MSC : Mobile Secure Communication Using SMS in Network Security : A Survey

Punam V. Maitri, Rekha V. Sarawade, Mayuri P. Patil, Sarika T. Deokate
Indira College of Engineering and Management, Department of Computer Engineering, Pune, India.

Abstract

The SMS based Mobile communications require high security in the network. Information as well as SMS security is important and challenging part for mobile communication. Some ethical hackers or attackers access the illegally sensitive data or messages. For solve this important issue and problems. Many users' uses the various algorithm and techniques for provide security to data and SMS in communication networks. Some users use encryption as well as decryption algorithms. Many people's implement own algorithm for SMS or data security in the communication network. The algorithms like AES, DES, Triple DES used by many authors for encrypt or decrypt SMS for communication. In the Wireless communication network for reducing processing time i.e. encryption or decryption time, developers uses various available algorithms. New algorithms implemented using AODV Protocols in wireless communication networks. In this paper we have propose the survey of SMS encryption as well as decryption techniques, algorithms, models use in communication network and security. The concept of Server key secure and Sender key secure messaging for SMS security.

Keywords: *Android, Network Security, Communication network, Advanced Encryption Standard (AES), Data Encryption Standard (DES), RSA key, public key infrastructure (PKI).*

1. INTRODUCTION

The network security is major problem in SMS based wireless communication. SMS or information sending from sender to receiver or source to destination for communication. At that time many illegal users access the sensitive data from SMS

And information communication. Some ethical hackers hack and access the data illegally from the network. So this is a one important security issue for communication network. For solve these problems users' uses the techniques and algorithms for security of SMS and information.SMS messaging uses the different keys for communication. Private Key, public key is used for secure and reliable message. [4] Many organization uses the SMS tools for communication. So they require strong security about SMS using Encryption as well as decryption techniques. [5]

Information or SMS security is important problem in network secure communication. Encryption and decryption algorithms uses by many authors for performance evaluation and security. Some algorithms gives better performance but require more time for encryption. [6] The users who uses the AES algorithms. They modified and doing changes in AES algorithm for reducing complexity in the

Encryption process. [7] In wireless communication SMS or data packets sending from source node to destination. So, latency require for reach SMS to the receiver is less. The encrypted packets should be reaching within seconds to receiver side. Here a less chances to cracker access information in the network. [8] The world of Android applications android users uses different types of applications for messaging. Only for message security and messages encryption developer uses AES algorithm for Android application security. [9] In wireless communication network SMS or information should be sending using mobile nodes. One message or data packet should be sending to multiple receivers or single receiver. Techniques of SMS sending using tools or applications are different in wireless communication. Encrypted or decrypted data should be sending and receiving using different

techniques. [10].In this paper we have doing survey for SMS encryption techniques, algorithms and performance analysis survey for encryption and decryption previous algorithms in communication networks. Detail survey part of this paper is present in next section of Survey of this paper.

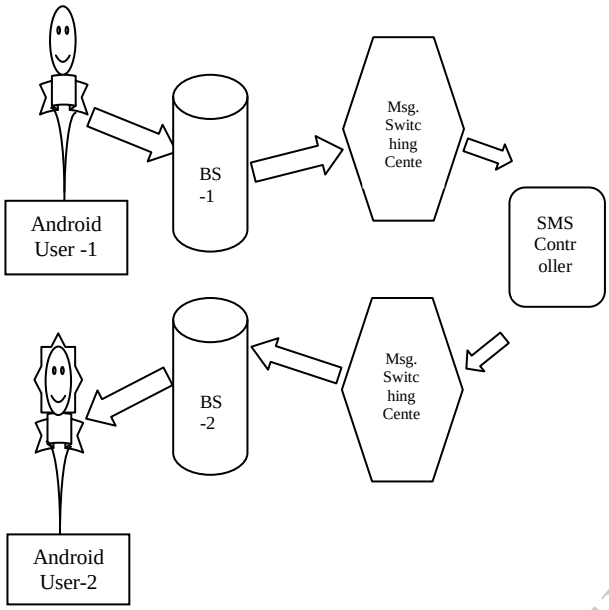

Fig 1. SMS Communication Architecture.

