SECURE DATA TRANSMISSION USING HYBRID CRYPTOGRAPHY

S. Deepika
Department of Computer Science and Engineering
Vignan's Institute of Engineering for Women
Visakhapatnam, India

V.D.L.Rajeswari
Department of Computer Science and Engineering
Vignan's Institute of Engineering for Women
Visakhapatnam, India

R.Yamini Varma
Department of Computer Science and Engineering
Vignan's Institute of Engineering for Women
Visakhapatnam, India

S.Ramya
Department of Computer Science and Engineering
Vignan's Institute of Engineering for Women
Visakhapatnam, India

Ms.Y.Vineela Sravya
Assistant Professor
Department of Computer Science and Engineering
Vignan's Institute of Engineering for Women
Visakhapatnam, India

ABSTRACT

As large amount of data is transmitted over the network, it is preliminary to secure all types of data before sending them. This is achieved through security controls. Protecting the information transmitted over the network is a difficult task and the data security issues become increasingly important. To improve the data transmission over the public network is very essential aspect. Cryptography provides some methods for securing the data. It is important to prevent the data from being infected by an intruder. To transmit the data efficiently, both speed and security play a vital role. In this project, Hybrid cryptography has been used in which it makes use of two algorithms they are RSA and AES. The RSA algorithm provides the security for the data and the AES algorithm provides fast encryption speed. By combining these two algorithms we can achieve both security and fast encryption speed.

Keywords: Hybrid Cryptography, RSA(Rivest,Shamir,Adleman) Algorithm, AES(Advanced Encryption Standard) Algorithm

1.INTRODUCTION

Cryptography provides for secure communication in the presence of malicious third-parties known as adversaries. Cryptography not only protects data from theft or alteration but can also be used for user authentication. Cryptography provides some methods for securing the data. For that Encryption Algorithms are used to protect the confidentiality of data. Hybrid encryption is a method used for securing the data. Hybrid encryption is a process by which combines two or more algorithms together and provides more security than a single encryption can do. This provides safe mechanism for data transmission over the network. This mechanism also provides dual protection by taking the advantages of the algorithms used, so the data transmission in the network will be more secure.

Internet is an open system to public it must face many safe problems. The problems include network attack, hacker intruding, interception and tampering of network information which lead huge threat to Internet. Information security becomes a hot problem which is concerned by our society. Cryptography is used f or safe data transmission over the network. Cryptography is the process by which the original message is converted into some other form. This conversion of original message to cipher text is called encryption and the encrypted message is called cipher text. This process is shown in. And the reverse process is called Decryption; that is, creating the original message from the cipher text. There are different cryptographic algorithms. Cryptographic algorithms are mainly classified into:

- Symmetric Encryption (Secret Key Cryptography)
- Asymmetric Encryption (Public Key Cryptography): Uses one key for encryption and another one for decryption.
- Hash Functions: Mathematical transformation is used for encryption

2.LITERATURE SURVEY

This chapter provides an overview of previous research on knowledge sharing. It introduces the framework for the case study that comprises the main focus of the research described in this thesis. It is important to set the context of the literature review work by first providing:

An explanation of its specific purpose for this particular case study; comments on the previous treatment of the broad topic of knowledge sharing, and the role of intranets in such activity; An indication of scope of the work presented in this chapter.

The main purpose of the literature review work was to survey previous studies on knowledge sharing and intranets. This was in order to scope out the key data collection requirements for the primary research to be conducted. The approach adopted was in line with current practice in grounded research work. It is now regarded as acceptable for researchers to familiarize themselves with existing research prior to collecting their own data even though this contradicts the advice of grounded theory as originally presented.

An appreciation of previous work in this area served three further purposes. First, providing direction in the construction of data collection tools, it guarded against the risk of overload at the primary data collection stages of the project. Second, working the findings from extant literature into a formal review helped maintain throughout the study a sense of the topic's perspective. Finally, this activity raised the opportunities for articulating a critical analysis of the actual "meaning"

of the data collected when the data analysis stages of the research were reached.

A range of secondary data sources served as the key bibliographic tools for identifying relevant work for review. Relevant publications were found in the literature of a number of academic domains. Most of these publications take the form of research papers.

The research papers help us to find the existing models and allow us to find the loop holes and guide us to develop a new thesis by overcoming the problems which have been found out in the survey.

3.EXISTING SYSTEM AND DRAWBACKS

RSA algorithm is asymmetric cryptography algorithm. Asymmetric actually means that it works on two different keys i.e. Public Key and Private Key. As the name describes that the Public Key is given to everyone and Private Key is kept private.

