MEDIATED CERTIFICATELESS CRYPTOSYSTEM FOR THE SECURITY OF DATA IN PUBLIC CLOUD

Nubila Jaleel[1], Chinju K[2]

[1]*Department of Computer Science And Technology M.G university nubilajaleel@gmail.com*
[2]*Department of Computer Science And Technology M.G university Ernakulam,Kerala,India*

Abstract

Security is a serious issue in cloud computing. Encryption is the solution for the security in cloud. There are many encryption techniques. Each one has its own merits and demerits. In the case of identity based encryption it is free from security mediator, predefined keys are there, and have the problem of key escrow and certificate revocation. Then the arrival of mediated certificateless scheme eliminates the key escrow problem, and certificate revocation problem. In certificateless encryption scheme, key generation process is divided in between the user and the cloud. In our system data owner encrypt the data using its secret key. Then the data owner encrypt the secret key twice. Hence formed intermediate keys. Then send this encrypted data and intermediate keys to cloud. The cloud partially decrypt the intermediate key and send partially decrypted data and encrypted data to required user. The user decrypt the partialy decrypted data. Then the user will get the required key for decryption. so the user can decrypt it completly.The main advantage of our system is, the data owner can send same data to multiple clients with minimum cost.

Keywords: *Cloud computing, Certificateless cryptography, Key escrow, Certificate revocation.*

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

1. INTRODUCTION

Cloud computing is a recently evolved computing terminology based on the consumption of computing resources. Cloud provide many options for the everyday computer user as well as large and small business. It increase the computing to a broader range of uses and increase the ease of use by giving access through any Internet connection. Many large business organizations and day to day computer users are using cloud computing because the cloud computing turns out to be cheapest and fastest method . And also it is very easy to maintain. However, with this increased ease also come drawbacks. Everyone must aware of the security risks of data stored on the cloud. The cloud is a big target for malicious users. There is a lot of personal information and potentially secure data that peoples stored on cloud. So the security of data stored in the cloud becomes a big issue.

There are many encryption techniques. They have its own merits and demerits. In identity based encryption it is free from security mediator, predefined keys are there, and have the problem of key escrow and certificate revocation. Then the arrival of certificateless scheme eliminates the key escrow problem, but have certificate revocation problem. In the case of identity based security mediated models do not have certificate revocation problem but have key escrow problem. So in the case of security mediated certificateless method, which is not free from security mediator, and do not have key escrow and certificate revocation problem. Another important thing is that bilinear mapping used. Every method employed bilinear mapping will be difficult and expensive. So there is a need for without using pairing approach. So to ensure the security of data shared in public cloud we can use security mediated certificateless encryption method without using pairing operation [4].

In order to assure confidentiality of sensitive data stored in public cloud , a commonly adopted approach is to encrypt the data before uploading it in to cloud. The cloud does not know the keys used to encrypt the data. Therefore the confidentiality of the data from the cloud is assured. But every organization requires fine grained encryption techniques [5]. A typical approach used to support encryption based access control is symmetric key encryption [2]. In this approach there is a private key. Even though the key derivation based approaches reduce the number of keys to be managed symmetric key based mechanism in general have the problem of high costs for key management. In order to reduce the overhead of key management an alternative is to use public key cryptography. Here we have a public key and private key. However a traditional public key cryptosystem requires a trusted Certificate Authority to issue digital certificates that bind user to their public keys. Overall certificate management is very expensive and complex. To address such shortcomings, identity based public key cryptosystem was introduced, but it suffers from key escrow problem. It means that the key generation center may learn about the private keys of all users. Recently, attribute based encryption [8]. However in addition to key escrow problem certificate revocation problem has been arrived. In order to address these problems certificateless encryption has arrived.

The rest of the paper is organized as follows. In section 2, Basic Encryption techniques are briefly described. Section

3 describes the related works. The Proposed approach and improved approaches are described in section 4. In section 5 Experimental result is included. And finally in section 6 summarizes the conclusion of this paper.

2. BASIC ENCRYPTION TECHNIQUES

In this chapter we make a comparisons on earlier approaches. One of the typical approach for encryption is symmetric key encryption technique. In this technique there is private key. We can encrypt using the private key. The advantages of symmetric key encryption includes it is relatively fast, and secure if we are using secure algorithms.

