Data Transmission using RSA Algorithm

Miss. Akshata Chavan[1], Miss. Asmita Jadhav[2], Miss. Shraddha Kumbhar[3] , Miss. Indira Joshi[4]

Ms. Akshata Chavan, Department of Computer Engineering, DRIEMS, Neral, Maharashtra.
Ms. Asmita Jadhav, Department of Computer Engineering, DRIEMS, Neral, Maharashtra.
Ms. Shraddha Kumbhar, Department of Computer Engineering, DRIEMS, Neral, Maharashtra.
Ms. Indira Joshi, Department of Computer Engineering, DRIEMS, Neral, Maharashtra.

---***---

Abstract - *The confidential details transferred through the internet are hacked by phishing in an electronic communication world. So information security plays an important role. The cryptographic algorithms are applied over many applications for secure transmission of data against malignant attacks. In this work, a discussion is made based on a method for the data security authentication in a network using the combination of symmetric and asymmetric algorithms. In order to have data security, all the data packets are encrypted and decrypted using symmetric cryptography algorithm AES and authentication can be obtained by asymmetric cryptography all using the RSA algorithm.*

Key Words*: *AES, RSA, Cryptography, Encryption, Decryption.

1. INTRODUCTION

The security in the network plays an important role and can be achieved by different cryptographic algorithms. Cryptography is the science and art of transforming messages to make them secure and immune to attacks by authenticating the sender to the receiver within the network. Cryptography basically works on the principle of mathematics that generates different algorithms known. The cryptographic algorithms are of two types: symmetric key and asymmetric key algorithms. The symmetric key algorithm uses a single key to encrypt and decrypt the data whereas, the asymmetric key algorithm uses two types of keys i.e. the public key for the encryption and private key for the decryption. Two important properties of cryptosystems are its speed and security. To solve the problem of attacks and threats the system needs to have strong security. In this project, the work is done to implement a security mechanism that will hold against security issues. Security is a process and not a product. The password is being the most common authentication technique which provides the claimant access to system resources. For encryption, symmetric algorithms and asymmetric algorithms can be used to design a secure system, but there are some drawbacks. Like the AES algorithm is symmetric key algorithm means it makes use of its secret key for encryption and decryption similarly RSA algorithm is an asymmetric key algorithm that makes use of public key and private key. Both the algorithms have their own disadvantage like the AES algorithm is fast but vulnerable to the Brute force attack and the RSA algorithm is slow but provides high security. So, a mechanism is designed using both the algorithms which help to overcome the problems of security in networking.

2. PROBLEM STATEMENT

The main objective of this work is to achieve data confidentiality and authentication by the RSA cryptographic algorithm followed by the AES cryptographic algorithm. So, a mechanism is designed using both the algorithms which help to overcome the problems of security. We have proposed a secure mechanism by using Multiple Encryption and OTP. OTP password provides strong authentication while the AES algorithm and RSA algorithm provide strong encryption security.

3. PROPOSED SYSTEM

We have proposed a secure mechanism by using Multiple Encryption and OTP. OTP password provides strong authentication while the AES algorithm and RSA algorithm provide strong encryption security.

3.1. User Authentication:

It consists of two phases in the introduced technique. They are the Registration Phase and Login Phase.

3.1.1. Registration Phase:

During registration, users will register by providing personal information like email and username along with the text-based password.

3.1.2. Login Phase:

To ensure the successful login, first of all, the user will enter the username and text-based password.

3.2. Multiple Encryptions:

After login successfully if the user wants to send a file or data to the receiver, the user has to first upload the file. During the upload phase the file gets encrypted with the AES algorithm, and the secret key of the AES algorithm gets encrypted by a public key of the RSA algorithm. The receiver can download the file by using the private key, and the system generated OTP password which is sent to the registered mobile no. The private key is sent to the receiver through another secured channel like email. Thus, a strong security mechanism for data security is obtained by using multiple encryptions.

3.2.1. AES Algorithm:

The Advanced Encryption Standard (AES), is a symmetric block cipher.

