KEY BASED SECURE DATA TRANSMISSION OVER THE NETWORK

A.AROKIA ROSELINE[(1)], R.BALA KIRETHIGA[(2)], G.GEETHA[(3)], K.GOWSIKA[(4)]
[(1)(2)(3)(4)]UG STUDENT, DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
M.KUMARASAMY COLLEGE OF ENGINEERING, KARUR

ABSTRACT

In order to make communication between multiple users or between one user to another user, security is needed. Security is provided by means of encrypting the data before the transmission could take place using the keys of the user and recipient. Only the cipher text is transferred over the network which is hard to analyze by the intruder. Here the key generation is based on the elliptical curve cryptography techniques rather than the normal RSA techniques.

The disadvantages of the RSA could be

- ***The speed of the key generation is slower when compared to ECC.***
- ***Authentication of the data for the encryption and decryption takes longer time than any other type.***

All these shortcomings are overcome by the ECC algorithm because the time taken to generate the key is fast and the speed is fast than RSA.

As long as separate key for each session data can be transferred easily and securely.

KEY WORDS: ***RSA algorithm, ECC algorithm (Elliptical curve cryptography).***

1. INTRODUCTION

Computer security is also called as secure computing or cyber security helps as to protect our system from our harmful access. It also helps as to how to transfer the data securely over the internet without being hacked by the intruders.

To secure a computer from attacks, we must know the possible attacks that can be made on the systems. Cyber security helps us to monitor the security incidents, forensic analysis, and to improve the security of the data being handled.

Cryptography is the technique that helps us to make secure communication even in the network. It helps us to analyze the protocols that secure us from the access of public users reading our messages.

Various cryptography techniques are available in which some uses two same key for both encryption and decryption while some uses different keys for the encryption and decryption to take place. Various encryption standards are available for the secure data transmission to take place.

In order to secure the communication two parties need to be authenticated and an encrypted session key need to be generated in advance. There are two models available for the authentication and for key exchange.

Securing the group communication involves the use of protocols for the group authentication for thee key exchange. It allows the group of users to communicate in an insecure network using a common secret key for the sharing of the information over the network.

Here session key is used for the encryption of the messages, since session key is also called as single use symmetric key. The same key is used for the entire message encryption also known as content encryption key. They are used because of its ability to solve many real time problems. The main reason to use such keys is

They are limiting the data to be encrypted by using the single key hence the ability to detect and attack the data becomes ridiculous.

2. EXISTING PROJECT

In the existing model the data is transferred between the client and the other storage device. Here the metadata server helps in the key exchange between the client and the other data storage. They do not provide the secrecy for the data transmission to take place. This means that once the key get compromised the data transferred using the keys can be compromised and it can be hacked. In this the communication takes place between the many to many communication channels that helps to access the storage device having large number of clients. This method focuses on the m

ethod for the key exchange and how to make a secure communication for the multiple line communication at the same time. The goal of this is to establish a secure key for the data transmission to take place. Also in earlier method password based authentication system has been used for the data transmission to take place which means that the hash functions that has been for the password. Two Server PAKE protocol was based on the authentication in which the server verifies the client with the server's help. In this two servers where used for the data transmission to the client. Here in this the failure of one server will not stop the entire transmission of data another server will continue for the data transmission to take place. Here in this session the secret key is established between the server and the client for the data transmission.

2.1 DISADVANTAGES

Here the Meta server can be compromised for the data so that it can be used for any other purposes. Here the system is mostly used for the closed and connected system. It cannot be used for scalability and parallel access in network. Also the used of same hash function will leads to the finding of the data.

3. PROPOSED SYSTEM

In this the user uses the elliptical curve cryptography because it generates the key at a faster speed than any other algorithm. Here the data is encrypted using the public of the recipient. The sender gets the authenticated public key of the receiver with the help of the trusted authority by sending a request to the third party for the key. The third party maintains the public key of several users. Here we use two servers for the data transmission to take place this helps us to split the data and transmit it over the

network in order to avoid that data being hacked and modified. Here the public key of the users can be changed in case the key is being tracked by the hacker. The two servers help us to split the data before transmission. This splitting of data helps us to secure the data for transmission. Incase if the intruder hacks any one part of the data and if it being modified and sent over the network on the receiver side when they try to decrypt the data if it is not the original message then the receiver can understand that the data is being modified. In that case we can go for retransmission of the data part which is modified. This helps for the secure data transmission of the data.

3.1 ADVANTAGES

The data can be transferred securely over the network if data is found missing retransmission helps for the data to get identified.

The trusted authority will maintain the public key of the user which when hacked will not be used for any other purposes.

The server when hacked will contains only the partial part of the data also cannot be used for any other purpose.

4. CONCLUSION

Thus the data can be transferred securely over the internet. They can be used for the cloud data storage and secure data storage and transmission.

The disadvantages of RSA algorithm has been overcome in this ECC such as

1) Complexity of the key generation

2) Slower in speed

And several other drawbacks has been overcome through this algorithm. The use of ECC helps us to lower the production cost and cheaper design yet the security is at the same level.

REFERENCES

P. Mell and T. Grance, "The NIST definition of cloud computing,"
Nat. Inst. Standards and Technology (NIST), Special Publication 800-
145, Aug. 2011

Authenticated key exchange protocol for parallel network system Hoon wei lim, guomin yang vol.27, no 1, January 2016.

Efficient two server password- only authenticated key exchange Xun yi, San ling and Huaxiong Wang vol:24 No:9 2013

ID based group password- Authenticated key Exchange Xun yi, Raylin Tso and eiji okamota

Proof of security for password based key exchange E.Bresson, O.Chevassut and D.Pointcheval