-SC may connect to some GSM networks and to some SMS GMSCs in a GSM network. Following the GSM roaming protocol, the SMS GMSC locates the current MSC of the message receiver and forwards the message to that MSC. The MSC then broadcasts the message through the BSS to the destination Mobile Device A.

III. SMS Security

a) SMS Security: What is needed?

- » Authentication: Confirm true identities between sender and receiver, and avoid impersonation attack from illegal intruders.
- » Confidentiality: Ensure that decrypted messages are accessible only to those authorized senders and receivers.
- » Integrity: Ensure that receivers can check out whether the message has been modified, and prevent tampered messages.

SMS travels as plain text and privacy of the SMS contents cannot be guaranteed, not only over the air, but also when such messages are stored on the handset. The contents of SMS messages are visible to the network operator's systems and personnel. The demand for active SMS based services can only be satisfied when a solution that addresses end-to-end security issues of SMS technology is available, where primary security parameters of authentication, confidentiality, integrity and non-repudiation are fulfilled. Authentication is concerned with only specific users with specific combination of device, application, memory card, and SIM card that are allowed to access corporate data. This way the users or unauthorized persons cannot change any part of the combination to obtain access to sensitive data. Confidentiality is about ensuring that only the sender and intended recipient of a message can read its content. Integrity is concerned with ensuring that the content of the messages and transactions not being altered, whether accidentally or maliciously. Non repudiation is about providing mechanisms to guarantee that a party involved in a transaction cannot falsely claim later that he/ she did not participate in that transaction. An end-to-end key based encryption technology for SMS plugs the gaps in transit security of SMS. Authentication added for local SMS security access together with encryption, addresses the confidentiality issue of SMS technology. Added features of message integrity and digital signing of SMS address integrity and Non Repudiation for SMS technology.

b) SMS Security Threats

Understanding the basics of SMS security opens the door to preventing some common security threats in SMS usage: [3]

- » Man-in-middle Attack: This is the network that authenticates users. The user does not authenticate network so the attacker can use a false BTS with the same mobile network code as the subscriber's authentic network to impersonate himself and perform a man-in-the-middle attack.
- » Replay Attack: The attacker can misuse the previously exchanged messages between the subscriber and network in order to perform the replay attacks.
- » Message Disclosure: Since encryption is not applied to short message transmission by default, messages could be intercepted and snooped during transmission. In addition, SMS messages are stored as plain text by the SMSC before they are successfully delivered to the intended recipient. These messages could be viewed by users in the SMSC who have access to the messaging system.

- Spamming: While using SMS as a legitimate marketing channel, many people have had the inconvenience of receiving SMS spam. The availability of bulk SMS broadcasting utilities makes it easy for virtually everyone to send out mass SMS messages.
- Denial of Service (DoS) Attacks: DoS attacks are made possible by sending repeated messages to a target mobile phone, making the victim's mobile phone inaccessible.
- SMS Phone Crashes: Some vulnerable mobile phones may crash if they receive a particular type of malformed short message. Once a malformed message is received, the infected phone becomes inoperable.
- SMS Viruses: There have been no reports of viruses being attached to short messages, but as mobile phones are getting more powerful and programmable; the potential of viruses being spread through SMS is becoming greater.
- SMS Phishing: SMS phishing is a combination of SMS and phishing. Similar to an Internet phishing attack using email, attackers are attempting to fool mobile phone users with bogus text messages. When users are taken in by a bogus text message, they may connect to a website provided in the SMS message, and be tricked into download a malware application into their mobile phones.

IV. THE CHNIQUES FOR SECURING SMS

All the fancy encryption algorithm that we have talked about earlier are mostly used for two different types of encryption:

- Symmetric key algorithms use related or identical encryption keys for both encryption and decryption.
- Asymmetric key algorithms use different keys for encryption and decryption—this is usually referred to as Public-key Cryptography.
- Symmetric key encryption

In Fig. 3 Alice puts her secret message in a box, and locks the box using a padlock to which she has a key. She then sends the box to Bob through even mail. When Bob receives the box, he uses an identical copy of Alice’s key (which he has somehow obtained previously, maybe by a face-to-face meeting) to open the box, and read the message. Bob can then use the same padlock to send his secret reply.

