Design and Implementation of SMS Security System for Mobile Environment

Young-Hwan Park*, Hea-Sook Park**

Contents

Ⅰ. Introduction

Ⅱ. Related Research

Ⅲ. Designs and Implementation of SMS System

Ⅳ. Implementation

Ⅴ. Conclusion

Key Words:SMS, DES, Encryption, Decryption, Information Security

Abstract

This paper aims at developing communication module and application program for client management module and developing database management module and managing wireless communication facilities for server systems. To construct these aims, we have adapted DES algorithm and researched on encrypting and decrypting module development applicable to SMS Security System and optimize module size and processing speed.

* Dept. of Computer Engineering Hansung University, yhpark@hansung.ac.kr

** Dept. of Computer & Information Technology 1Kyungin Womens's College. 548-4 Gyesan-dong, Gyeyang-gu, Incheon 407-740 Korea . edpsphs@kic.ac.kr

I. Introduction

SMS (Short Message Service) is a two-way mobile data communication service for mobile (cell-phones, PDA) may exchange short messages without additional equipment [1,2]. SMS is widely used domestically due to the accuracy and promptness and other advantages of SMS, and GSM(Global System Association) reported that 19 billion messages were transmitted per month worldwide last year [3]. Unlike the electronic mailing service, the SMS is a service that could receive the transmission immediately that it can be classified largely in two service types. First, This is the living information service that uses the unilateral one-way communication concept including the exchange of simple information between the two terminals, transmission of advertisement information, and informing of voice mail of mobile phone system. Second, it is a custom-made information service by using the consecutive message forwarding and receiving. The systems developed by using SMS are purported to provide a variety of services in these fields. In addition, the on-going researches are focusing on the system research and development for M-Commerce by using 3A (Anytime, Anywhere, Anyone), an advantage SMS has under the mobile Internet environment. However, there are still insufficient efforts in resolving the shortage of SMS, the issue of security.

SMS may have the users incur damages by exposing the message or altering the message by those people with malicious intent when the users wish to use the e-commerce service and receiving various transaction and payment information or since the security functions on information exposure by the third party and ensuing information alteration, and in the event that a credit card is stolen or lost, the transaction information may not be made to deliver to the owner. These shortages may become the factors in interfering with the safe e-commerce environment. Therefore, if the security of SMS is strengthened to remove the risks on information exposure and alteration, it would be applied effective on the areas of services on order of goods for M-Commerce and E-Commerce, proceed payment, confirmation of payment, forwarding of electronic receipt and others, services on balance inquiry, transfer, introduction of new financial product on mobile internet banking service, and services on various auction service, reservation service area.

In this thesis, in order to present the message exposure by a third party and ensuring alteration of messages from the SM transmission, the security system for SMS with the basis of applying the encryption technology is to be developed. For this purpose, the DES algorithm is to be applied with the appropriate algorithm to use the small resource of mobile device effectively. DES has the advantage in easy realization of encryption device implementation with a little calculation volume than other algorithm when encrypting and decrypting of the information. This thesis implements the SMS security system to use such strengths to enable the client side to encrypt and decrypt the messages while the server undertakes function in many areas.

The structure of this thesis is as follows. In Chapter 2, the characteristics of several researched and developed systems on SMS and the features of SMS are observed, learns briefly on the DES encryption algorithm applied to implement the SMS security system, in Chapter 3, the entire structure chart of the system and the implemented portion of design are studied in detail, and in Chapter 4, the transmission process for the actually encrypted message by using the system implemented is shown. And, in the Chapter 5, I present the conclusion and the future research plans.

Ⅱ. Related Research

2.1 Research related to SMS

SMS related researches are mainly the studies on system structuring that, on [4], the mobile system using SM is designed and implemented, and the system extracts the samples in Random Digital Sampling method, forwarding the SM by the predetermined scheduler on the extracted sample, and the response result is stored on the database to analyze and process in real time.

[5] is implemented to enable the wired and wireless linkage for the auction system that can be supported in real time under the wireless environment that the bidding price on the auctioned product is confirmed on wired and wireless environment. This system is made up on J2SE base for the desktop environment and J2ME, the Java2 platform for the wireless environment. In order for capability assessment, the processing delay time following the number of user contact and the processing time of system following the size change of pool that connects the database are measured. In [6], the system to deliver the stock information with voice is developed and it designed the Voice XML server module for stock information, SMS server module to perform the authentication procedure, the PSTN network, CTI module for interface and others. At this time, the SMS certification based on random disposable password is attempted as for the method of certification.