As shown in (Fig 1) of SMS Communication Architecture. Two Android users are shown in figure. One user act as a SMS or information Sender and second Android User act as receiver in wireless communication network. SMS sending from senders goes through various stations. Like Base station, Message Switching Center and SMS Controller station reach up to the receiver. The phase from sender to SMS Controller and SMS Controller to Receiver are same. Message reach to the Base station first later send to the Message Switching center. SMS Controller is work as an intermediate station between sender and receiver. Sender MSC sends SMS to SMS controller. And finally reach up to receiver station.

2. SURVEY

The author D.T Lee Propose the Pandora Messaging architecture for Mobile Devices. One sender sends the SMS to another receiver. At that time consider security is important issue in network communication. SMS contain important data packets or sensitive information. Some unauthorized people access this data. In this paper author implement the self message destructing technique. This application or system enable the set times to sender. This application provides the fast encryption and decryption scheme. Pandora message system proposes the technique of self-message-destructing scheme to users. So, after some time this message unreadable to receiver side due to this message is self destroyable message. One sender sends the destroyable message to receiver with temporary key to receiver. So, Pandora android application provides better Security to SMS communication. [1].

In general process of encryption many application developers develop the android applications using the previous encryption algorithm like AES symmetric cryptography algorithm. Some authors use private and public keys for security of SMS or information. The author David Lisonek design and implement the secure SMS communication application in the network. This application prevents or stops the unauthorized access and exploitation of information. For security purpose author use the RSA asymmetric cipher. A certificate contains or stores the public key. And this certificate signed by legal authorized person. [2] to prevent attacks and protect the SMS author propose the new hybrid encryption algorithm using Eliptic curve compression and lossless compression algorithm. [3] Marko Hassinen author use the public key cryptosystem for SMS communication in android mobile system. These applications provide reliable, complete and secure communication for the mobile communication. This application provides the strong authentication in communication. Public key infrastructure (PKI) verifies the signature of the valid person. And signature also not exploit outside. So this provides strong security. [4]

Many Business organizations and industries are used SMS Tools for communication in the networks. SO, they require End to End encryption and security for communication. Author use calculate the encryption as well as decryption time for various size SMS. Using random SMS scheme evaluate the encryption techniques like RSA, ELGamal, and Elliptic curve. The results of this algorithms show the effectiveness. When increase the key size then increase the encryption, decryption and key generation time. So select the effective algorithm for the SMS encryption. [5] Byte rotation encryption algorithm is a new

implemented algorithm by author sunita bhati. Data or SMS security is a major problem in network. Organization demands the strong encryption algorithm for encrypt the data and difficult to crack. Earlier developers develop various encryption and decryption algorithms for security like AES, DES, triple DES, Blowfish, RSA algorithm. After performance analysis the authors conclude that the AES and Blowfish algorithm is the better performance algorithm but time-complexity of this algorithm is high. In this paper authors propose the parallel encryption model which is gives high security and fast data or SMS encryption. This new encryption algorithm uses the multithreading as well as multiprocessing concept in only single system for processing. They introduce the concept of parallel encryption. [6] Complex algorithms always give best performance due to complex process of encryption or decryption.

Author Priyanka P. [7] modify the AES algorithm for improve the security and strong encryption process. Complex process of encryption and decryption resist the unauthorized access and strong security to SMS or data encryption. If reduce the latency for encryption and decryption processing. And SMS sending as well as receiving latency reduce. Then the reliability and security of SMS communication in the wireless network improve. [8] Author Priyanka Pimpale develops the Android application for the SMS Encryption using AES algorithm. Before sending the data to the receiver SMS require encrypt for security.

Due to brute force attacks or ethical hackers data or SMS require security. AES, DES, Triple DES like many algorithms are used by developers for encryption of the data. But as compare to all other Encryption algorithms AES algorithm gives fast, reliable, and secure performance for the data encryption. So, due to the better performance of the AES algorithm author use this algorithm for SMS encryption using Android application. [9][10] The new algorithm and technique propose the author for strong and secure encryption as well as decryption. This algorithm encrypts the message before second of transfer to receiver so security should be increase. And difficult for ethical hackers to hack or crack the data in the network. This algorithm prevents the Brute force attacks for secure mobile communication.

3. PERFORMANCE REVIEW

Performance analysis shows the behavior and performance of this particular algorithm. And Quality of Services achieved by that algorithms or protocols. As like same here we have done performance review for different algorithms used in survey section of this paper. The bellow given table of Performance Review contains. The Paper Reference Number, Algorithms or Techniques, Parameters achievement and Working as well as Use of this algorithm in that paper. This table is created after analysis of papers result and algorithms. And using papers included in survey.

