Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 5, Issue. 2, February 2016, pg.139 – 145

Secured Message Transaction System with Strong Security Services

Tasnova Farhana[1], Md. Iftakharul Islam Bappy[2], Sohel Chowdhury Prince[3], Ditee Yasmeen[4]

[1 2 3] B.Sc (Hons.), Department of Computer Science and Engineering, Institute of Science and Technology, National University, Bangladesh

[4]Senior Lecturer, Department of Computer Science and Engineering, Institute of Science and Technology, National University, Bangladesh

[1] farhana.nova.cse@gmail.com

[2] iftekharbappy@gmail.com

[3] sohelc21@gmail.com

[4] ditee.yasmeen@yahoo.com

Abstract: Secured message transactions are very much demanding issues for any electronic transactions system. Now a day when more and more sensitive information is stored on computers and transmitted over the Internet or other communication means. The system presented in this paper can be applied for many cryptographic applications where strong security is highly demanded. It is a set of participants and their interactions towards an efficient, effective and secured exchange of information between the participants. Hence, Public-key and Private Key cryptography techniques jointly employ to perform message transactions in any length in this regard. In this paper we present a different approach of how RSA, DES3, SHA1 and Envelop data can be applied to provide most secured message transaction system. We are using PKCS #7 standards with RSA algorithm so actually our process is divided into four parts. The first part describes the top-level type Enveloped Data, the second part describes the per-recipient information type Recipient Info, and the third and fourth parts describe the content-encryption and key-encryption processes. So we are providing strong security system than other existing system.

Keyword- Security, Cryptography, Public key, RSA, Envelop Data, DES3, SHA1.

I. INTRODUCTION

Now a day when more and more sensitive information is stored on computers and transmitted over the Internet or other communication means, we need to ensure information security and safety. Sending sensitive messages, documents and files over the Internet. Your message is totally open to interception by anyone along the way, so anybody can read your message. Once your data has been encrypted, a person cannot make sense of your data without valid key (or figuring it out).With regards to confidentiality, cryptography is used to encrypt data residing on storage devices or traveling through communication channels to ensure that any illegal access is not successful[1]. It is a way in which communications and data can be encoded to prevent disclosure of their

© 2016, IJCSMC All Rights Reserved

contents through eavesdropping or message interception, using codes and other methods, so that only certain people can see the real message. Public key cryptography uses a pair of keys to encrypt and decrypt message. Encryption is basically an indication of users' distrust of the security of the system, the owner or operator of the system, or law enforcement authorities. The RSA algorithm used to encryption and decryption process. The Rivets- Shamir- Adelman (RSA) cryptosystem is a well-known public-key encryption method that is applied to many systems for encryption and decryption.

II. RSA

RSA is an algorithm used by modern computers to encrypt and decrypt messages. It is an asymmetric cryptographic algorithm. Asymmetric means that there are two different keys. This is also called public key cryptography, because one of them can be given to everyone. The other key must be kept private. It is based on the fact that finding the factors of a integer is hard (the factoring problem). RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978[3]. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

III. HOW EXISTING RSA BASED SYSTEM WORKS

Using an encryption key (e,n), the algorithm is as follows[4]:

Represent the message as an integer between 0 and (n-1). Large messages can be broken up into a number of blocks. Each block would then be represented by an integer in the same range.

- Encrypt the message by raising it to the eth power modulo n. The result is a cipher text message C.
- To decrypt cipher text message C, raise it to another power d modulo n. The encryption key (e, n) is made public. The decryption key (d, n) is kept private by the user.

