e-ISSN: 2349-9745
p-ISSN: 2393-8161

Scientific Journal Impact Factor (SJIF): 1.711

International Journal of Modern Trends in Engineering and Research

www.ijmter.com

# CIPHER SMS:RELIABLE AND SECURE SMS TRANSMISSION USING ANDROID

D.GOMIATHI[1],K.LAVANYA[2],M.S UDHAYA[3]
[123]Department Of Information Technology
S.K.P.Engineering College, Tiruvannamalai.

**ABSTRACT -** EasySMS which provides end-to-end secure communication through SMS between end users. Due to increase in use of Short Message Service (SMS) over mobile phones in developing countries, But when we send an SMS from one mobile phone to another, the information contained in the SMS transmit as plain text. Sometimes this information may be

Hacked.inorder to provide secured sms we use AES and MD5 to procect. Providing security with image transaction

**Keywords:**Attacks,transmission,end-to-end Transmission,authentication,security.

## I. INTRODUCTION

Sometimes, we send the confidential information like password, pass code, banking details and private identity to our friends, family members and service providers through an SMS. But the traditional SMS service offered by various mobile operators surprisingly does not provide information security of the message being sent over the network. In order to protect such confidential information, it is strongly required to provide end-to-end secure communication between end users. SMS usage is threatened with security concerns, such as

we present the related work on SMS Spam filtering problem.SMS disclosure , man-in-the-middle attack , replay attack and impersonation attack . There are some more issues related to the open functionality of SMS which can incapacitate all voice communications in a metropolitan area , and SMS-based mobile botelnet as Android botnet . SMS messages are transmitted as plaintext between mobile user (MS) and the SMS center (SMSC), using wireless network. SMS contents are stored in the systems of network operators and can be read by their personnel.

## II. PROPOSED SYSTEM

aspects; firstly, the solution's ability to provide peer- to-peer SMS security. Secondly, the security services which are

provided by the solution, in this case we give attention to four main security services; confidentiality, integrity, authentication and non-repudiation.

Initsusualform,algebraiccryptanalysisonlyrequiresoneplaintext/ciphertextpairtobemou

## III. ATTACK MODEL

An attack model describes different scenarios for the possibilities of various attacks where a malicious MS can access the authentic information, or misguide the legitimate MS. Since, the SMS is sent as plaintext, thus network operators can easily access the content of SMS during the transmission at SMSC. This leads to SMS disclosure attack.The attacker may fraudulently delay the conversation between both MS and can capture or reuse the authenticated information (during the protocol execution) contain in previous messages which results in the form of replay attack. Later, the attacker may send the captured information to the server or token. An attacker can also perform a man-in- the-middle attack when an MS is connected to a BTS through wireless network and eavesdrops the session

In order to overcome the above stated attacks, various cipher algorithms are implemented with the proposed authentication protocol. We recommend that the cipher algorithms should be stored on to the SIM (part of MS) as well as in the AS. Since providing security needs to do some extra effort which is measured in terms of cost, thus providing or adding extra security means increasing more cost. Authors propose to include one more service as ‘Secure Message’ in the menu

## IV. PROTOCOL

In this section, we propose a new protocol named SMS with two different scenarios which provide end-to-end secure transmission of information in the cellular networks. First scenario is illustrated in  where both MS belong to the same AS, in other words share the same Home Location Register (HLR) while the second scenario is presented in  where both MS

nted. In non-server architecture mobile security systems, all the cryptographic operations will be achieved in the user mobile phone deviceThis section focuses on the attack model, system and communication model, basic assumption.

