Smart Message Communication for Warrior

Santhosh kumar S[1,] Athmaranjan K[2], Lohith[3], Basavanagouda Patil[3]
[1] *Srinivas Institute of Technology valachil, mangalore, India*

Abstract:

Message Service is getting more popular now-a-days. Message (SMS) was first used in December 1992, when Neil Pap worth, a 22-year-old test engineer used a personal computer to send the text message "Merry Christmas" via the Vodafone GSM network to the phone of Richard Jarvis in the UK. It will play a very important role in the future business areas of mobile commerce (M-Commerce). SMS's security has become a major concern for business organizations and customers.

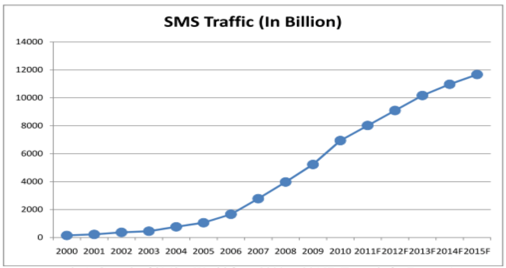
Many people send delicate information and conduct private conversations via text with little protection from third parties who might intercept the message (SMS) or the storage of their information in phone company records but this is not case for soldiers .The message (SMS) communication between soldiers in order to fill this void and offer soldiers a more securely private means of textual communication, Smart Message Communication for Warrior Using Android is developed.

We used ECC cryptosystem for encryption and decryption of message (SMS). Text Encryption will be a third-party application capable of running on any Android system. It will allow users to send and receive encrypted text messages using our application. About key exchange we used Diffie Hellman key exchange mechanism it'll allow automatically exchange key between soldiers and start a secure session. In this way, we hope to provide a safe and secure means of transferring private messages between any two Android phones and it'll also provide identifying end user as a valid user or not.

Keywords: *Android, Decryption, Encryption, ECC, SMS, Text secure, Cryptosystem.*

I. INTRODUCTION

Messaging (SMS) is getting more popular now-a- days. It will play a very important role in the mobile messa mobile commerce [3] (M-Commerce). Up to now many business organizations use SMS for their business purposes. SMS's security has become a major concern for business organizations and customers. There is a need for an end to end SMS Encryption in order to provide a secure medium for communication. Security is main concern for any business company such as banks who will provide these mobile banking services. Currently there is no such scheme that provides complete SMSs security. The mobile messaging market is growing rapidly and is a very profitable business for mobile operators. It can be seen from figure1 that the growth rate of SMS in worldwide during 2000 – 2015F (F stands for forecast) in billion.SMS has a variety of advantages and disadvantages for M-Commerce purpose [3]. The advantages are easy to use, common messaging tool among consumers, works across all wireless operators, affordable for mobile users, no specific software required to installation, allows banks and financial institutions to provide real-time information to consumers & employees, stored messages can be accessed without a network connection.



Growth of SMS – World from 2000 to 2015F (F stands for Forecast)

Fig. 1: SMS Traffic

Very few disadvantages are text data and limited up to 140-160 characters per message, does not offer a secure environment for confidential data during transmission and there is no standard procedure to certify the SMS sender. Presently researchers proposed some security concepts regarding SMS security. Most of the proposals are software frames to be installed on mobile device and /or on the SIM cards to implement security [4].

Two are the major security vulnerabilities affecting SMS [1] based communication: the lack of confidentiality during the transmission of a message and the absence of a standard way to certify the identity of the user (or at least his phone number) who sent the message.

This project regarding to exchange message in secure manner at peer level. It has a software framework to enable user to transfer message in secure manner using ECC [5] and security parameters for transmitting secure message to achieve better cost and efficiency of the operation.

This represented in external architecture of project as shown in figure 2.

The remaining part of the paper is organized as follows: Section II gives a view about secure messaging, Section III describes the System Architecture, Section IV describes the Implementation details, and finally Section V gives the conclusion and future work.

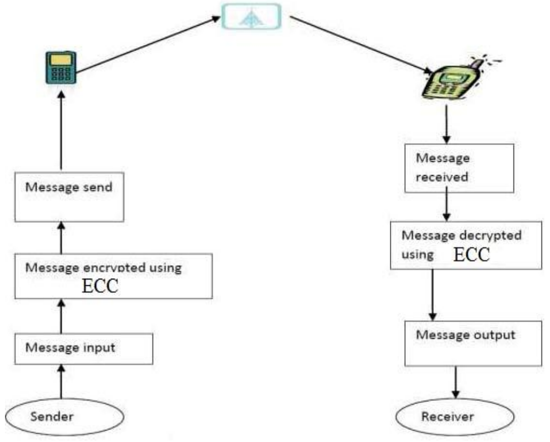


Fig. 2: External architecture

II. SECURE MESSAGING

Project is based on non-server architecture mobile communications; security solutions are implementable for individuals due to its independency from the mobile phone network operator or service provider. Thus, the user does not need to make any agreement with the mobile phone network operator or service provider and use of ECC cryptosystem [4] through a non-server based architecture makes better choice to easily experiment. As a result, all the cryptographic operations are achieved on the user's mobile phone. Terms of overhead cost of communication is less than server architecture system, due to discard in the communication between the user and the server

Secure messaging will be a third-party application capable of running on any Android system. It will allow users to send and receive encrypted text messages using the standard SMS [10] text messaging system and will only sends encrypted data over that system. Without the secure SMS program and an appropriate key/password, any intercepted or stored messages will appear unreadable. In this way, we hope to provide a safe and secure means of transferring private messages between any two Android phones.

