JIT DYNAMIC CRYPTOSYSTEM

Anntinu.T.J[1], Sherly.K.K[2]

[1]*PG Student, Department of Computer Science, Toc H Institute of Science & Technology, Kerala, India*
[2]*Associate Professor, Department of Information Technology, Toc H Institute of Science & Technology, Kerala, India*

Abstract

Conventional cryptography systems use a static key or a pair of keys for the encryption and decryption process. It is known from the study of the authentication method that the dynamic 2-factor based methods are more secure than the static parameter based authentication method. Also in the static key based encryption technique the entire security is based on the secrecy of the key used. Since the computational power of computers are increasing the key length is also increasing, which in turn force us to record it somewhere which makes it vulnerable. Here arises the need for a dynamic 2-factor based encryption technique in which the keys are generated based on Just in Time (JIT) principle for the encryption and decryption process. Here we utilize the property of RSA method for the generation of the JIT dynamic key for encryption and decryption process using a mobile agent in Client-Server architecture. In this system both the encryption key and decryption key is generated by the mobile agent in association with the server. A random number generated in both mobile agent and the server using time and a secret parameter as its seed makes the JIT key different for different users at same time and different JIT key for same user at different time. This method provides dynamic nature to the key and protects our system from key compromise. This method also provides an inborn authentication scheme for the users in the system. In conventional RSA system there is a chance for key compromise by brute force attack, but in this system the RSA key changes for every encryption and decryption without the overhead of key generation which make the system reliable and robust.

Keywords: *2-FACTOR, JIT, RSA, Client-Server, Dynamic.*

----------***----------

1. INTRODUCTION

The growth of information technology has increased the value of data. Data security is of utmost importance in today's E-world. Confidentiality of data can be achieved by using cryptography and steganography. Cryptography is the dexterity of secret writing. The major hotspot in today's research world is secure communication through insecure channel like internet. Internet plays a major role in data communication in this digital world. The development in internet technology and increase in the computational power of computer are causing challenges to data security. Last but not the least, we should also consider the fact that we are mainly relying on encryption technique certified by NSA who is also behind the clandestine prism project.

Usually, the security of an encryption method is determined based on the complexity of its mathematical operation. But we are forgetting the fact that the security of an encryption method is actually depending on the secrecy of encryption key. One time key is a good method for increasing the security of encrypted data but the key exchange will be always an overhead. Many dynamic encryption techniques have been proposed in order to increase the security but still the key or key pair for encryption and decryption will be the same. So security of the cipher data is directly related to the secrecy of key. For improving the security it is better to change key with respect to time. But the limitation of this approach is that same or pair key is necessary for decryption. In our method we are reconfiguring RSA encryption algorithm in client-server model in such a way that the key for encryption and decryption will be generated using Just in Time(JIT) methodology and the key for decryption process will be different at different time for same cipher text. So the security of key is achieved using a mobile key generator. Here the system is similar to that of 2-Factor authentication method.

The remaining portion of the paper is organized as follows. In section 2, the existing literatures are analyzed. The proposed system and its working are discussed in section 3 and 4.Section 5 deals with the analysis part and finally conclusion is made in section 6.

2. RELATED WORKS

Many works have been done in the field of authentication using 2-Factor authentication method which clearly point out the security improvements. But so far no works were done in the field of 2-Factor encryption and JIT key generator. There are many papers exploring the use of dynamic encryption. In[1] Fabian et al proposes a new method in which dynamic key will be generated for AES encryption using a Pseudo-Random Number Generator(PRNG) and using a hash function from an image. This helped us to utilize the dynamic key generation from PRNG.

In our method for generating the JIT key we are using a random number generator. Cryptographic PRNG of[2] can be

reconfigured for our need. In [2] chalama reddy et al proposed cryptographic PRNG using blow fish encryption algorithm. The advantage of this method is that we can generate a random number of infinite length by using a 64 bit plain text and variable length key. In our method we are utilizing this PRNG in our server and mobile key generator side for generating JIT key.

