ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

Security of File through Splitting and Hybrid Encryption Mechanism

Vishu Sharma [1], Meenakshi Sharma [2]

Student, CSE, SSCET, Badhani, India [1]

Associate Professor, Ph.D (Pursuing), CSE, SSCET, Badhani, India [2]

Abstract: The rapid growth of internet and networks applications has given rise to many data security issues. Encryption algorithm plays a crucial role in information security systems. This paper presents the hybrid encryption scheme which combines the fast encryption speed of symmetric algorithm (Blowfish) with the security of asymmetric cipher algorithm (SRNN). The proposed approach includes file splitting and merging mechanism along with hybrid encryption where each slice is encrypted by its corresponding key.

Keywords: Hybrid cryptosystem, File Splitting, SRNN, RSA, Blowfish.

I. INTRODUCTION

A network is a series of individual elements transmitting and receiving various data. Whenever sensitive or confidential information is transmitted, there is a possibility of an unauthorized third party "eavesdropping" on a transmission and learning the contents of the sensitive message. Cryptography is the process of transmitting a message into form which is unreadable to everyone except the intended recipient. This is typically done with the help of keys. The original text is converted into scramble equivalent called cipher text and the process is called encryption and the reverse is called decryption. Two types of cryptographic schemes are available on the basis of key.

A. Symmetric Key Cryptography: The cryptographic scheme which uses a single common key for enciphering and deciphering the message. The key should be distributed before transmission between entities. The strength of the symmetric key algorithm depends on the size of key being used.

B. Asymmetric Key Cryptography: The cryptographic scheme which uses two different keys for encryption and decryption. For the encryption process, public key is used whereas for decryption, private key is used. Public key is known to everyone and private key is known only to the intended user. So, there is no need of distributing the keys earlier to the transmission. Considering the computational processing power, asymmetric encryption techniques are almost 1000 times slower than symmetric techniques

II. HYBRID CRYPTOSYSTEM

The term "hybrid" [1] is borrowed from natural sciences, it means "crossbreed". In cryptography it refers to the combination of symmetric and asymmetric algorithms and thus, serves the benefits of both symmetric and asymmetric cryptosystems as it is more secure as compared to symmetric cryptosystems and faster in comparison to asymmetric cryptosystems. The ISO/LEC standardization committee suggests that hybrid cryptosystem can be defined as the branch of asymmetric cryptography that makes use of convenient symmetric techniques to remove some of the problems inherent in normal asymmetric cryptosystem.

A. Blowfish

Bruce Schenier[2], one of the world's leading cryptologists, designed the Blowfish algorithm and made it available in the public domain. Blowfish is a variable length key,64-bit block cipher. The algorithm was first introduced in 1993, and has not been cracked yet. It can be optimized in hardware applications due to its compactness.

The algorithm consists of two parts: a key-expansion converts a key of at most 448 bits into several sub-key arrays totalling 4168 bytes. Data encryption occurs via 16-round (commonly) network. Each of the 16 rounds consists of a key-dependent permutation, and a key and data dependent substitution. All XORs and additions operations are performed on 32-bit words.

The additional operations include four indexed array data lookups per round.

Bruce Schenier demonstrated that differential cryptanalysis on Blowfish is possible either against a reduced number of rounds or with the piece of information which describes the F-function. However, the boxes are well designed to resist to on an attacks while they are randomly generated in Blowfish. As we know, there is no successful cryptanalysis against Blowfish since 1993.

The power of the Blowfish algorithm relies on its sub-key generation and its encryption. It is one of the fastest symmetric algorithms among other symmetric algorithms. Among the various symmetric algorithms like AES, DES etc., Blowfish is superior in terms of throughput, processing time and power consumption.

The working is explained in the following figure1.

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

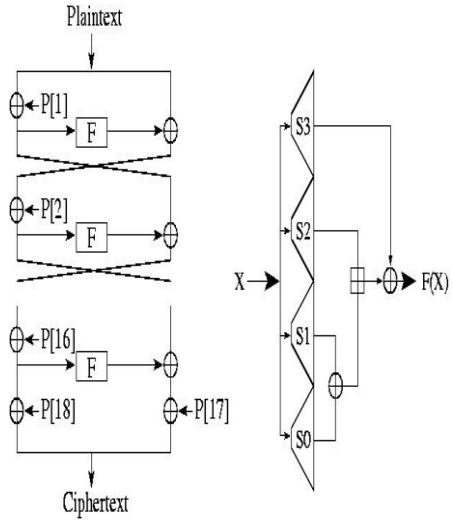

Fig.1 Blowfish Algorithm [2]