III. SYSTEM ARCHITECTURE

The SMS system is a service provided by mobile network company. Our main motto is implementing a security[4] at application level this process contains 4 fundamental elements sender, receiver, encryptor and decryptor which are shown in figure 3.

Sender: The sender using "Secure Message Communication for Battlefield Soldiers Using Android" application allowed to enter passphrase for generating a local key value .After generating key value sender can establish a secure session with other device .This secure session indicates a encrypted SMS transfer between sender and receiver.

Receiver: As soon as message arrived from sender to receiver, receiver is intimated by a notification message indicating that key exchange and processing of key is completed and secure session can start now. Both at sender and receiver encryption (while sending) and decryption (while receiving) occurs automatically.

Encryptor and Decryptor: This takes a text message entered by user and key which is exchanged between two parties before session begins. Encryptor module automatically encrypts SMS and sends that to receiver. Sender also nowhere aware about cipher pattern. Whereas decyptor takes a cipher text which is received from SMS System and takes key which is exchanged before secure session established. As soon as cipher SMS is received from sender , the decryptor module converts that into plane text and displays in device screen.

SMS System: This is built in mobile network where it performs a store forwarding of message to or from end users.

Shared key: This key is generated at both end automatically by using a local key pairs generated in communicating parties. This generated local key pairs are exchanged by using Diffi Hellman key exchange algorithm.

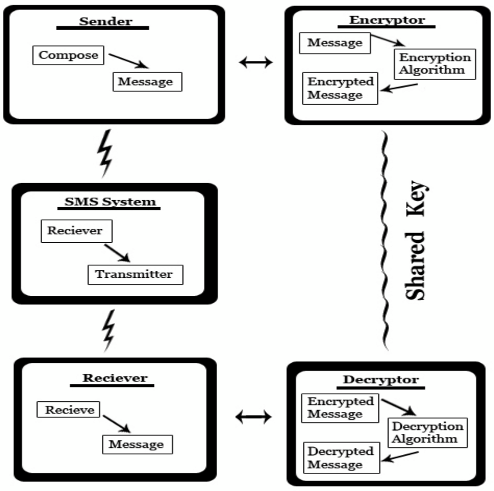


Fig. 3: System architecture

IV. IMPLEMENTATION

Secure message application developed using Android JAVA and which uses crypto packages from java library. The implementation includes dividing complete project into four modules they are sender, receiver, encryption and decryption modules and GUI for sender is such that sender is allowed to enter receiver mobile number, raw key and message which is to be transmitted while at receiver end, receiver is allowed to enter same raw key to decrypt and read. The coding keeps users away from the internal key generation and encryption/decryption part this makes project simple and efficient.

V. RESULTS

Transferring a encrypted messages in a secure session with a less delay by automatic encrypting and decrypting the message before transmission begins and also identifying a man in middle attack. There will be dialog which accepts passphrase value from Soldiers to generate local encryption key. Then we get toast message showing a generation of encryption key pair. Then we get dialog showing establishment of secure session with particular soldier. Then we get automatic key exchange message between two parties. This indicates a secure session is established. Then we get dialog showing identification of session. This feature helps to identify man in middle attack. Finally we get menu options i.e. verify recipients identity, verify secure session and aborting session.

REFERENCES

[1] Ahmed MA, Kiah MLM, Zaidan BB, Zaidan AA. "A Novel on Linux for Android Mobile Devices". J. Appl. Sci., 10(1): 59-6

[2] Lisonek, David, Drahansky, Martin. “SMS Encryption for Mobile Commerce”, Security Technology, International Conference, 2008, doi:10.1109/SecTech.2008.48.

[3] R Agoyi Mary, Seral Devrim. “SMS Security in GSM[4]: An Asymmetric Encryption Approach”, 6th International Conference, 2010, pp. 448-452, doi: 10.1109/ICWMC.2010.87.

[4] J. Hoffstein, J. Pipher, J. H. Silverman, “AES: Cryptosystem”, Algorithmic Number Theory (ANTS III), Portland,266-278.

[5] Alam GM, Kiah MLM, Zaidan BB, Zaidan AA, Alanazi HO ,“Usingthe features of mosaic image and AES[20] cryptosystem to implement an extremely high rate and high secure data hidden: Analytical study” Sci. Res. Essays, 5(21): 3254- 3260.

[6] Alanizi HO, Kiah MLM, Zaidan BB, Zaidan AA, Zaidan Alam GM . “Security Using AES for Electronic Record Transmissions.” Int. J. Pharmacol., 6(6):54-958. Barkan E.

[7] W Balitanas M, Robles RJ, Kim N, Kim T, (2009). "Mobile Communication in Server and Non- Server Mode." Proceedings of BLISS 2009, Edinburgh, GB,IEEE CS.

[8] Challa N, Pradhan J .” Performance Analysis of Public key Cryptographic Systems RSA and AES-128 BIT”. IJCSNS Int. J. Comput. Sci. Netw. Security, 7: 87-96. Al-Bakri et al. 93.

[9] Hassinen M, Markovski S (2003).” Secure SMS messaging using Quasi encryption and Java SMS API”. Google-developed Java API In: SPLST'03, Finland.

[10] Hassinen M (2006). “Java based Public Key Infrastructure for SMS Messaging” Inf. Commun. Technol., ICTTA'06. 2(1). Hermans, J, Vercauteren F, Preneel B (2010). Speed records for AES-128 BIT. Topics Cryptol., CT-RSA: 73-88.