For our system we are utilizing the exponential property of RSA encryption algorithm. It is this property through which we are achieving the half encryption. In [3] improvements of RSA key generation are proposed through which we can achieve better security to our system. In [3] instead of two prime numbers we are utilizing three prime numbers for key generation which will further increase the complexity of factorization.

3. THE PROPOSED METHOD

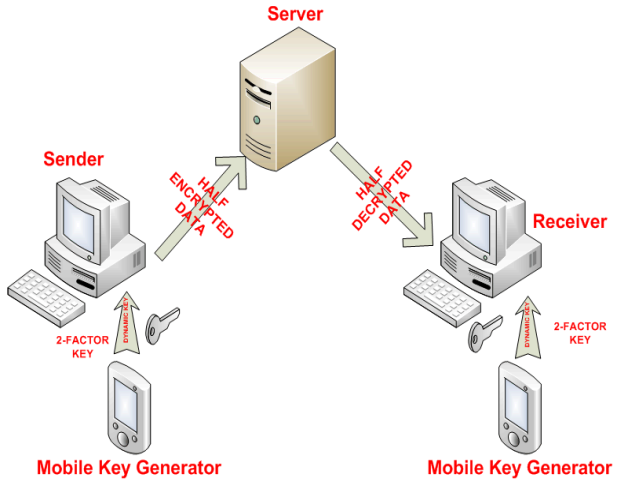

Fig -1: Abstract representation of proposed system

The key logic in our system is in RSA half encryption. We achieve a high degree of security for information with help of this two factor encryption. Here the RSA algorithm is implemented in two stages,

1. In the client part the Intermediate text is encrypted using {Public key[receivers] minus Random number [at time t1]}. The Mobile agent generates the random number using synchronized time seed and Secret UID.

2. In the server part the half encrypted message is encrypted using the random number [at time t1] generated using the synchronized time seed by the server.

The fully encrypted cipher text is stored in the server's database for further use. The static key is the public key-private key pair of RSA and the dynamic factor is generated by the PRNG using time and secret User ID. The decryption process is also implemented in two stages of RSA,

1. In the server part half decryption is achieved using the random number [at time t2] generated using the synchronous time seed by the server.

2. In the client part the half decrypted data is again decrypted by using {Private key [receiver]-Random number [at time t2]} generated by the mobile agent having synchronous time seed.

Our proposed system consists of several sub systems. These sub systems are discussed below,

3.1 Random Number Generator

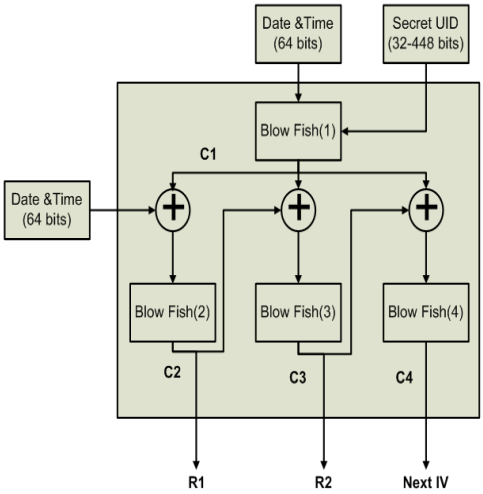

Fig -2: Crypto Based Pseudo Random Number Generator (CBSRNG)

The random number generator used in our system is crypto based pseudo- random number generator[2] with blow fish algorithm. Here we are reconfiguring [2] according to our requirements. In our method we are using date and time together with a secret user id as the seed to the crypto based pseudo- random number generator (CBPRNG). Here the 64 bit date and time act as the plain text for encryption and secret user id(SUID) act as the key with variable size of 32-448 bits. The results provided by the CBPRNG were quiet promising. We are using this random number generator for both the mobile key generator and server. For generating same random number at both ends the seed should be same. The SUID is shared with the server by the mobile key generator at the time of registration. Then at the time of encryption the mobile key generator interact with the server and select a common time seed.

3.2 RSA Key Generation & Encryption-Decryption Process

For key generation we are using [3] in which they are using two prime number for key generation. But we are using three prime number for key generation which increases security of the system. Using [3] the complexity of factorization also increases.