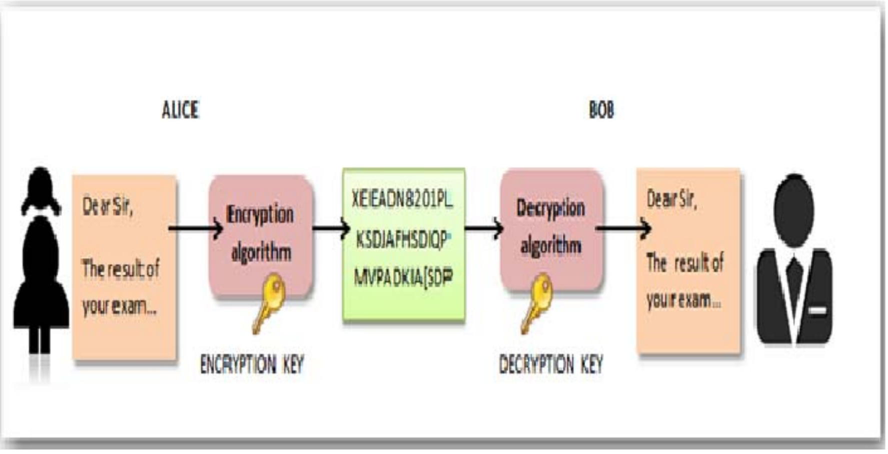

Fig 3. Symmetric Key Encryption

Symmetric-key algorithms can be divided into stream ciphers and block ciphers—stream ciphers encrypt the bits of the message one at a time, and block ciphers take a number of bits, often in blocks of 64 bits at a time, and encrypt them as a single unit. There’s a lot of different algorithms you can choose from—the more popular and well-respected symmetric algorithms include Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, RC4, TDES, and IDEA.

Asymmetric Key Encryption

In an asymmetric key system Fig .4, Bob and Alice have separate padlocks, instead of the single padlock with multiple keys from the symmetric example. Note: this is, of course, a greatly oversimplified example of how it really works, which is much more complicated, but you'll get the common idea. First, Alice asks Bob to send his open padlock to her through regular mail, keeping his key to himself. When Alice receives it she uses it to lock a box containing her message, and sends the locked box to Bob. Bob can then unlock the box with his key and read the message from Alice. To reply, Bob must similarly get Alice's open padlock to lock the box before sending it back to her.

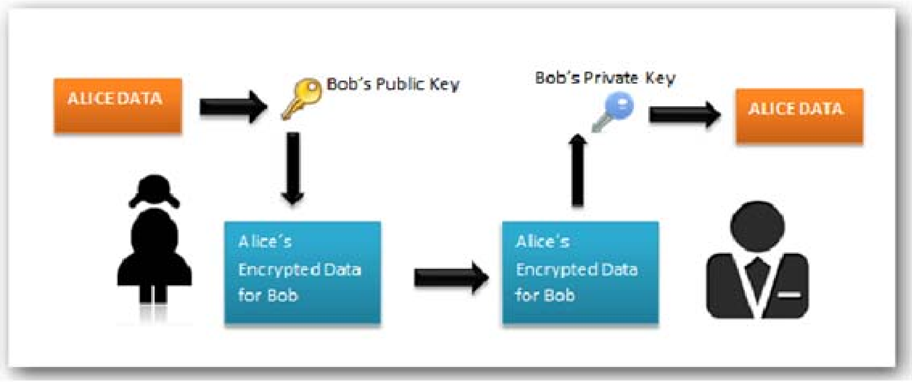
ALICE DATA
Bob's Public Key
Bob's Private Key
ALICE DATA
Alice's Encrypted Data for Bob
Alice's Encrypted Data for Bob

Fig. 4. Asymmetric Key Encryption

The serious advantage in an asymmetric key system is that Bob and Alice never need to send a copy of their keys to each other. This prevents a third party (perhaps, in the example, a corrupt postal worker) from copying a key while it is in transit, allowing said third party to spy on all future messages sent between Alice and Bob. In addition, if Bob were careless and allowed someone else to copy his key, Alice's messages to Bob would be compromised, but Alice's messages to other people would remain secret, since the other people would be providing different padlocks for Alice to use. Asymmetric encryption uses different keys for encryption and decryption. The message recipient creates a private key and a public key. The public key is distributed among the message senders and they use the public key to encrypt the message. The recipient uses their private key any encrypted messages that have been encrypted using the recipient's public key.