The AES (Advanced Encryption Standard), is a symmetric block cipher. The AES encryption process uses a set of derived keys known as round keys. These keys are used with other operations that hold only one block of data to be encrypted.
The following steps of AES encryption are for 128 bits block:

1) Derive the set of round keys by using a cipher key.
2) Initialize the state array with the block of data i.e. plaintext.
3) Starting state array is added with initial round key.
4) Perform the four operations for nine rounds which consist of several processing steps like substitution step, row-wise permutation, a column-wise mixing step and the addition of the round key.
5) Perform the tenth and final round which does not have (MixColumns) it includes only SubBytes, ShiftRows and AddRoundKey.
6) Copy the final state array as the encrypted data i.e. cipher text. The process of transforming the cipher text to plaintext using the same encryption key is called a decryption process of AES. During the decryption process, the set of rounds is just the reverse of encryption rounds.

3.2.2. RSA Algorithm

The Rivest-Shamir-Adleman (RSA) cryptosystem is one of the best-known public key cryptosystems for key exchange or encryption of blocks of data. The RSA uses a variable size encryption block and a variable size key. The key-pair is derived from a very large number, n, that is the product of two prime no. chosen according to special rules. The difficulty of factoring large numbers is the basis of the security of RSA Algorithm. Over 1,000 bits long numbers are used for RSA. The RSA can be used to encrypt and decrypt actual messages, and it is very slow if the message is long. Therefore, the RSA algorithm is useful for short messages. Since the algorithm uses two keys for encryption and decryption: the public key and the private key, the RSA algorithm is considered as an example of asymmetric key cryptography.

Existing RSA algorithm Key generation:

1) Select two prime numbers, x and y, and $x \neq y$.
2) Calculate $n = x * y$. Calculate $\varphi (n) = (x -1) x (y -1)$.
3) Select integer e such that $\gcd (e, \varphi (n)) = 1$ such that $1 < e < \varphi (n)$.
4) Calculate the private key, $d = e^\wedge(-1) (\bmod \varphi (n))$.
5) Then public key = {e, n}.
6) Private key = {d, n}.
7) Encryption: c = me mod n.
8) Decryption: m = cd mod n.
9) Where, c - ciphertext, m – message

The key feature of the public-key cryptosystem is that the encryption and decryption procedure is done with two different keys - the public key and private key.

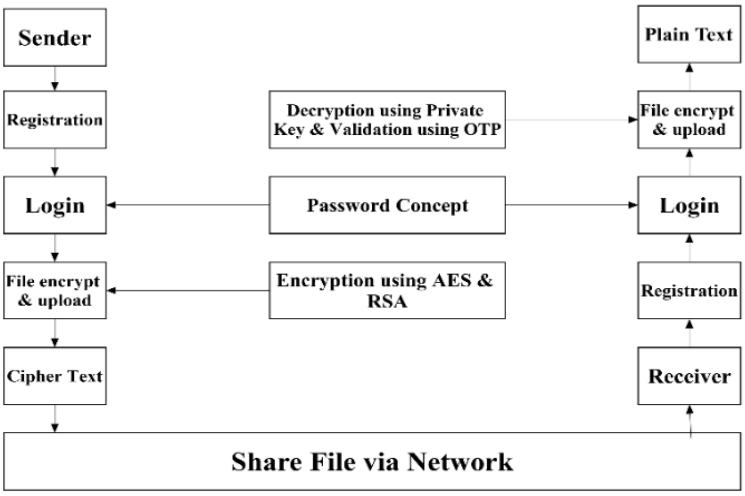

Fig-1. System Architecture

4. CONCLUSION

The project is focused on the improvement of security and performance of cloud computing by building a secure mechanism for transferring data over the internet. The approach is built by using a Text-based password and Multiple Encryption. One time password provides privacy and confidentiality by restricting the unauthorized user and Multiple Encryption prevents the system from the attacks by maintaining the loopholes of the securing mechanism.

5. REFERENCES

[1] Stallings, William, "Public Key Encryption and RSA," in Cryptography and Network Security, 5th ed. Published by Pearson Education, Inc, Copyright © 2011, pp. 293-314.

[2] R. Rivest, A. Shamir, and L. Adleman, "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems", Communications of ACM, Vol.-21, Issue-2, February 1978.

[3] Evgeny Milanov, "The RSA Algorithm," June 2009.

[4]W. Stallings, Cryptography and network security 4th Edition. prentice hall, 2005.

[5] Wentao Liu, Dept. of Comput. & Inf. Eng. ,Wuhan Polytech. Univ., Wuhan, China "Research on cloud computing security problem and strategy, "in Proc. Consumer Electronics, Communications and Networks (CECNet), 2012 2nd International Conference, Yichang, 21-23 April 2012, pp.1216-1219.