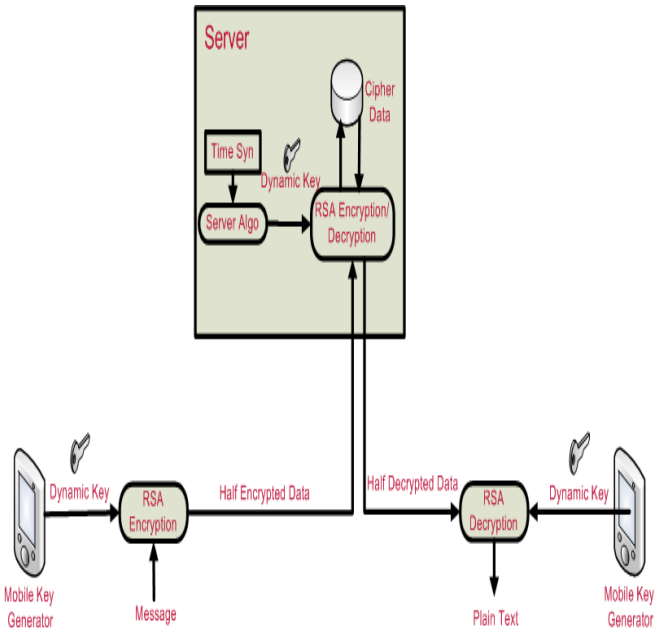

Fig -3: Functional diagram of proposed system

3.2.1 RSA Key Generation Steps:

(a) Choose three distinct prime numbers p, q and s.
(b) Find n such that n = p*q*s. n will be used as the modulus for both the public and private keys.
(c) Find the Phi of n, ϕ (n) = (p-1)(q-1)(s-1).
(d) Choose an e such that 1 < e < ϕ (n), and such that e and ϕ (n) share no Divisors other than 1 (e and ϕ (n) are relatively prime). e is kept as the public key exponent.
(e) Determine d (using modular arithmetic) which satisfies the congruence relation .d*e ≡ 1 (mod ϕ (n)).

3.2.2 Encryption & Decryption

The key idea in our system is half encryption/decryption for achieving the two factor encryption. It is achieved by utilizing the property of RSA encryption algorithm. The mathematical operation involved in RSA is exponential operation, M^e(mod n) & C^d(mod n). The half encryption is possible in RSA due to properties of exponential and modular arithmetic.

$$C=M^e \pmod n \equiv (M^{e1} \pmod n)^{e2}) \bmod n \text{ ----------(1)}$$

$$M=C^d \pmod n \equiv (C^{d1} \pmod n)^{d2}) \bmod n \text{ ----------(2)}$$

Where,

$$e= e1+e2 \quad (3)$$

$$d=d1+d2 \quad (4)$$

In our method in the sender side e1 is the Receiver's public key minus Random number(Ra) and e2 is Random number(Ra). ie, e= (Pu-Ra) + Ra = Pu. So in effect after the two half encryption the total process is equivalent to encryption with public key of receiver. Likewise in the receiver side d1 is the Receiver's private key minus Random number(Rb) and d2 is Random number(Rb). ie, in effect d= (Pr-Rb) + Rb = Pr. So in effect after the two half decryption the total process is equivalent to decryption with private key of receiver.

The system consists of four parts. They are,

1. Sender: The function of the sender is to perform half encryption using the part key(half encryption /decryption key generated in mobile key generator or server) and sending it to the server.
2. Mobile key generator: Mobile key generator generates the part key for encryption & decryption. For the part key generation process, it interacts with the server for date and time synchronization and by using this synchronized date and time and Secret user ID as the seed it generates the random number. By subtracting this random number from receiver's public key it generates part key for encryption and by subtracting from receivers private key it generates the part key for decryption. The mobile key generator also generates the RSA key pair and enrolls the user with the system. The public key, user details & SUID is registered with the server at the time of enrollment process.
3. Server: The server performs half encryption and half decryption by using the random number generated using synchronized date and time and Secret user ID as seed. It also stores the full encrypted file for serving users request.
4. Receiver: The receiver requests the encrypted data from the server and performs the completion of decryption process by using the part key generated by the mobile key generator.