From [7], the existing SMS is designed to operate on the main memory data structure that the DBMS concept is applied to point out and supplement the shortcomings of recovery function simultaneous control function deficiency. The SMS system is implemented on main memory, DBMS, and disc based DBMS, and makes the comparison and analysis on capabilities. For the result of capability assessment, up to 1,700 messages per second is processed in the capability assessment using the main memory DBMS, and up to about 80 messages per second on the cache condition under the disc-based DBMS. For other related research, [8] implements the various format of MMS (multimedia message service including image) forwarding system, not a simple message.

2.2 DES (Data Encryption Standard)

The data encryption method for information protection is largely divided into the symmetric algorithm and asymmetric algorithm depending on the presence of symmetry of key value. In addition, it is classified depending on the size of encryption data. The symmetric algorithm is called symmetric algorithm in the event that the encryption key value used in encryption of the plane text has the same decryption key value with the encrypted date is decryption into the plane text. And, in the event that the encryption key value and the decryption key value are different, this is called as asymmetric algorithm. In addition, the algorithm that produces the fixed size of encryption data is called as block algorithm, while the algorithm that produces the encrypted data in the stream form by accepting the stream form without the limitation of input size is referred to as stream algorithm. The DES (Data Encryption Standard) applied in this thesis is symmetric encryption method with the block algorithm[9]. DES is a block encryption method to divide the plane text block for 56 bits, and converts the encryption key of 56 bits of each length of the plane text block to convert into 64 bits of encryption text through the 16 times of substitutions and replacements. At this time, the same key is used for the sender and the receiver to encryption and decryption of information. This method has the advantage in fast speed to encryption of the message. It also has a little calculation volume when encrypted and decrypted of the message comparing to the open key encryption method that the implementation of encryption device is easier. For short-comings, the sender and the receiver use the same key that it may cause some difficulty in safe use of secret key among the users in an open environment like internet, and in the event of encrypted text becomes decryption in damaged condition, it may be decrypted differently from the original text.

Ⅲ. Designs and Implementation of SMS System

3.1 Security Request of System

In this thesis, the security requirement needed to the system under the mobile environment is presented as follows. First, in order to maintain the confidentiality, the secret key uses the random number generator to generate 1024 bits of random numbers, and in order to keep the secret key safely, it uses the Diffie–Hellman key distribution algorithm. Client that safe key management is possible makes the generated key. Second, in the event the receiver gets the message when designing the database for the non–repudiation function, it shall be able to confirm. Third, for the mobile authentication and user authentication, the database is designed accordingly.

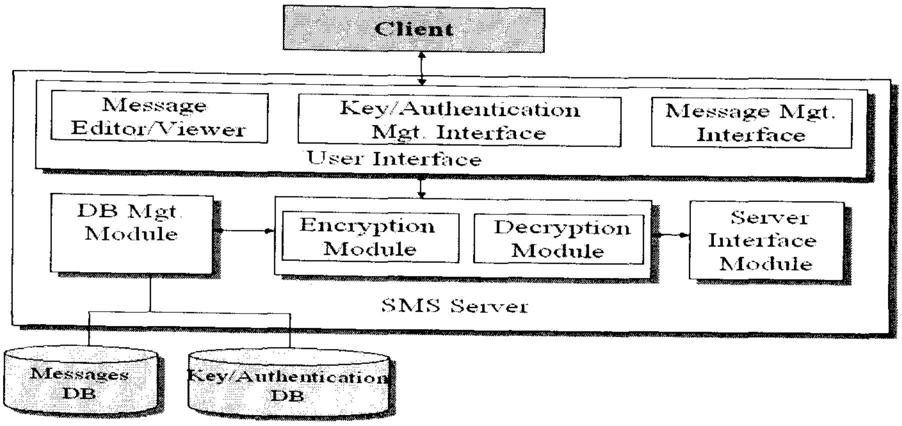
3.2 Structure of System

The entire structure of the SMS system is like the Fig. 1.