B. RSA

The Rivest-Shamir-Adleman(RSA) [3] cryptosystem is one of the best known public key cryptosystems employed for digital signatures or encryption of data blocks. RSA uses a variable size encryption block and a variable size key. The key-pair [4] is derived from a very large number n, where n is the product of two prime numbers chosen according to special rules. The prime numbers may be 100 or more digits in length each, yielding n with roughly twice as many digits as the prime factors.The public key includes n and a derivative of one of the factors of n such that an attacker cannot determine the prime factors of n (and, and therefore the private key) from this information alone and this key feature make RSA algorithm so secure. RSA's safety is due to the difficulty in factoring large prime numbers. RSA algorithm has some important parameters affecting its level of security and speed. Increasing the modulus length increases the length of private key and hence it will be difficult to decrypt cipher without the knowledge of the decryption key. The security of RSA increases when bit length of RSA is increased to 2048 bits but it suffers on the aspect of speed in encryption and decryption. To overcome thi, natural numbers are used in pair of keys in addition to existing parameters of RSA which gives the good balance between speed and security. This modification lead to algorithm named SRNN (Short Range Natural Number).

C.SRNN:

The SRNN [3] algorithm is a public key cryptography algorithm which is similar to RSA with some modifications. In this algorithm we have extremely large number that has two prime factors (similar to RSA). In addition, two short range natural numbers have been used in pairs of keys. This modification increases the security of cryptosystem. So its name is short range natural number public key algorithm.

SRNN Key Generation.Algorithm [3] for key generation is as follows:

i) Generate two large random primes p and q , such that their product n= p x q .

ii) Compute phi where, phi = (p-1)(q-1)

iii) Choose an integer , 1<e<phi such that, gcd(e,phi) = 1

iv) Compute the secret d, 1<d<phi, such that, (e x d)mod phi=1

v) Pick a short range natural number u, such that, u< phi-1

vi) Pick another short range natural number a, such that, phi> a > u , and compute u^a

vii) Find d such that, e * d mod ((p-1)*(q-1)) = 1

The public key is (n,e,u^a) .The private key is (d,a,u).

The encryption is performed using equation 1.

$$c = (mu^a)^e \bmod n \qquad (1)$$

where,

c is the cipher text, m is the plain text.

The decryption is performed using the equation 2

$$m = (v^e c)^d \bmod n \qquad (2)$$

where,

v= u^(phi-a) mod n.

III.PROPOSED SYSTEM

This software involves cryptographic enciphering and deciphering along with File splitting and merging mechanism. In this approach [5], a file which has secret data is sliced into desired number of pieces upon user's specification and then the cryptographic encryption phase is carried out system. The hybrid algorithm is used for cryptographic enciphering and deciphering. The modified version of blowfish is used in hybrid algorithm for encrypting decrypting files.Original function F is defined as follows.

F(X) = ((S1 + S2 mod 2^32) XOR S3) + S4 mod 2^32

Instead, the F-Function is modified by replacing 2 addition operations as XOR Operations . Thus the modified F-Function is written as,

F(X) = ((S1 XOR S2 mod 2^32) + (S3 XOR S4 mod 2^32))

This modification leads to simultaneous execution of two XOR operations. In this way the security is further enhanced.

A.Encryption Phase

The input file is first sliced into n slices upon user specification. Then the each slice is encrypted by password given by the user at the time of encryption for each slice. The password serves as blowfish key which is used to encrypt the file slice. Each password is further encrypted by SRNN public key. Since symmetric

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

algorithm is faster than asymmetric algorithm, so file slices are encrypted by Blowfish (symmetric algorithm) and small sized key is encrypted using SRNN (asymmetric algorithm). At the end of encryption phase, we are left with n ciphers and corresponding n public, private and encrypted keys. The n ciphers and n encrypted keys are transmitted to the reception side which makes the file infeasible to breach and less suspicious to get to know that hybrid crypto schemes are being employed.

Steps at encryption phase. The steps at encryption phase are as follows:

i) The input file is sliced into n slices upon user specification

ii) Each slice is encrypted with the corresponding password given by the user using Blowfish algorithm.

iii) Each password which served as Blowfish key is encrypted by SRNN.

Where, k1, k2, …, kn are the blowfish keys.

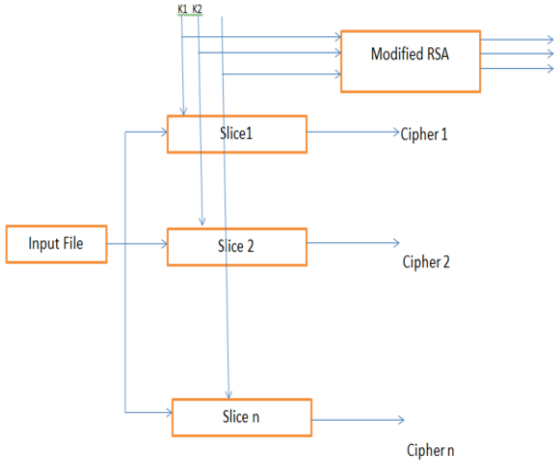

Fig. 1 Encryption Phase

B.Decryption Phase

At the receiver end, firstly the n encrypted keys are decrypted by the corresponding n private keys. After decryption we are left with Blowfish keys which are served to decrypt n slices. At the end, the n slices are merged to get the original file.