4. WORKING

The system can be explained with the help of sample data used in the Fig-4.

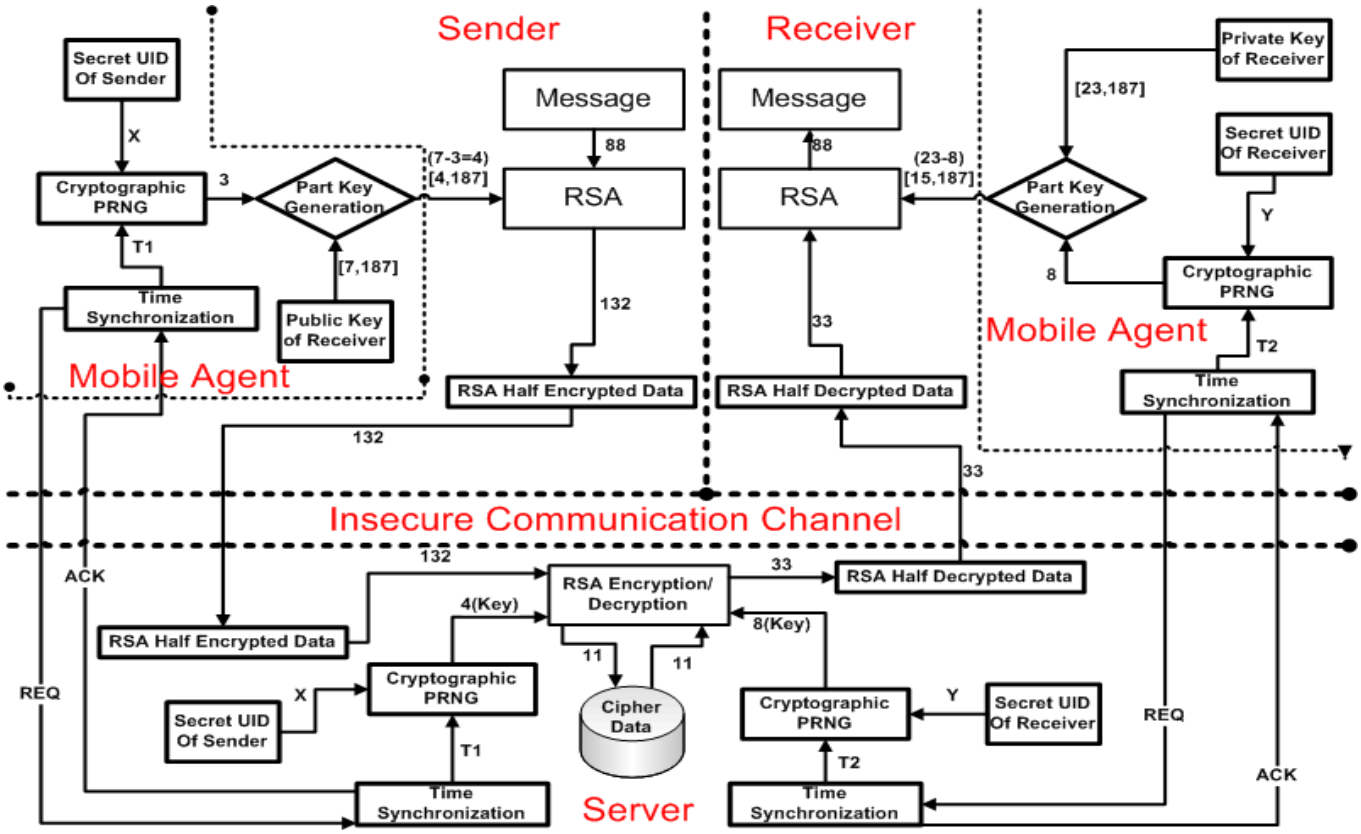

Fig -4: Working with Sample data.