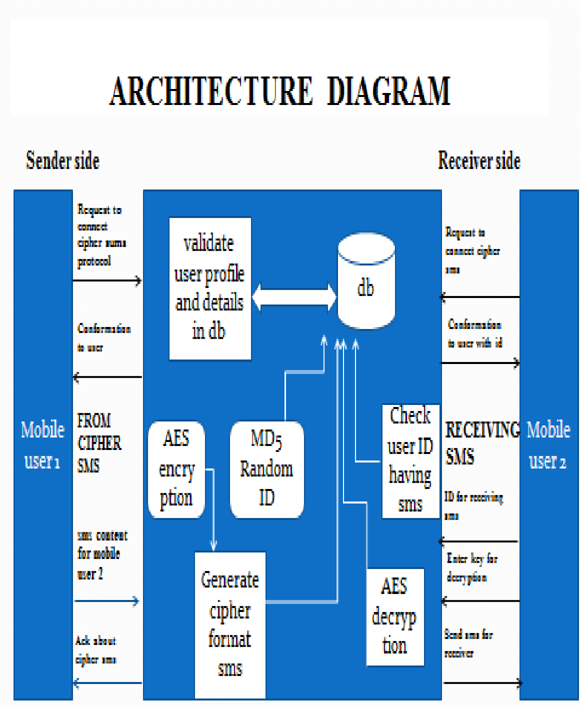
initiated by legitimate MS. The above requirements can be accomplished by proposing a protocol called EasySMS which provides end-to-end security during the transmission of SMS over the network. The EasySMS protocol prevents the SMS information from various attacks including SMS disclosure, over the air (OTA) modification, replay attack, man-in-the-middle attack, and impersonation attack. This EasySMS sends lesser number of transmitted bits, generates less computation overhead, and reduces bandwidth consumption and message exchanged as compare to SMSSec.

## V. COMMUNICATION MODEL

of mobile software developed by various mobile companies as shown in Mobile operators can add some extra charges to send secure message by their customers over the networks. Whenever a user wants to send a secure message to other user, the proposed protocol namely SMS is executed which makes available the symmetric shared key between both MS and then ciphering of message takes place using a symmetric key algorithm.

Belong to different AS, in other words both are in different HLR. There are two main entities in the SMS protocol. First is the Authentication Server (AS), works as Authentication Center (AuC) and stores all the symmetric keys shared between AS and the respective MS. In this paper, we refer AuC as the AS. Second entity is the Certified Authority/ Registration Authority

(CA/RA) which stores all the information related to the mobile subscribers. We assume that every subscriber has to register his/her mobile number with CA/RA entity and only after the verification of identity, the SIM card gets activated by this entity. Thus, this entity is responsible to validate the identity of the subscribers.  We also assume that a symmetric key is shared between the AS and the CA/RA which provides the proper



Previously, various authors have proposed different techniques to provide security to

1) SMS Disclosure: In EasySMS protocol, a cryptographic encryption algorithm AES/MAES is maintained to provide end-to-end confidentiality to the transmitted SMS in the network. Thus, encryption approach prevents the transmitted SMS from SMS disclosure.
2) Replay Attack: The proposed protocol is free from this attack because it sends one timestamp the transmitted messages. An implementation of a public key cryptosystem for SMS in a mobile phone network has been presented in [19] but the security analysis of the protocol has not discussed. A secure SMS is considered to provide mobile commerce services in [20] and is based on public key infrastructure. A framework Secure Extensible and Efficient SMS (SEESMS) is presented in [21] which allows two peers to exchange encrypted communication between peers by using public key cryptography. Another new application layer framework called SSMS is introduced in to efficiently embed the desired security attributes in SMS to be used as a secure bearer for m-payment systems.
with each message during the communication over the network. These unique timestamp values prevent the system from the replay attack. This attack can be detected if later previous information is used or modified.
3) Man-in-the-Middle Attack: In EasySMS protocol, a symmetric algorithm AES/MAES is used for encrypting/ decrypting end-to-end communication between the MS and the AS in bothscenarios.

## VI. CONCLUSION

Cipher sms is designed in order to provide a secure sms communication and secured image chating.it preventes from various attacks, It consumes very low bandwidth and provides a good data security tan smssec and Easysms.it provides end to end secure transmission.

## VII. REFERENCE

[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
[4]Experience," 6th MobiSys, No. 33, 2009. Kuldeep Yadav, "SMSAssassin: Crowdsourcing Driven Mobile-based
[5]System for SMS Spam Filtering," Workshop Hotmobile, 2011, pp. 1-6.
[6]J. Chen, L. Subramanian, E. Brewer, "SMS-Based Web Search for Lowend Mobile Devices," 16th MobiCom, 2010, pp. 125-135.
[7] B. DeRenzi, "Improving Community Health Worker Performance through Automated SMS," 5th ICTD, 2012, pp. 25-34.
[8]M. Densmore, "Experiences with Bulk SMS for Health Financing in Uganda,"ACM CHI, 2012, pp. 383-398.
[9]Anuar N, Kuen L, Zakaria O, Gani A, Wahab A (2008). GSM mobile SMS/MMS using public key infrastructure: m-PKI. WSEAS