V. Proposed System

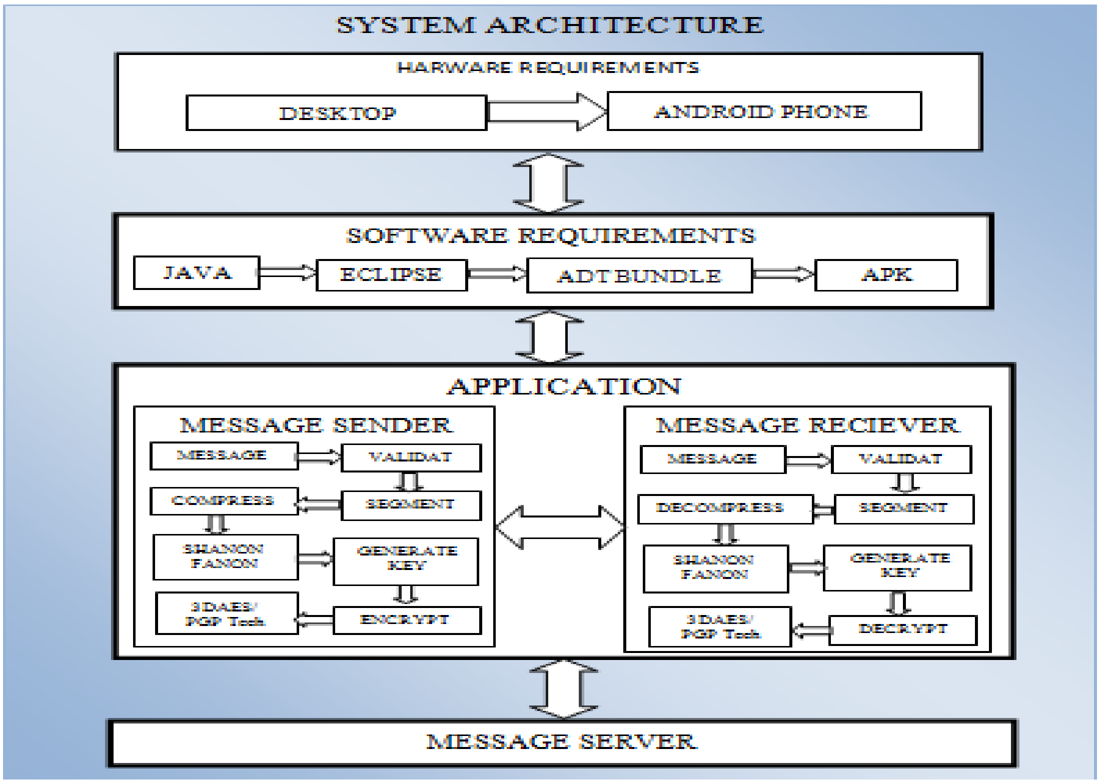

Fig 5. Proposed System 3D-AES/PGP Architechture

a) 3D-AES Block Cipher

The 3D-AES block cipher [5] is based on the AES block cipher [6][7] which is a key-alternating block cipher, composed of rotation key function, minimum 3 iterations of round function and key mixing operations. The round function consists of nonlinear substitution function, permutation function and transposition function. A block diagram of the 3D-AES block cipher is given in Fig. 2 in the form of 4 x 16 bytes. The original message is called the plaintext, denoted P_i, where $i = \{0, 1, 2, 3\}$. The unreadable form is called the ciphertext, denoted by C_i, where $i = \{0, 1, 2, 3\}$. The secret master key is denoted by K. The transformation of P into C is called encryption and the reverse process is called decryption. The P, as it goes through each round of the cipher, is referred to as the cipher state, denoted as F. Note that, the output cipher state, F of the key mixing layer of round r_1 forms the input cipher state to the next round r. The 3D-AES block cipher is improved confusion performance [10] of round transformation.