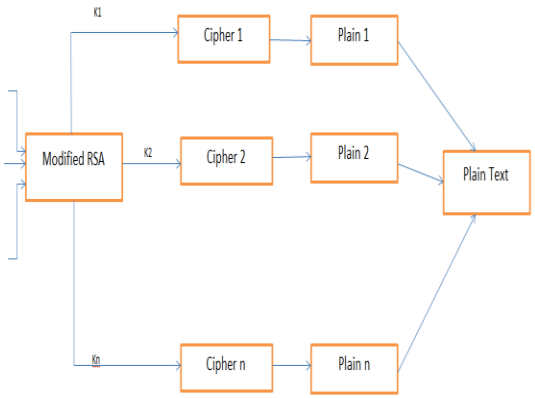

Fig. 2 Decryption Phase

In this way, this proposed scheme of hybrid encryption becomes impossible to breach. The advantage of file splitting and merging is that every slice is encrypted with a different key. If the eavesdropper manages to find the key of one slice, still the remaining file is hidden from him.Ek1,Ek2, …, Ekn are the encrypted keys shown in figure (Fig. 3).

IV. DESIGN AND IMPLEMENTATION

For the purpose of simulating the file splitting and hybrid encryption scheme, we used Java which is well known for its platform independency and better GUI features. Various libraries have been used like javax.crypto, java.security to implement hybrid encryption scheme.

RESULTS

The following figures represent the implementation of the proposed scheme in Java. This implementation takes input as file and splits the file into n number of slices on the basis of user specification and finally encrypts the file slices accordingly. In decryption phase, the encrypted file slices are firstly decrypted and then merged to give the final output as a single file.

Encryption Frame

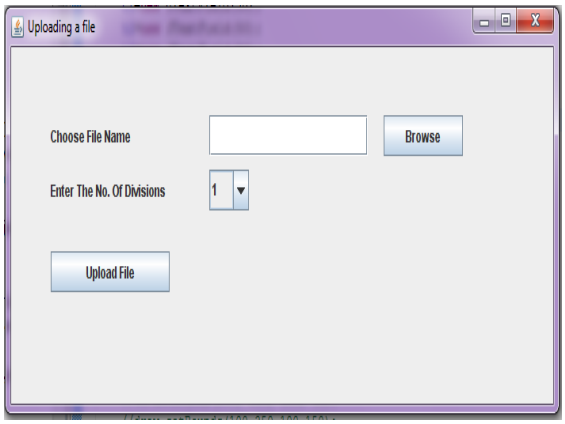

Fig.4 File Splitting

The above frame(Fig. 4) lets the user to specify the filename along with the number of slices in which the user wishes to split the file.

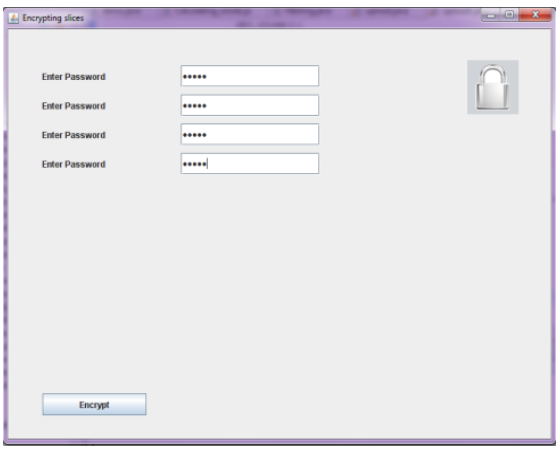

Fig.5 Encryption Frame

ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 9, September 2015

This frame(Fig.5) provides an interface for the user to specify the passwords (Blowfish key) for each file slice which will encrypt the corresponding file slices using Blowfish algorithm.