4.1 Algorithm

4.1.1 Sender

1. The message for encryption is given as input into the RSA module.
2. The time synchronization module of the mobile agent interacts with the time synchronization module of the server and agrees upon a common time. The cryptographic PRNG in server and Mobile Agent generate a random number using time(T1) and Secret UID of sender as seed.
3. Encryption key for sender is generated by subtracting the random number produced by PRNG from the Public key of the receiver. The data is then half encrypted and send to the server.
4. The RSA encryption process is completed in the server using the random number as key and the result is stored in the database for future use.

4.1.2 Receiver

1. The receiver will request for the file along with a time synchronization request by the Mobile agent.
2. The data from the database will be half decrypted using the random number generated by PRNG using time(T2) and Secret UID of the receiver. This half decrypted data will be send to the receiver.
3. In the receiver side, the decryption is done using the key obtained by subtracting the random number from the private key of the receiver.
4. Finally, the plain message will be returned.

In the Fig-4 the inputs and outputs along with the intermediate result are shown. For better understanding simple input is given. In the system we can see that the encrypted data in the insecure communication channel is different for the same message, minimizing the chances for external attack.

5. ANALYSIS

In our proposed system, the hacker can access the file when it is being transmitted through the network. The data that is send to the server is not completely encrypted so the data won't have the characteristic of RSA encryption. Also the same property exists for the sending process from the server. Here we can also see that the data send from the server to receiver and from the sender to server is entirely different. Also our method will provide authenticity and non repudiation as an inborn feature. Here the encryption key and decryption key will be generated only at the time of need so one time

compromise will not affect the security of key pair and the system. Our system will provide better security than the currently exiting system. One of the major disadvantages of our system is time and space complexity.

6. CONCLUSIONS

Maintaining security is becoming more and more challenging with time. In the field of cryptography, static key encryption is currently used resulting in decrease of security with time. The current problem in the field of cryptography is the need for changing the encryption key or key pair periodically. It is essential in order to ensure confidentiality. In this paper we are proposing a new dynamic encryption method in which both encryption and decryption key change with respect to time. Here a mobile key generator is used to generate dynamically changing key. Our method will provide authenticity together with non repudiation as an inborn feature. In this paper we are proposing a new approach to the cryptographic world known as "Two Factor Cryptography". Here both encryption and decryption key is generated only at the time of need generally known as Just in Time (JIT) key generation. Here this approach is possible due to the exponential feature of RSA method. Here the possibility of key compromise will reduce since the encryption key is different from decryption key and changes with time. Hence, in our proposed system the security is not compromised with time.

REFERENCES

[1]. Septimiu Fabian Mare, Mircea Vladutiu and Lucian Prodan,"Secret data communication system using Steganography, AES and RSA",2011 IEEE 17th International Symposium for Design and Technology in Electronic Packaging (SIITME).

[2]. T.Chalama Reddy 1, Dr.R.Seshadri2,"New Design of Crypto- Based Pseudo random number generator (CBPRNG) using BLOW FISH cipher",International Journal on Computer Science and Engineering (IJCSE), Vol. 5 No. 06 Jun 2013.

[3]. Prof.Dr.Alaa Hussein Al-Hamami and Ibrahem Abdallah Aldariseh, "Enhanced Method for RSA Cryptosystem Algorithm", 2012 International Conference on Advanced Computer Science Applications and Technologies.

BIOGRAPHIES

Anntinu.T.J received his B.Tech in Computer Science & Engg from Calicut University, Kerala and currently pursuing M.Tech in Computer Science & Engg with specialization in Data Security from CUSAT, Kerala. His research interest are Data security, Network security, Image processing.

Sherly K.K received her B.E degree in Electronics & Communication from Karnataka University, Dharwad and M.Tech degree in Information Technology from Punjabi University, Patiala in 1990 and 2004 respectively. Presently she is working as Head of Department of Information Technology at Toc H Institute of Science & Technology, Arakunnam .She has more than 20 years of academic experience. Her research interests are Network security, Knowledge Discovery in Databases, Distributed Database Systems and Parallel Processing.