IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

END TO END TRANSMISSION OF SMS USING CRYPTOGRAPHY TECHNIQUE

Saurabh M. Chaudhari*, Prof. Chetan Bawankar
* Department of Computer Science & Engineering, Wainganga COE&M, RTM Nagpur University, Nagpur, India,
Department of Computer Science & Engineering, Wainganga COE&M, RTM Nagpur University, Nagpur, India,

ABSTRACT

Short message service (SMS) is a very popular and one of the easy to use communication technologies for mobile phone devices. Originally, this service was not designed to transmit secured data, so the security was not an important issue during its design. Short Message Service is normally used to transport unclassified data, but with the rise of mobile commerce it has become a fundamental tool for conducting business. However SMS does not guarantee confidentiality and integrity of the message. Now a days, short message service (SMS) is being used in many daily life applications, including mobile banking, mobile commerce, and so on. But when we send an SMS from one mobile device to another, the information contained in the SMS transmit as plain text. Sometimes this information may be confidential like account numbers, passwords, license numbers, and so on, and it is a major drawback to send such information through SMS while the traditional SMS service does not provide encryption to the information before its transmission. In this paper, we propose an efficient and secure technique, which provides end-to-end secure communication through SMS between end users. This paper proposes encryption technique that can be used to secure a SMS communication, when SMS is transmitting form source to destination, it have to be reached up to the destination securely means SMS transmission have to be secure.

KEYWORDS: Authentication, network, security, SMS, symmetric key etc.

INTRODUCTION

Various types of tools have been created to make human communications simpler and faster. The most significant communication tool is the modern telephone which was first invented by Sir Alexander Graham Bell in the 19th century. Short Message Service, better known as SMS is a service that enables the sending of text messages over a mobile cellular network. Short Message Service (SMS) has become one of the fastest and strong communication channels to transmit the information across the worldwide. A secure SMS is considered to provide mobile commerce services and is based on public key infrastructure. It is not clear whether the proposed approaches are able to prevent SMS against various attacks. All the above mentioned approaches /protocols/frameworks generate a large overhead as they propose an additional framework for the security of SMS. Due to physical limitations of the mobile phones however, implementation of framework always increases the overall overhead which is not much suitable for the resource constraints devices such as mobile phones. Short message service (SMS) is a very popular and easy to use communications technology for mobile phone devices. Short Message Service (SMS) has become an extension of our lives and plays a very important role in everyday life. SMS may be a standard medium for delivering price more Services and ar appropriate for mobile banking, payment reminders, stock and news alerts, railway and flight enquiries etc. These styles of messages are usually computer generated messages sent over Short Message Peer to look (SMPP) protocol. Causation an SMS is reasonable, quick and easy. The service permits for brief text messages to be sent from one cell phone to a different mobile phone or from the net to a different mobile phone. Once someone sends an SMS he or she sometimes uses her phone keyboard or physical or onscreen keyboard to sort out a message. The user selects the recipient's signal (or alternative address information) and clicks "send." From there, the message is distributed to a brief message service center (SMSC) that stores it and tries to send it on to the recipient. If the receiver is on another network, the message could travel through entry mobile change center (MSC) that permits the various systems to speak. The SMSC sometimes stores the message if it can't be sent straightaway and retries later; in some cases, however, the message are born if it's not delivered with success on the primary try. Messages will be sent while not the voice perform of a mobile phone being activated as a result of it uses the management channel. This pathway is usually active whenever the phone is turned on, and frequently sends and receives signals from the closest cellular tower. We propose encryption technique that can be used to secure a SMS communication, when SMS is transmitting form source to destination, it have to be reached up to the destination securely means SMS transmission have to be secure.

BACKGROUND

Following method plays an important role in our project work to protect data from attack to improve security.

Encryption Method

Encryption method mainly resolves the problems that, prevents various attacks, including SMS disclosure, over the air modification, replay attack, man-in-the middle attack, and impersonation attack when people send a message over the network. In this system we will create a server that register the user and authenticate the end user. The work of the server is creating a communication the user and acknowledgment is only done via server. By doing this we can remove man-in-the middle attack and when we transmitting data we encrypt it by using advance encryption algorithm.

RELATED WORK

Previously, various authors have proposed different techniques to provide security to the transmitted messages. EasySMS protocol is consider to provide secure from various attack and transmit massage securely[1] and a custom designed GPS-GSM unit is placed on a vehicle and users van query server over SMS with their own non-GPS enable cell phones[3]. A mobile based system SMSAssassin that can filter SMS spam messages based on Bayesian learning and sender blacklisting mechanism [4].

Above mentioned all previous papers have approaches/frameworks/protocols generate a large overhead as they propose an additional framework for the security of SMS. Due to physical limitations of the mobile phones, it is recommended to develop highly secure technique which would make minimum use of computing resources and would provide better security. We wanted to compare our proposed technique with some existing technique devoted to provide end-to-end SMS security with symmetric key cryptography. Existing protocols are having two phases similar to the proposed technique and are based on symmetric as well as asymmetric key cryptography while the proposed technique is completely based on symmetric key cryptography.

