COMPARATIVE STUDY - SMART TEXT COMPRESSION AND ENCRYPTION OF MESSAGE FOR MOBILE COMMUNICATION

Mrs.Mayura V.Shelke
Department of Computer Engineering
JSPM's Bhivarabai Sawant Institute of Technology and Research
Pune, India
Mayura.shelke@gmail.com

Abstract—**Today's mobile phones are widely used for personal communication as well as for official purpose. The data security and reliability are important issues in mobile communication. So Short text compression is a great concern for data engineering and management. Also the encryption technique provides greater security of compress data.**

In this paper we compare the different techniques used in text compression and encryption for mobile devices

***Keywords*— Text Compression, Text Encryption, Smart Devices, Mobile phones,AES,DES,RSA**

I. INTRODUCTION

In Mobile communication, one of most important way of communication is SMS. SMS is now become a popular and uses by every individual user. Short message service (SMS) is a text message service that enables users to send short messages to other users on the global system for mobile communication (GSM) network. In today's environment, most banks are using the SMS's for exchanging the information with their customers. SMS is very popular that's why the research direction are moving towards the security solutions through SMS like in M-banking, M-Commerce, value added services etc. The advantages of using SMS's are its ease of use, common messaging tool among consumers, works across all wireless operators, affordable for mobile users, no specific software required for installation, allows banks and financial institutions. To provide real-time information to consumers and employees, stored messages can be accessed without a network connection.
A primary shortcoming of GSM is that, it does not offer a secure environment for confidential data during transmission and there is no standard procedure to certify the SMS sender. There is a requirement for an end to end SMS encryption with errorless message transmission in order to provide a secure with error free data transmission for communication. The paper reviews the different text compression techniques and encryption.

II. THE SHORT MESSAGE SERVICE ARCHITECTURE

The Short Message Service is a standardized facility defined as part as of the Global System for Mobile Communications (GSM) series of standards. Figure 1 shows the architecture of an SMS cellular network.

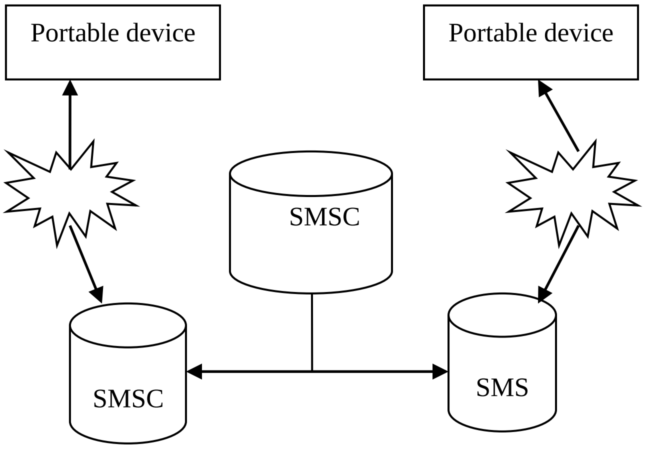

Fig. 1. : A simplified view of the SMS Architecture.

Any message, sent via SMS, is not directly delivered to its destination, but it is stored into an SMS Center (SMSC) after passing through a Mobile Switching Center (MSC), which If the destination device is unavailable or not connected to the GSM network, the messages are stored in the SMSC and delivered when the destination becomes available again, through another message switching center.
But a secure SMS system requires

a. Authentication: Confirm true identities between sender and receiver, and prevent Impersonation attack from Illegal intruders.
b. Confidentiality: Ensure that decrypted messages are accessible only to those authorized senders and receivers.
c. Integrity: Integrity of information refers to protecting information from being modified by unauthorized parties.

III. SMART TEXT AND ENCRYPTION FOR SHORT MESSAGE SERVICE(STCESMS)

A. SMS Ccompression Schemes

Smart Text Compression and Encryption for Short Message Service (STCESMS), that, from one source, compresses and sends an input message/file via SMS, and, from the other one, receives and decompresses the data received via multiple SMSes. There are several commercial SMS compression schemes available.

a. The IDBE (Intelligent Dictionary based Encoding) – IDBE is used to compress short messages up to an optimal level, which requires optimal space, consumes less time and low overhead and reduces the communication costs. IDBE is used to design a semantic dictionary which will store compressed short forms.
b. GSM TS03.42 - GSM Association (GSMA) developed Technical Standard (TS) 03.42, a standard for compression of SMS messages.
c. LZW - LZW is a general compression algorithm capable of working on almost any type of data. LZW compression creates a table of strings commonly occurring in the data being compressed, and replaces the actual data with references into the table. The table is formed during compression at the same time at which the data is encoded and during decompression at the same time as the data is decoded. LZW compression replaces strings of characters with single codes. It does not do any analysis of the incoming text.