Decryption Frame

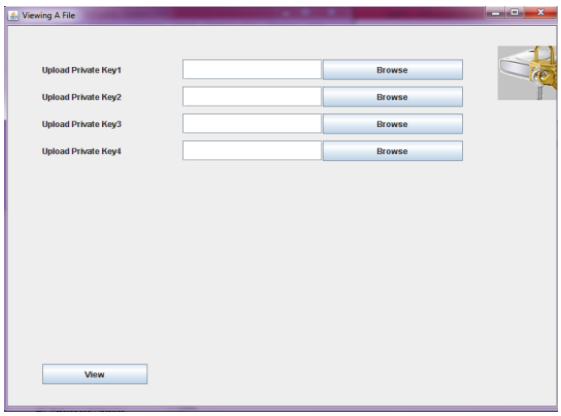

Fig.6 Decryption Frame

Here(in Fig.6), the user need to provide SRNN private key which will decrypt the encrypted Blowfish keys and then the decrypted Blowfish keys decrypts the corresponding file slices.The decrypted files slices are finally merged to give the final output(Fig. 7).

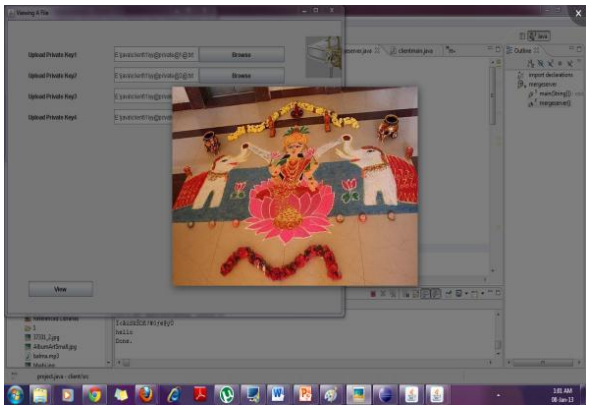

Fig.7 Decrypted File

Algorithm Vs. Time

The approximate time taken when tested on file size of 36 bytes and SRNN of 256 bits key is shown in the graph.

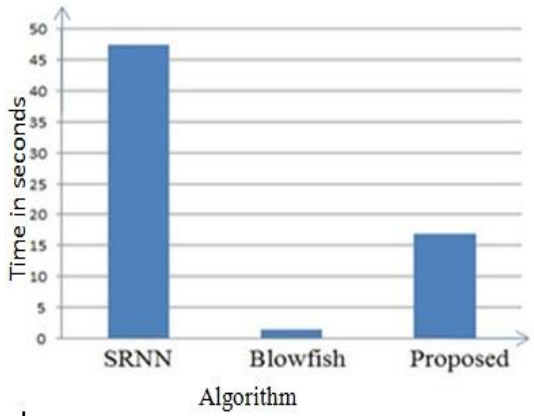

Fig .8 Algorithm Versus Time

The graph demonstrates the relationship between the various algorithms and the respective time taken by them to encrypt and decrypt the data. From the results, it can be concluded that the proposed hybrid scheme has a good speed in contrast to SRNN Algorithm, but relatively less than Blowfish algorithm.The results are tested for image and audio files.

V. BENEFITS OF PROPOSED MODEL

The proposed model is liable to meet the required security needs of data. Blowfish used for the encryption of file slices takes minimum time and has maximum throughput for encryption and decryption from other symmetric algorithms. Modified RSA (SRNN) has increased security than RSA. The idea of splitting and merging adds on to meet the principle of data security. The hybrid approach makes the server more secure and thus, helps the Providers to fetch more trust of their users. For data security and privacy protection issues, the fundamental challenge of separation of sensitive data and access control is fulfilled.

The various benefits are as summarized:

- The public key cryptography used helps to facilitate authorization of user for each file.
- The file splitting and merging makes the model unfeasible to get attacked.

VI. CONCLUSION

The combination of hybrid encryption along with file splitting and merging mechanism makes the proposed algorithm better in terms of speed and security. It provides a high end datasecurity while transmission over any insecure medium. The proposed scheme is more secure than blowfish and also better than SRNN in terms of both time and security as. The hybrid approach serves agood purpose where security needs are prominent. It can be further improved by increasing its throughput compared to symmetric algorithm.

REFERENCES

[1] M.AyoubKhan and Y.P Singh (2005), 'On the security of joint Signature and Hybrid', Proc. of IEEE 7thMalaysia International Conference on Communication,vol.1.
[2] TingyuanNie andTengZhang (2009), 'A study of DES and Blowfish encryption algorithm',TENCON 2009 –2009 IEEE Region 10 Conference, pp.1-4.
[3] Jitendra Singh Yadavet al.(Aug 2012), 'Modified RSA Public Key Cryptosystem Using Short Range Natural Number Algorithm', International Journal of Advanced Research in Computer Science and Software Engineering,vol.2.
[4] Sattar J Aboudet al. (April 2008), 'An Efficient RSA Public Key Encryption Scheme',Proc. of IEEE Fifth International Conference on Information Technology NewGenerations,pp127-130.
[5] Manikandan.Get al.(Jan 2012), "A modified cryptographic scheme enhancing data",Journal of Theoretical and Applied InformationTechnology, vol. 35 no. 2.