Key distribution in RSA is easy. According to number theory, it is easy to finds two big prime number, but the factorization of the two prime numbers is hard. In this theory, every customer has two keys. They are encryption key and decryption key. Customer opens public key. Each person who wants to transmit information can use the key. However, customer keeps private key to decrypt the information. Here, n is the product of two big prime number p and q (the bits of p and q which are decimal number extend 100). e and d satisfy certain relation. When e and n are known, d cannot be got.

Since this is asymmetric, nobody else except browser can decrypt the data even if a third party has public key of browser.

The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of two numbers where one number is multiplication of two large prime numbers. And private key is also derived from the same two prime numbers. So if somebody can factorize the large number, the private key is compromised. Therefore, encryption strength totally lies on the key size and if we double or triple the key size, the strength of encryption increases exponentially. RSA keys can be typically 1024 or 2048 bits long, but experts believe that 1024bit keys could be broken in the near future. But till now it seems to be an infeasible task. The drawbacks are:

1. Public keys should/must be authenticated: No one can be absolutely sure that a public key belongs to the person it specifies and so everyone must verify that their public keys belong to them.

2. Slow: Public key encryption is slow compared to symmetric encryption. Not feasible for use in decrypting bulk messages.

3. Uses up more computer resources: It requires a lot more computer supplies compared to single-key encryption.

4.PROPOSED SYSTEM

Hybrid Cryptography is proposed in which RSA and AES algorithms are combined, AES provides high speed and RSA provides security during data transmission. AES and RSA two-layer encryption are used in the hybrid encryption algorithm, and the encryption process undergoes a sequence of transformations and procedures. The operations involved in the file encryption scheme of the two algorithms are listed in detail below, according to the encryption order. The processing units are clustered in the AES algorithm, and the 128bit data grouped in order will be allocated to a state matrix of 4*4. Centered on the state matrix, all transformations in the algorithm are completed. Involved in the process are four simple arithmetic techniques, Sub Bytes, Shift Rows, Mix Columns and Add Round Key.

1) Bytes Sub :Sub Bytes, also known as s-box permutation, is the only non-linear byte transformation in an AES algorithm encryption round, and each byte in the state is determined independently using the substitute table. The Sub

Bytes mapping approach is to take the high 4 -byte bits as the row value of the matrix and the low 4 byte bits as the column value and take the unit as the output with the column value as the index from the corresponding location in the s box.

2) Rows Shift: Each row is cyclically moved to the left in the forward Shift Rows by a row number offset, that is, the ith row of the state matrix is shifted left by I bytes.

3) Mix Columns :Mix Columns transform operates on each column in state and treats each column as a fourth degree polynomial. The addition and multiplication of Mix Columns operation are both defined on the finite field on GF.

4) Introduce the Round Key: When converting Add Round Key, the value obtained is the 128-bit State xor by bit and the 128-bit key. When encrypting the AES key with an RSA algorithm, the plain text is divided into groups, and the binary values of each group m are all less than n, where n is the product of the large prime numbers p and q, e is a random positive integer, and the cipher text c generated can be obtained from the following formula [12]: c = me mod n, and 0 <= m <n.

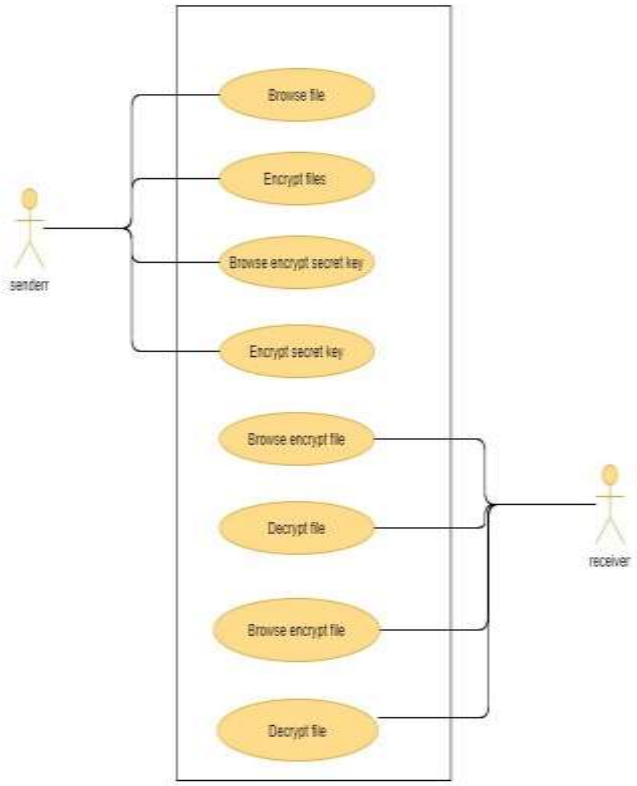
Hybrid Algorithm Decryption Principle:

In the hybrid algorithm, the private key of the RSA algorithm is used to decode the cipher text encrypted by the public RSA key in the first layer, and then the AES key is used to decrypt the cipher text and get the plaintext. As RSA decryption is used, the encrypted cipher text c is decrypted and transformed, and the plain text m is obtained by the following calculation.