There are many symmetric key encryption algorithms are available. One of secure method is The Advanced Encryption Standard (AES). One of the Advanced Encryption Standard is Rijndael algorithm. AES is different from DES in many ways. In DES there is a fixed key size and block size. The Rijndael algorithm have variety of key size and block size supported. For 128 bit key length number of rounds will be 10 and for 192 and 256 the number of rounds will be 12 and 14 respectively. The symmetric key encryption can be used for large data encryption and decryption. But the disadvantage is on sharing of keys. When a malicious user gets the secret key he can decrypt all the data encrypted using this key. So it is very dangerous if compromised.

Another approach is the public key cryptography. Here we have public key and a private key. We can either use public key or private key for encryption. If we are using public key for encryption then encrypt the data using receiver's public key. For this every must aware of the public key of receivers. Then the receiver can decrypt by using his private key. Another method is to encrypt the data by using senders private key and distribute his public key to the receiver. But both of these method require a trusted third party called certificate authority. When a malicious user obtained the private key used for encryption then he can only decrypt the message sends to the owner of the private key. But this is not in the case of symmetric key encryption. One of the drawback of public key approach is that overall certificate management is very expensive and difficult, and it is relatively slow. And public key encryption have certificate revocation problem. To overcome such shortcomings identity based encryption has been arrived. Here any user can generates its public key from a known identity. Which may be ASCII string. The corresponding private key is generated by private key generator. Here any authorized user can generates any ones public key by using identity and master key. One of the advantages of identity based encryption is there is no need of certificates. The receivers public key is derived mathematically from its identity and master key from private key generator. The disadvantages of identity based encryption is that it is centralized approach and key generation center may learned about the private key. It is knows as key escrow problem. Here the certificate expired. So there is no certificate revocation problem but have key escrow problem.

In order to overcome the key escrow problem in identity based encryption another method called certificateless encryption arrived. Here the private key generation process is divided between the user and the server. It is not based on identity based because the public key will not be generated by the identity alone. And the private key is not exposed to key generation center. Hence ther is no key escrow problem.

3. RELATED WORKS

This section includes some related works based on certificateless encryption. And also make a comparison of related works.

S.Al-Riyami and K.paterson introduced a paper named certificateless public key cryptography [1]. This parer deals with the concept of certificateless public key cryptography (CL-PKE), which solves the key escrow problem and certificate revocation problem. In this scheme do not require certificates and do not have the feature of built in key escrow. Certificateless public key cryptography is the intermediate between traditional public key cryptography and identity based public key cryptography. One of the drawback of this scheme is that it is based on pairing operation.

A CL-PKC system still make use of a key generation center (KGC), but it contrast to PKG in ID-PKG. In this KGC does not have access to entities private key, instead the KGC supplies an entity A with a partial private key which is computed from an identifier IDA for the entity A and a master key. The entity A then combines its partial private key DA with some secret information to generate its actual private key SA. So that its private key does not know by the key generation center. The entity A also combines its secret information with the KGC's public parameters to compute its public key PA. The public key and private key is generated by using same secret information. This system is not based on identity alone. The public key of entity is available to the other entities by transmitting it along with message or by placing it in a public directory. To send a message to A by an entity B it makes use of only PA and IDA.This scheme is based on bilinear mapping. Computational cost for the pairing is expensive. So in effect this scheme is expensive

In order to over come this problem Y. Sun, F.Zhang, and J. Baek, introduce a paper named Strongly secure certificateless public key encryption without pairing [9].

It enjoys the advantage of identity based public key cryptography without suffering from key escrow problem. It was the first certificateless certificateless encryption without using pairing operation. This method proved the security against adaptive chosen ciphertext attack in the random oracle model.

Sherman S. M., Colin, and Juan Manual Gozalez introduced a paper named Security Mediated Certificateiess Cryptography. In this paper introduced the concept of

security mediated certificateless cryptography. It would have the ability of instantaneous revocation of keys. And also this avoid key escrow problem. This model provide security against a fully adaptive chosen cipher attacker, who have a rogue key generation center. but this scheme is based on bilinear pairing. This scheme is more efficient than the identity based mediated encryption scheme. Mediated cryptography was deigned as method to allow immediate revocation of public key. The basic idea of mediated cryptography is to use an on line mediator for every transaction. This on line mediator is referred to a Security mediator(SEM). When the SEM is notified that a user's key is to be revoked then its use can be immediately stopped.