RP. No.	Algorithms	Parameters Achievement	Working & Use
1.	Pandora: Encryption Application.	1. High Reliability. 2. Better Feasibility.	1. Self Message destroy 2.Temporary Key used
2.	Asymmetric RSA Cipher encryption.	1. High security 2.Prevent Attacks & Tapping.	1.Attack Prevention 2. RSA Public Key Uses.
3.	Hybrid Encryption Algorithm = Eliptic curve encryption & lossless compression	1.Confidentiallity 2.Integirity 3.Security 4.Reliability	1. Encrypt SMS. 2. Reduce length of Encrypted SMS.
4.	Implement Public Key Cryptosystem.	1. Integrity. 2.Confidentiality 3.Non-repudiation	1.Use PKI 2.Provide Security to key
5.	RSA & ELGamal & Elliptive Curve encryption	1. Security with small Key. 2. High Reliability.	1. Improve Security. 2.Reduce Processing Time
6.	Byte-Rotation Encryption Algorithm.	1. Fast Encryption. 2. Decrease Processing Time.	1. Parallel Encryption Model. 2. Multithreading. 3. Block-wise Parallel Encryption.
9.	Android Based Encryption AES algorithm.	1. Attack prevention. 2. Strong Authentication. 3. Security for data Sending.	1. Detect corrupted message during Transmission. 2. E-to-E reliable data Transfer.

Table 1. Performance Review Table for Different Algorithms.

In the above table (1) contain the algorithm or technique used in that particular paper. Parameters or Quality of Services achieved after using this algorithms which is depends upon performance of this algorithm. And finally last column of table shows that working as well as idea behind this algorithm's, this table shows the easy way of

consider performance of algorithm used by developers.

4. CONCLUSION AND FUTURE WORK

Secure mobile communication needs encryption and decryption algorithms. Many developers use, modify and implement new algorithms in previous algorithms for mobile communication. AES, DES, Triple DES etc. are the previous most used algorithms for encryption and decryption.

In this paper we have do the survey of previous and new encryption as well as decryption android application and algorithms. Finally here prove that the AES algorithm is secure, fast and strong encryption algorithm for mobile communication. But one drawback of AES algorithm is its time complexity is more as compared to other algorithms. AES algorithm solves the major issue of security in mobile communication and SMS encryption in network. In future work we have doing survey of the more encryption and decryption algorithms. And develop stronger, secure, and easy new algorithm for encryption and decryption for Android mobile communication.

5. REFERENCES:

[1] T.Tung, L.Lin, D.T.Lee, "Pandora Messaging: An Enhanced Self-Message-Destructing Secure Instant Messaging Architecture for Mobile Devices", IEEE, Internat. Conf. On Advanced Info. Networking & Application Workshops, pp. 720-725, 2012.

[2] David L., Martin D.,"SMS Encryption for Mobile Communication", IEEE, International Conf. on Security technology, pp.198-201, 2008.

[3] R.R. Chavan, M. Sabnees, "Secured mobile Messaging ", IEEE, ICCEET,pp.1036-1043, 2012.

[4] Hassinen M., Java based Public Key infrastructure for SMS Messaging, IEEE, ICTTA, pp.88-93, 2006

[5] M.Agoyi, D.Seral," SMS Security: An asymmetric encryption approach " , IEEE, Internat. Conf. on Wireless Mob.Comm.", pp.448-452,2010.

[6] Sunita B. , Anita B., S.K.Sharma " A new Approach towards Encryption Schemes: Byte-Rotation Encryption Algorithm", World CECS 2012.

[7] Priyanka Pimpale,Rohan Royarikar, Snaket Upadhyay,"Modification to AES Algorithm for Complex Encryption,vol 11,no 10,pp.183-186, IJCNCS Oct 2011.

[8]Dattatray S. Waghole, Vivek S. Deshpande, "Reducing Delay Data Dissemination Using Mobile Sink in WSNs."IJSCE, vol 3, issue 1, pp.305-308, 2013.

[9] Rohan R.,Sanket U.,Priyanka P.,"SMS Encryption using AES Algorithm on Android", IJCA, vol 50, no.19, pp.12-17, jully 2012.

[10] Dattatray S. Waghole, Vivek S. Deshpande "Techniques of Data Collection with Mobile & Static Sinks in WSN's: A Survey.", IJSER, vol 4, issue 10, pp.501-505, Oct 2013.