5.DESIGN

Design is the first step in the development phase for any techniques and principles for the purpose of defining a device, a process or system in sufficient detail to permit its physical realization. Once the software requirements have been analyzed and specified the software design involves three technical activities design, coding, implementation and testing that are required to build and verify the software. The design activities are of main importance in this phase, because in this activity, decisions ultimately affecting the success of the software implementation and its ease of maintenance are made. These decisions have the final bearing upon reliability and maintainability of the system. Design is the only way to accurately translate the customer requirements into finished software or a system. Design is the place where quality is fostered in development. Software design is a process through which requirements are translated into a representation of software. Software design is conducted in two steps. Preliminary design is concerned with the transformation of requirements into data.

In the sender's side interface the encryption of secret key and message is done and in the receiver's side decryption of the previously encrypted secret key and message id carried out .



6.OUTPUT SCREENS

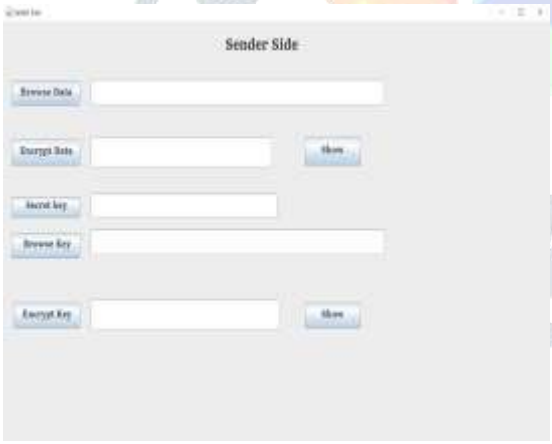


Fig 6.1:sender side interface

Fig 6.2:browse text file and perform encryption on data

Fig 6.3:Generate secret key and perform encryption on key

Fig 6.4**:**Receiver side interface

Fig 6.5: browse encrypted key and perform decryption on key

Fig 6.6: browse encrypted file and perform decryption on file

7.CONCLUSION

By using hybrid cryptography which means the combination of AES and RSA, will give us security and with fast encryption speed from sender to receiver. RSA is used for secure data transmission. ASE is used to encrypt the data in minimum time. AES is a symmetric key and RSA is an asymmetric key. For symmetric-key algorithm, the same cryptographic key is used for both encryption and decryption, in comparison to asymmetric-key algorithm symmetric-key algorithm like AES is usually high speed. For asymmetric-key algorithm, it requires two separate keys, one of which is secret (or private) and one of which is public. AES is used to generate secret key and RSA is used to generate the key pairs. So, by using hybrid cryptography the data is transmitted in secure way and with fast encryption speed.

8.REFERENCES

[1] Padate, R., & Patel, A. (2014). Encryption and decryption of text using AES algorithm. International Journal of Emerging Technology and Advanced Engineering, 4(5), 54-9.

[2] IEEE 1363: Standard Specifications for Public-Key Cryptograph

[3] IEEE :Application of AES and RSA Hybrid Algorithm in E-mail

[4] Kui-He Yang, Shi-Jin Niu,(2009), _Data Safe Transmission Mechanism Based on Integrated Encryption Algorithm', International Conference on Computational Intelligence and Software Engineering,Vol.7, pp.1 – 4.

[5] Zou L., Ni M., Huang Y., Shi W., Li X. (2020) Hybrid Encryption Algorithm Based on AES and RSA in File Encryption.

[6]Yuan Kun, Zhang Hanli Zhaohui, 2009 "An Improved AESalgorithm based on chaos", Multimedia Information Networking and Security, INES'09,InternationalConference.

[7] Behrouz A.Forouzan "Cryptography and network security" TATA McGraw Hill publication, 2007 edition.

[8] Avi Kak, Avinash Kak, "Computer and Network Security on Public-Key Cryptography and RSA" May 15, 2013 Purdue

[9] Vikas Kaul, S K Narayankhedkar, S Achrekar, S Agrawal, PGoyal, "Security Enhancement Algorithms for DataTransmission for Next Generation Networks", International Journal of Computer Application (IJCA).

[10] William Stallings:"Cryptography and network Security: Principles and Practices".