The client performs the functions of message management and transmission, user and group management. If the client wishes to transmit the message, it logs in on the server, prepares and encrypts the message and the encrypted message is transmitted to the server. The message prepared at this time becomes the encryption with the secret key of the client. If another client receives the messages from the server, receive the encrypted message after logging in. The message encryption in its own secret key is decrypted.

The message management function of server is largely divided into two stages. Server decrypts the encryption message transmitted from the client, then encrypts again with the secret key of the receiver to store in the database. Server makes the contents of transmitting messages unable to read. If the receiving client wants the message reception, the encrypted message

Fig. 1 System Architecture of SMS



is forwarded after the client certification.

3.3 System Design

In this research, the component modeling method of UML–base is used for the SMS security system development for the message transmission between sending client and receiving client. Through the diagram in case of using UML, sequence diagram, and component diagram, each objects and components are extracted and their relationships are expressed.

Fig. 2 is the diagram displaying the relationship between each component that is generated for message forwarding and the interface. Each component has the equivalent interface existing. The functions of each interface are shown in Table 1.

Fig. 2. Component Diagram

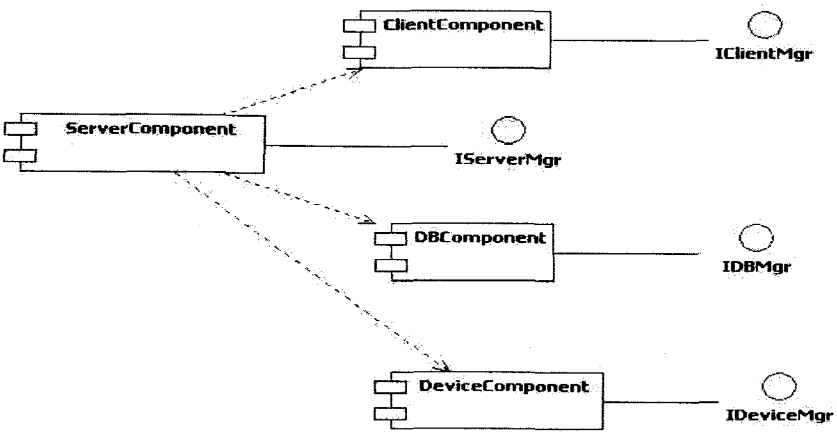


Table 1. Types and functions of interface

Interface Name	Functions
IServerMgr	The message is encrypted/decrypted. It integrates encryption module and decryption module.
IClientMgr	It manages the client contacts and cancels. It manages the user and group. It manages and forwards the messages.
IDBMgr	It stores the client information. It stores the receiving and forwarding messages.
IDeviceMgr	It stores the receiving and forwarding messages by using the mobile communication devices.

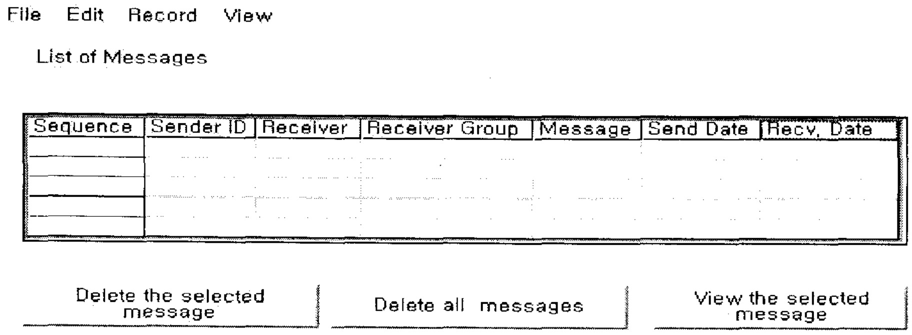
Ⅳ. Implementation

The server of the developed SMS security system is implemented on the computer with Intel Pentium Ⅳ 2GHz 256 DDR RAM, and the development tool is used of Visual Studio 6.0. And, in order to develop the client program, the Embedded Visual Studio 3.0 and Pocket PC SDK are used on the above PC. And, in order to test the program, the server program developed from the above PC is implemented and the Win CE implements the client program on the Compaq IPAQ used as the OS.