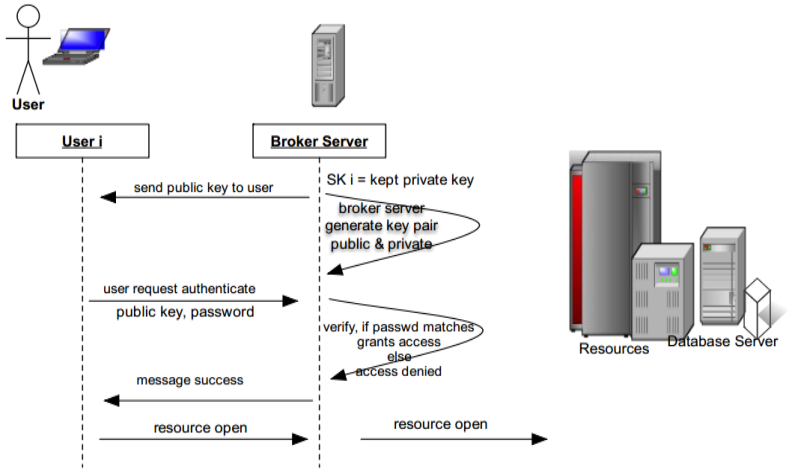

Figure 1: RSA Working Process

IV. ENVELOPED DATA

The enveloped-data content type consists of encrypted content of any type and encrypted content-encryption keys for one or more recipients. The combination of encrypted content and encrypted content-encryption key for a recipient is a "digital envelope" for that recipient [10]. Any type of content can be enveloped for any number of recipients in parallel. It is expected that the typical application of the enveloped-data content type will be to represent one or more recipients' digital envelopes on content of the data, digested-data, or signed-data content types.

© 2016, IJCSMC All Rights Reserved

The process by which enveloped data is constructed involves the following steps:

1. A content-encryption key for a particular content-encryption algorithm is generated at random.
2. For each recipient, the content-encryption key is encrypted with the recipient's public key.
3. For each recipient, the encrypted content- encryption key and other recipient-specific information are collected into a Recipient Info value.
4. The content is encrypted with the content-encryption key.
5. The Recipient Info values for all the recipients are collected together with the encrypted content into an Enveloped Data value.

A recipient opens the envelope by decrypting the one of the encrypted content-encryption keys with the recipient's private key and decrypting the encrypted content with the recovered content-encryption key. The recipient's private key is referenced by an issuer distinguished name and an issuer-specific serial number that uniquely identify the certificate for the corresponding public key. This section is divided into four parts. The first part describes the top-level type EnvelopedData, the second part describes the per-recipient information type RecipientInfo, and the third and fourth parts describe the content-encryption and key-encryption processes. This content type is not compatible with Privacy-Enhanced Mail (although some processes it defines are compatible with their PEM counterparts), since Privacy-Enhanced Mail always involves digital signatures, never digital envelopes alone.

V. DES3

In cryptography, Triple DES (DES3) is the common name for the Triple Data Encryption Algorithm (TDEA or Triple DEA) symmetric-key block cipher, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. The original DES cipher's key size of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made brute-force attacks feasible [8].

Triple DES takes three 64-bit keys, for an overall key length of 192 bits. In Stealth, you simply type in the entire 192-bit (24 character) key rather than entering each of the three keys individually. The triple DES DLL then breaks the user-provided key into three sub keys, padding the keys if necessary so they are each 64 bits ling. The procedure for encryption is exactly the same as regular DES, but it is repeated three times, hence the name DES3. The data is encrypted with the first key, decrypted with the second key, and finally encrypted again with the third key. Triple DES runs three times slower than DES, but is much more secure if used properly. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Although the significant bit in in each byte is a parity bit, and should be set so that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most significant bits of each byte are used, resulting in a key length of 56 bits. This means that the effective key strength for Triple DES is actually 168 bits because of the three keys contains 8 parity bits that are not used during the encryption process [9].

VI. PROPOSED SYSTEM ARCHITECTURE

Security mechanisms are only effective when used correctly. Ensuring comprehensive network security visibility is not easy task. So we are concerning on Secure Message Transaction by using private key and public key with PKCS#7 Standards. Public Key Cryptography [2] can therefore achieve Confidentiality. The Public and Private Key pair comprise of two uniquely related cryptographic keys. In our Encryption technique, if new user is to send the file with the private key, in this file is saved in encrypted format in table. So this private information is not known to any other user. It provides a better security to our application. Also we have provided the decryption technique for the user to read the information is correct or not. This data is known to only that user who logged in the system. The user to send the file in encrypted format using RSA algorithm and then that file is stored in our database with unique private key and public key. Then the authorized download user only to view that private key after to access that file using the private key.

© 2016, IJCSMC All Rights Reserved

As we are using PKCS #7 [7] standards with RSA algorithm so actually our process is divided into four parts. The first part describes the top-level type Enveloped Data, the second part describes the per-recipient information type Recipient Info, and the third and fourth parts describe the content-encryption and key-encryption processes.