PROPOSE METHODOLOGY

In our system we will create a network of mobile, so that they communicate with each other and so we create a server that registers all the mobile and responsible of their communication. We use Rijndael algorithm (i.e. Advance AES) and server is responsible for remove various attacks. In this system we will create a server that register the user and authenticate the end user. The work of the server is creating a communication the user. And acknowledgment is only done via server. By doing this we can remove man-in-the middle attack and when we transmitting data we encrypt it by using Rijndael Algorithm based on Advance AES (advance encryption standard).

Rijndael Algorithm based on Advance AES is based on the Rijndael cipher developed by two Belgian cryptographers, Joan_Daemen and Vincent_Rijmen, who submitted a proposal to NIST during the AES selection process. Rijndael is a family of ciphers with different key and block sizes. For AES, NIST selected three members of the Rijndael family, each with a block size of 128 bits, but three different key lengths: 128, 192 and 256 bits. AES (advance encryption standard) requires the block size to be 128 bits, the original Rijndael cipher works with any block size (and any key size) that is a multiple of 32 as long as it exceeds 128. The state array for the different block sizes still has only four rows in the Rijndael cipher. However, the number of columns depends on size of the block. For example, when the block size is 192, the Rijndael cipher requires a state array to consist of 4 rows and 6 columns.

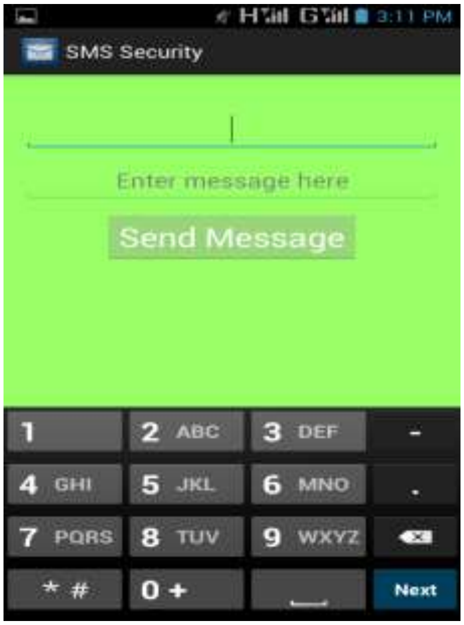
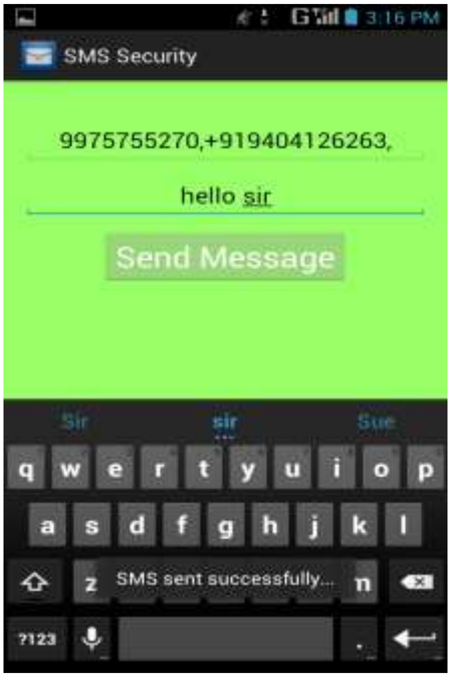


Fig.1 Snapshot for creating a message



9975755270,+919404126263,

hello sir

SMS sent successfully...

Fig. 2 Snapshot for transmission of message

The above snapshot shows, for adding contact from contact list and write a message to send. On clicking the Send Message button, toast appears SMS sent successfully.

CONCLUSION

Encryption algorithm will be provide end-to-end secure communication through SMS between mobile user and also prevent form various attacks. This technique provide more secure end to end communication will be reduces message exchange ratio during authentication than other previous protocols and techniques.

REFERENCES

[1] Neetesh Saxena and Narendra S. Chaudhari, “EasySMS: A protocol for end-to-end secure transmission of SMS” IEEE Transaction on Information Forensic and Security, VOL. 9, NO. 7, JULY 2014.

[2] Shuangqing Wei, “Trade-off between security and performance in block ciphered systems with erroneous cipher texts” IEEE Transaction on Information Forensic and Security, Vol. 8, Issue: 4, April 2013.

[3] Duangphasuk S, “Design and accountability analysis of a secure SMS-based mobile payment protocol” IEEE Transaction on Information Forensic and Security, May 2011.

[4] R. E. Anderson, “Experiences with a transportation information system that uses only GPS and SMS” in Proc. IEEE ICTD, no. 4, Dec. 2010.

[5] K. Yadav, “SMSAssassin: Crowdsourcing driven mobile-based system for SMS spam filtering” in Proc. Workshop Hotmobile, 2011, pp. 1–6.