B. *Encyption*

Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text; encrypted data is referred to as cipher text. There are two main types of encryption: asymmetric encryption (also called public-key encryption) and symmetric encryption. There are different algorithms used to achieve security for data. Here is survey for SMS encryption techniques, algorithms and performance analysis survey for encryption and decryption

TABLE I.

Sr. No	*Algorithm*	*key length*	*Working & Use*	*level of security*	*encryption speed*
1	RSA	Key length depends on no. of bits in the module	Attack Prevention RSAPublic Key Uses	Good level of security	Average
2	DES	64 (56 usable)	Exclusive Key search, Linear cryptanalysis, Differential analysis	Adequate security	Very slow
3	AES	128,192,256	Detect corrupted message during Transmission. E-to-E reliable data Transfer.	Excellent security	Excellenct
4	IDEA	128	Linear attack	Secure	Fast
5	BLOW FISH	Variable key length	No attack is found to be successful against blowfish	Highly secure	Very fast
6	ECC	Smaller but effective key	Doubling attack	Highly secure	Very fast

IV. Comparative study

1. Low-complexity compression of short messages

This paper describes a low-complexity scheme for lossless compression of short text messages. Arithmetic coding and a specific statistical context model these two methods used for prediction of single symbols .This model gives good compression rates with a RAM memory size of 128 kByte, thus making lossless data compression with statistical context modeling readily applicable to small devices like wireless sensors or mobile phones.

2. Short text compression for smart devices

This paper, proposed an approach of compressing short English text for smart devices. The prime objective of this proposed technique is to establish a low-complexity lossless compression scheme suitable for smart devices like cellular phones and PDAs (personal digital assistants) having small memory and relatively low processing speed. The main target is to compress short messages up to an optimal level, which requires optimal space, consumes less time and low overhead. Here they propose a new static-statistical context model to obtain the compression. They analyze the performance of the proposed scheme as well as the other similar existing schemes with respect to compression ratio, computational complexity and compression-decompression time.

3. SMS Text Compression through IDBE (Intelligent Dictionary based Encoding) for Effective Mobile Storage Utilization

This paper proposes a technique for maximizing the utilization of the storage space present in mobile phones. Thus it is important to utilize the space occupied by SMS files in phone’s memory, which take maximum space. The objective involved is designing a semantic dictionary based on Intelligent Dictionary Based Encoding (IDBE) which provides a high text compression ratio to utilize the space in phone’s memory. When SMS file will be received, English words present in the text will be replaced by the respective short words in the designed semantic dictionary. Thus replacing English words by the respective short forms reduces the space occupied by the SMS file.

4. Text Compression and Encryption Through Smart Devices for Mobile Communication

This paper investigate the possibility of reliably sending
a small file via Short Message Service (SMS) by using data
Compression for a more effective mobile data exchange in which basic GSM is the only available data communication option. They present an application for portable devices, called Smart Text Compression and Encryption for Short Message Service (STCESMS), based on Google Android OS that can compress and/or encrypt a file or generic message and send it via SMS, according to different strategies properly influenced by the containment of delivery cost or energy consumption objectives. STCESMS also provides encryption services, implemented by using the Data Encryption Standard, after the compression process.

V. CONCLUSION

In this paper we presented comparative study of different techniques used in text compression and encryption for mobile devices

References

[1] Raffaele Pizzolant, Bruno Carpentieri, Francesco Palmieri, ”Text Compression and Encryption Through Smart Devices for Mobile Communication” IEEE pp.672-677,2013

[2] S. Rein, C. Guhmann, and F. H. P. Fitzek, “Low-complexity compression of short messages,” in Data Compression Conference, 2006. DCC 2006.Proceedings, pp. 123–132., 2006

[3] M. Islam, S. Ahsan Rajon, and A. Podder, “Short text compression for smart devices,” in Computer and Information Technology, 2008. ICCIT 2008. 11th International Conference on, pp. 453–458, 2008

[4] Parul Bhanarkar & Nikhil Jha,”SMS Text Compression through IDBE (Intelligent Dictionary based Encoding) for Effective Mobile Storage Utilization,”, IJCCT, Vol- 3,pp.22-26

[5] Paul Gardner-Stephen, Andrew Bettison, Romana Challans, Jennifer Hampton, Jeremy Lakeman, Corey Wallis,” Improving Compression of Short Messages”, Int. J. Communications, Network and System Sciences, pp.497-504,2013

[6] Punam V. Maitri, Rekha V. Sarawade, Mayuri P. Patil “MSC : Mobile Secure Communication Using SMS in Network Security : A Survey” International Journal of Engineering Research & Technology (IJERT) pp. 3446- 3448

[7] Gurpreet Singh , Supriya “A Study of Encryption Algorithms (RSA, DES, 3DES and AES) for Information Security”, nternational Journal of Computer Applications ,vol-67,pp.33-38,2013