4.1 Server Implementation

When the server program is implemented, it generates the screen as shown on Fig. 3. The server manager may confirm the sender, receiver, group ID, message, sent date, received date and others related to the wait message through this screen. In addition, the server manager may delete the unnecessary messages from the database. At this time, the message displayed on the screen is encrypted that the server manager also is not able to confirm the message. Table 2 is a description on the functions of server application.

Fig. 3 Application of Server Side



Sequence	Sender ID	Receiver	Receiver Group	Message	Send Date	Recv. Date

Table 2. Description of Major Functions of Server Application

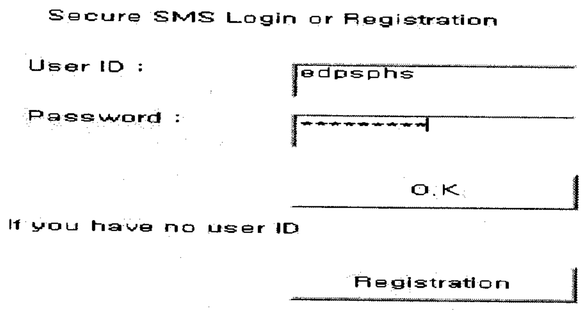
Button	Functions
Delete the selected message	Function to delete the selected message from the stand by message information list
Delete all messages	Function to delete all messages of the stand by message information list
View the selected message	Message is encrypted that the content cannot be confirmed.

4.2 Client Implementation

4.2.1 Client log in and registration function

Client application includes the functions of log in on the server system, registration, forwarding messages, receiving messages and others. Fig. 4 displays the screen of log in of the client application. Client takes on the initial works for the message preparation through this screen.

Fig. 4 Login



Secure SMS Login or Registration

User ID : edpsphs

Password : **********

O.K

If you have no user ID

Registration

4.2.2 Client message reception function

The major functions for client message reception are shown on the Table 3.

Table 3. Message reception functions

Button	Functions
Read new messages	Bring all messages forwarded to me
Refresh	Newly revise the screen
Delete message	Delete the selected message from the reception list
Delete all messages	Delete all messages
Exit	Return to the previous screen

V. Conclusion

In this study, safe message use environment is implemented by applying the security technology on the SM that is broadly used under the mobile environment today. For this purpose, it applies the security algorithm, DES, of symmetric key method, and implements the SMS. SMS is consisted of DB server module, encryption/decryption module and server interface module. And it is designed and implemented by encrypting the message prepared by the sender to store in the database of the SMS server, and perform the reception and decryption of the message by the receiving party. SMS that is developed by this study is evaluated as satisfying all sectors, such as message confidentiality, sender authentication, mobility and others when compared to the other messenger systems. The system implemented by this thesis is evaluated as applicable to many fields serviced under the mobile Internet environment.

References

1. H S. Choi, "Reports of Mobile Services 2002, Softbank Korea, pp.20-78
2. K. C. Kim, "The trend of Mobile Service", Journal of KIPS, Vol 9. No 2, pp.17~pp.23, March, 2002
3. "The survey of Mobile Service", http://www.mic.org, June, 2003
4. W. S. Choi, Y. W. Gu, "Design and Implementation of Mobile Survey System", Journal of KIPS, vol.10 no.2 pp. 317~326. 2003 . 04
5. Y. N. Go, " Implementation and Performance Analysis of Wired & Wireless Real-time Auction System based on Java 2 Platform", Journal of KIPS, vol.28 no.2 pp. 0637~0639, 2001. 10
6. S. I. Ou, J. H. Go, "Voice Portal based on SMS Authentication at CTI Module Implementation by Speech Recognition", Journal of KISS, vol.28 no.1 pp. 439 ~ 441,2001. 04
7. W. H. Lee, "Performance Evaluation of Short Message Service System based on Main-Memory DB and Disk-Resident DB" Journal of KISS,, vol.27 no.2-1 pp. 216~218, 2000. 10
8. T. H. Kim, H. K. Kang, K. J. Kang, "Implement of Multimedia Messaging Service", Journal of KISS, vol.27 no.2-3 pp. 343 ~ 345, 2000. 10
9. Cipher text", Journal of KCIE, vol.3, no.5, 2002