A detailed description of all the layers of 3D-AES block cipher follows:

- » $P^i_{D^n}$ is a plaintext for ith slice at nth cube.
- » $C^i_{D^n}$ is a ciphertext for ith slice at nth cube.
- » Q is a rotation key .
- » D^n_Q is the output of nth cube from arranging function at rotation key Q.
- » E^i is an encryption function for ith slice.

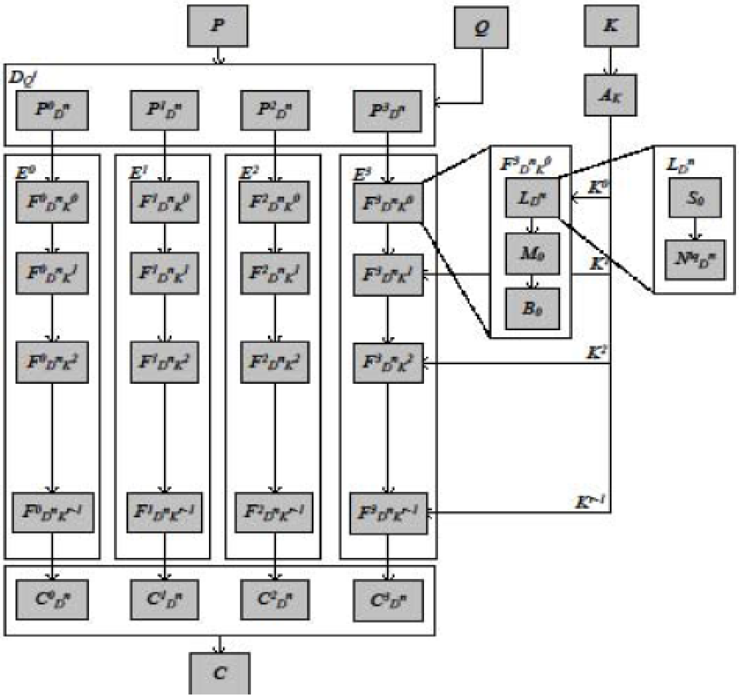

Fig.6 The structure of 3D-AES block cipher

- » $F^i_{D^n K^r}$ is a output block of encryption function for ith slice at cipher state for nth cube in round r.
- » K^r is the sub key used in round r.
- » A_K is key scheduling function.
- » $L^i_{D^n}$ is a output block of linear transformation function for ith slice at Q rotation key at nth cube.
- » S_i is a nonlinear transformation of the ith slice at round function .

» $N_{D^n}^{iq}$ is a rotation function at arranging function of i^{th} slice and q degree at n^{th} cube.

» M_i is a linear transformation of the i^{th} slice at round function.

» B_i is a XOR operation.

The 3D-AES block cipher identified the encryption and decryption functions. When r = 3, the output cipher state is the ciphertext. The third round of the 3D-AES block cipher operates on plaintext size of 16 x 4 bytes to produce an output ciphertext 64 bytes. The secret key size required by the 3D-AES block cipher is 16 bytes. All the operations in the 3D-AES block cipher are performed in the finite field of order 2^8, denoted by $GF(2^8)$.This immune-inspired block cipher adopted amino acid sequences model that can be rotate with a different angle. However for the purpose of evaluation and testing the implementation of the 3D-AES block cipher, every *Slice* of the *Cube* module will be rotate at *3D-SliceRotate* module implementation in four types of angel and clockwise rotation only, which is denoted as $N_{D^n}^{iq}$. The q degree is based on the rotation angel for every i^{th} *Slice* where i = {1, 2, 3, 4} and q = {0, 1, 2, 3}. There is no rotation slice for the first slice, second will be rotate in 900, third slice will be rotate in 1800 and fourth slice will be rotate in 270^0.

b) PGP(Pretty Good Privacy)

Pretty Good Privacy (PGP) is a data encryption and decryption computer program that provides cryptographic privacy and authentication for data communication. PGP is often used for signing, encrypting, and decrypting texts, e-mails, files, directories, and whole disk partitions and to increase the security of e-mail communications. It was created by Phil Zimmermann in 1991. Encryption: PGP combines some of the best features of both conservative and public key cryptography. PGP is a hybrid cryptosystem. When a user encrypts plaintext with PGP, PGP first compresses the plaintext. Data compression saves transmission time and disk space and, more importantly, strengthens cryptographic security. PGP then creates a session key as shown in Fig. 7 which is a one-time-only secret key. This key is a random number generated from the random movements of your mouse and the keystrokes you type. This session key works with a very secure, fast conventional encryption algorithm to encrypt the plaintext; the result is ciphertext. Once the data is encrypted, the session key is then encrypted to the recipient's public key. This public key-encrypted session key is transmitted along with the ciphertext to the recipient.