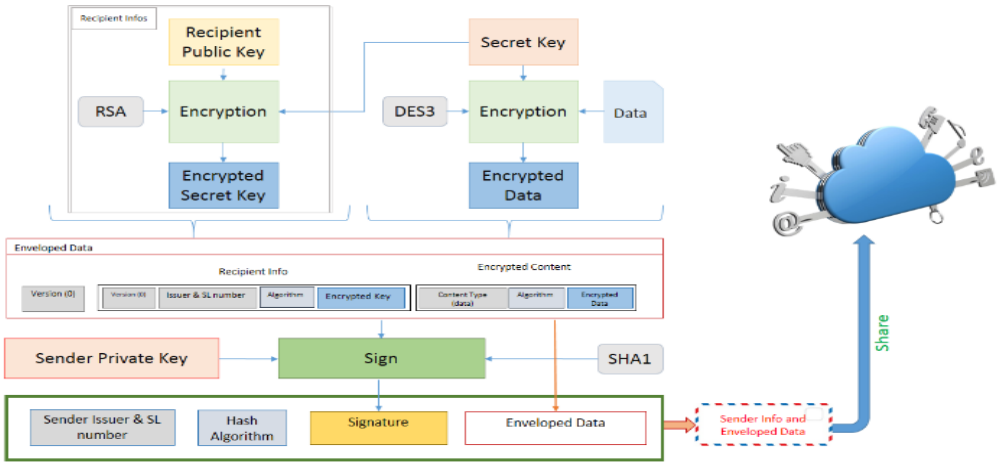

Figure 2: Prepare Secure Data and Share

Messages are encrypted with the secret key. The different secret key is generated for every individual message. Triple Data Encryption Standard (*DES3*) algorithm is used to encrypt a message. An encrypted message decrypt with the same secret key and algorithm. In the message sharing process, secret key (that is used to encrypt messages) encrypt with recipient public key generated by RSA. An envelope data, prepare with encrypted secret key, encrypted message and recipient information. A digital signature which is generated by using SHA1 adds to the enveloped data and share it to the specific recipient. Enveloped data share via Server Message Block (SMB).

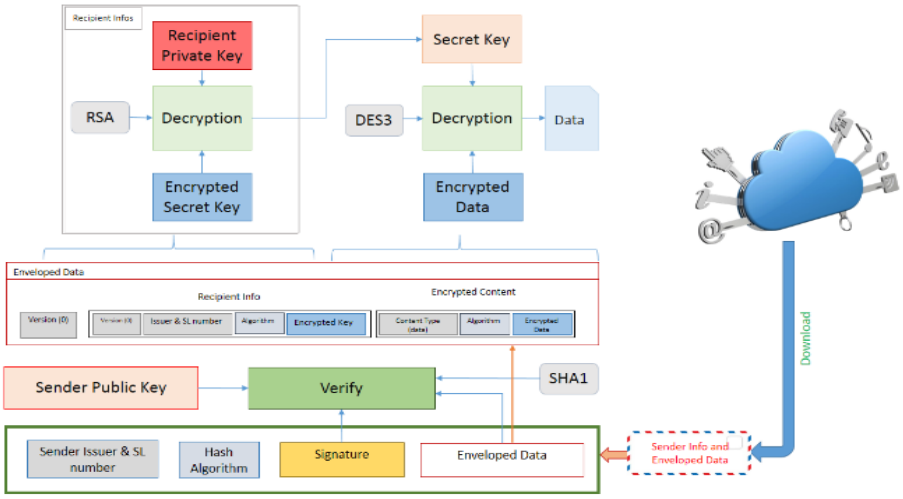

Figure 3: Enveloped Data Download and Parse

The specific recipient can view all the shared message. But recipient able to download if shared message contains his/her information. In this case, the system verify the signature and check proper recipient information using SHA1 algorithm. After completion of the download process, encrypted secret key is decrypted with recipient private key generated by RSA. Then by using the DES3 algorithm decrypt the encrypted message with this secret key and able to view the message.