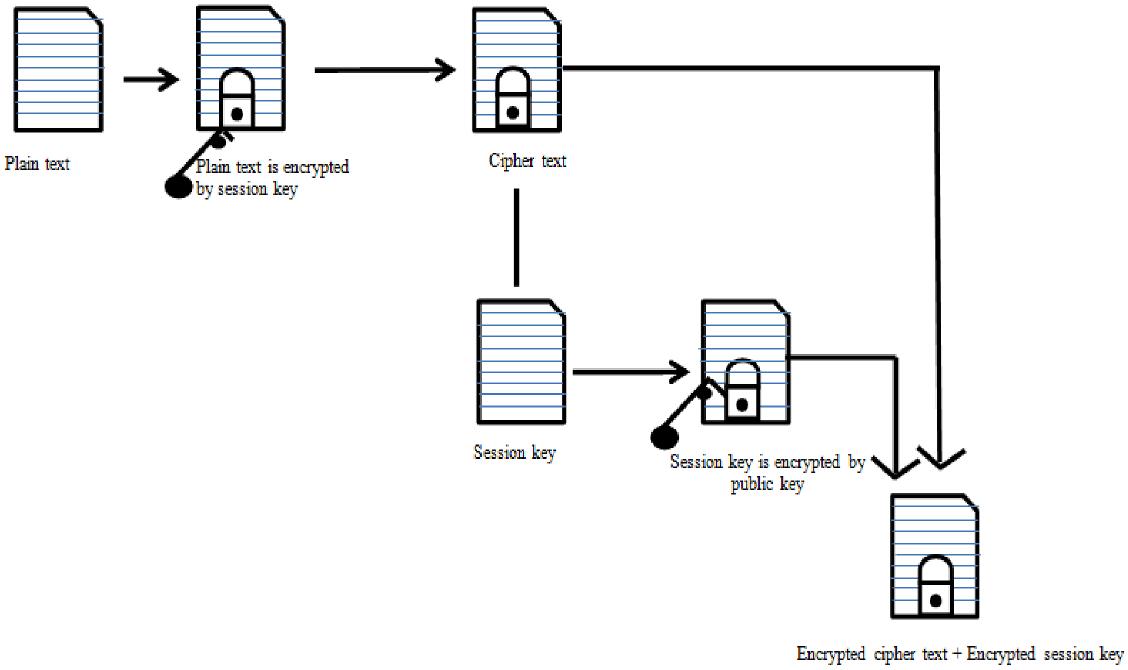
Plain text
Plain text is encrypted by session key
Cipher text
Session key
Session key is encrypted by public key
Encrypted cipher text + Encrypted session key

Fig. 7 Encryption using PGP technique

Decryption: Decryption works in the reverse as shown in fig. 8. The recipient’s copy of PGP uses his private key to decrypt the temporary session key, which PGP then uses to decrypt the conventionally-encrypted ciphertext.

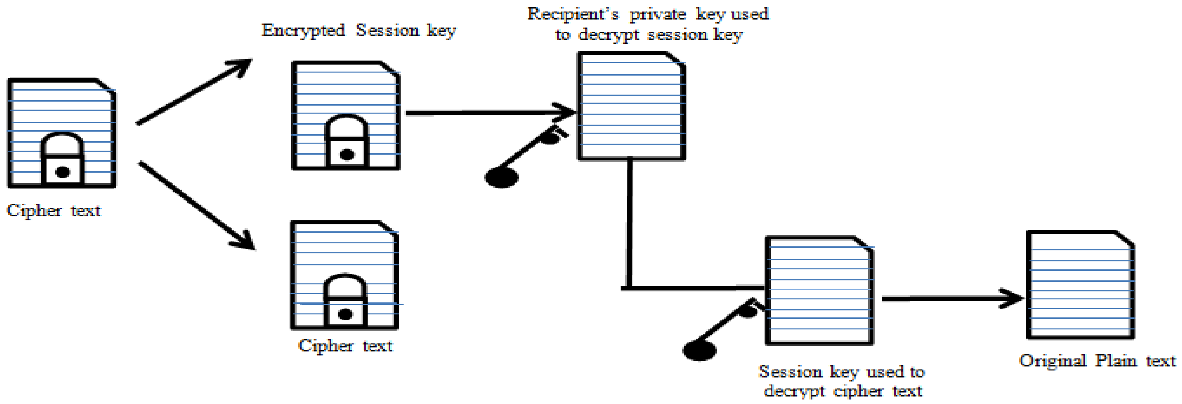
Encrypted Session key
Recipient's private key used to decrypt session key
Cipher text
Cipher text
Session key used to decrypt cipher text
Original Plain text

Fig. 8 Decryption using PGP technique

VI. Compression

The second step is compression. The encrypt message usually gets larger than the original message leading to excessive charge in sending SMS encrypted message. Therefore data compression will be used on the encrypted message; this will reduce it bit size. Thereby reducing the additional cost incurred in sending SMS encrypted message.[4] Compression is the art of representing the information in a compact form rather than its original or uncompressed form. When data compression is used in a data transmission application, speed is primary goal. Speed of transmission depends upon the number of bits sent. Compression can be classified as either lossy or lossless. Lossless compression techniques reconstruct the original data from the compressed file without any loss of data. [6] Various lossless data compression algorithm have been proposed and used. Some of the main techniques in use are the Huffman Coding, Run Length encoding, Arithmetic Encoding and Dictionary Based Encoding. For compressed the text message we will go with Shannon fano algorithm. This is loss less compression algorithm. This is the variant of static Huffman coding algorithm.[6] Static Huffman algorithm calculates the frequencies first and then generates the common tree for both the compression and decompression processes. Details of this tree should be saved or transferred with the compressed file.

VII. Conclusion

The proposed technique combines the encryption and compression process. It encrypts the SMS using 3D-AES algorithm or PGP , then encrypted SMS compressed using a lossless algorithm, Shannon Fano algorithm. The advantage of this technique is achieving the protection criteria such as confidentiality and authenticity between two communication parties and at the same time decreasing the message lengths. This application is running on smartphones and does not require any other encryption device. Users can exchange the sensitive information via SMS through the proposed technique that prevents from attackers.

References

1. A. Medani, A Gani, O.Zakaria, A.A. Zaidan "Review of mobile short message service security issues and techniques towords the solution", Scientific Reaserch and Essays voI.6(6),pp. I 147-1 165,18 March, 201 IJ. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed,vol. 2. Oxford: Clarendon,1892,pp.68-73.

2. Tarek M Mahmoud, Bahgat A. Abdel-Iatef, Awny A Ahmed & Ahmed M Mahfouz, "Hybrid compresion encryption techniques for securing SMS", International Journal of Computer Science and Security(UCSS),Volume(3):issue(6)K Elissa,"Title of paper if known," unpublished.

3. NJ Croft and M.S Olivier, "Using an approximated one-time pad to secure short messaging service(SMS)", Information and Computer Security Architecture(ICSA) Research Group.

4. S.R. Koituwakku,U,S. Amrasinghe, "Compression of lossless data compression algorithm for text data". India journal of computer science and engineering VOL INo 4 I 6-425.

5. S.Ariffin, R.Mahmod,A. Jaafar and M.R.K. Arffin, "Byte Permutations in Block cipher Based on Immune Systems", International Conference on Software Technology and Engineering 3rd(ICSTE 2011), ASME Press,New York,NY,2011.

6. NIST, "Fips197: Advanced Encryption Standard(AES)", FIPS PUB 197 Federal Information Processing Standard Publication 197,Technical report, National Institue of Standard and Technology,2001.

7. J.Daemen, V. Rijmen, V. ,"The Design of Rijndael, AES-The Advanced Encryption Standard",Springer-Verlag.2002.