© 2016, IJCSMC All Rights Reserved

VII. IMPLEMENTATION OF THE PROPOSED SYSTEM

We have used Swing (Java) for design user interface (UI). Swing is used to build a Java program with a graphical user interface (GUI). Swing is part of Java Foundation Class (JFC). Swing is not a replacement for Abstract Window Toolkit (AWT), actually it is built on top of the core AWT libraries to provide a more sophisticated set of GUI components.

The following are some of the Graphical Interface of the proposed Secured Message Transactions:-

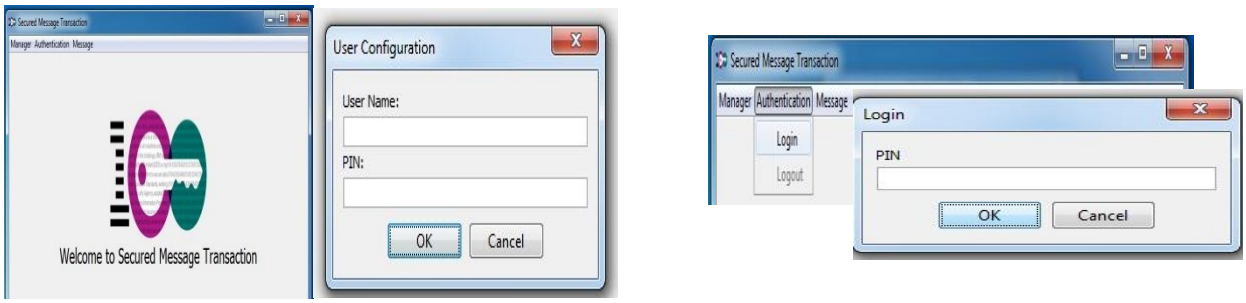

Figure 4: User Configurations and Login

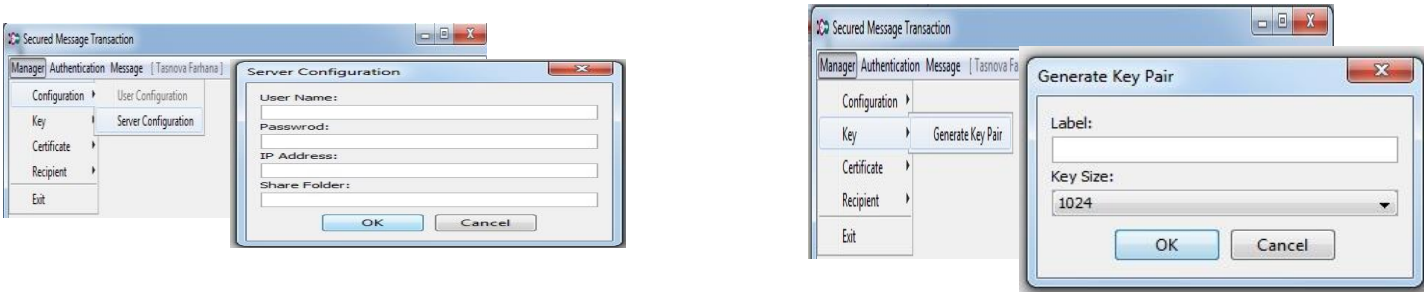

Figure 5: Server Configuration and Key Pair Generation

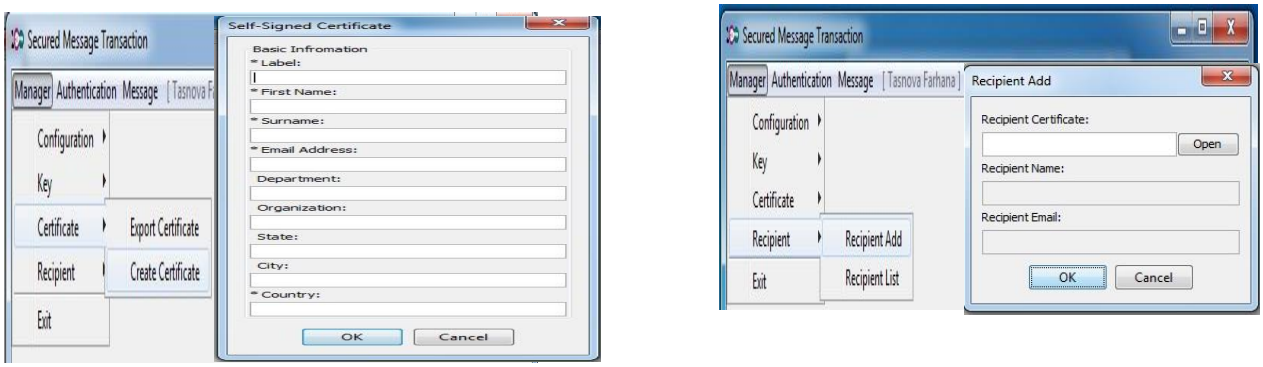

Figure 6: Certificate Creation and Recipient Addition

© 2016, IJCSMC All Rights Reserved

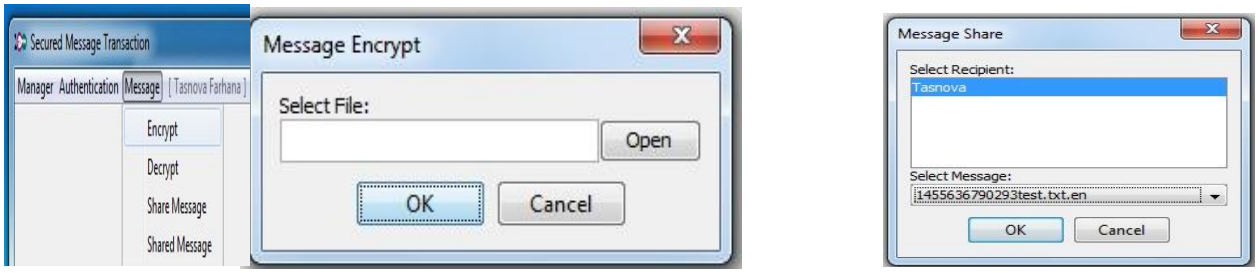

Figure 7: Message Encryption and Sharing

Figure 8: Shared Message Receive and Download Process

VIII. COMPARISON OF PROPOSED SYSTEM WITH CONVENTIONAL SYSTEM

The comparison between proposed Secured Message Transaction System with Strong Security Services with conventional system is given below.

Table 1: Comparison of Proposed System with Conventional System

System	User Authentication	Data Confidentiality	Data Integrity	Digital Signature	Digital Certificate
Conventional	Yes	Yes	No	Yes	No
Proposed	Yes	Yes	Yes	Yes	Yes

IX. CONCLUSION

Secured Message Transactions are very much desirable for many reasons. The Internet as an open forum has created some security problems like confidentiality, integrity, and authentication. In this paper, conventional RSA, Envelop Data, DES3 and SHA1 based message transaction techniques, methods, and related issues are studied, analyzed and presented. The fundamental security service issues - confidentiality, authentication, integrity checking, non-repudiation and availability are discussed. The technique presented here may applicable in secured electronic communications for many cryptographic applications. Although the processing overhead of the proposed system is slightly increased but the system provides strong security services in comparison to others. In future we will improve this system with less complexity and better efficiency.

© 2016, IJCSMC All Rights Reserved

REFERENCES

[1] William stallings, Cryptography and Network Security, Fourth Edition
[2] ANSI X9.42, Public Key Cryptography for the Financial Services Industry: Agreement of Symmetric Keys Using Discrete Logarithm Cryptography, January 2003.
[3] Public-Key Cryptography Standards (PKCS), RSA Laboratories.
[4] Kaliski, B. and M. Robshaw. "The Secure Use of RSA." RSA Laboratories' CryptoBytes 1, no. 3 (Autumn 1995).
[5] Menezes, A., P. van Oorschot, and S. Vanstone. Handbook of Applied Cryptography. Boca Raton: CRC Press, 1997.
[6] Lloyd, Steve (September 2002). Understanding Certification Path Construction (PDF). PKI Forum.
[7] PKCS #7 Cryptographic Messaging Syntax Concepts
[8] https://en.wikipedia.org/wiki/Triple_DES
[9] http://www.vocal.com/cryptography/tdes/
[10] https://en.wikipedia.org/wiki/Envelop_DATA

© 2016, IJCSMC All Rights Reserved