The drawback of all identity based and security mediated cryptosystems so far proposed is that they require a trusted third party to generate keys of all entities. This is widely known an escrow problem. To avoid key escrow problem completely certificateless cryptosystem has been arrived. Each entity have public key but do not have certificate. Instead the identity string is used to ensure that only the correct entity can be in possession of the private key corresponding to the public key. But this method does not provide how to get instant revocation when desired. This problem is solved in this paper.

One of the drawback of these method is that it uses bilinear pairing. It is expensive. when we implement this scheme into cloud computing, if many users are authorized to access same data, the encryption cost at data owner become high. In this case the data owner has to encrypt the same data encryption key multiple times, once for each user with user's public key. From the above papers we can conclude that each technique have its own merits and demerits. In the case of identity based encryption [3] it is free from security mediator, predefined keys are there, and have the problem of key escrow and certificate revocation. Then the arrival of certificateless scheme eliminate the key escrow problem, but have certificate revocation problem. In the case of identity based security mediated models do not have certificate revocation problem but have key escrow problem. So in the case of security mediated certificateless method, which is not free from security mediator, and do not have key escrow and certificate revocation problem.

Another important thing is that bilinear mapping used. Every method employed bilinear mapping will be difficult and expensive. So there is a need for with out using pairing approach. So to ensure the security of data shared in public cloud we can use security mediated certificateless encryption method with out using pairing operation [6].

4. PROPOSED METHOD

We know that certificateless encryption is intermediate between public key cryptography and identity based cryptography. In this paper we combine public key and identity based cryptography to make certificateless encryption. Here at first each user generates its own identity public key and private key pair using any public key encryption algorithm. For autherisation along wih identity these pubic key is send to the cloud. Cloud verify its idenity and generates another pair of public key and private key for the above user. This is done in registration phase. So ecch user have its own pubic key, private key such as Upu, Upr and cloud generated public key, private key such as Cpu, Cpr respectively.

Next is the encryption phase. Here when a data owner wants to share some data to other user, first he send a request to cloud for obtaining the recievers cloud generated public key and reciever's Upu . When the data owner obtained these, first encrypt the data by using receiver's Upu and then with the receiver's Cpu. For autherisation last encrypt the same with the data owners Cpu. Send the result in to the cloud

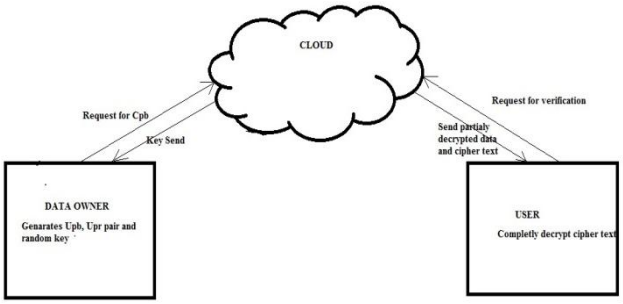

Figure 1: System Architecture

Next is the cloud decryption phase. Cloud first decrypt the data using data owner's Cpr for verifing. Next again decrypt using receiver's Cpr. Then send the remaing to the corresponding user.Next is the receiver decryption phase. Here the reciever completely decrypt the cipher text and obtained the plane text.

5. IMPROVED SECURE CLOUD STORAGE

We can either use only public key encryption or combine pubic key and symmetric key encryption for better result. One on the disadvantage of public key encryption is it is very slow. In order to over come this we can combine symmetric key encryption with public key encryption. For making this improvement each user have a private key, it is generated by using AES and the Cpu, Cpr, Upu, Upr generated by using RAS. Here we first encrypt the data using AES and encrypt the AES key using RSA. First encrypt the key using public key Upu of reciever, then encrypt by using cloud generated key of receiver. This is known as intermediate key. The data owner send this cipher text and intermediate key to cloud. Cloud first decrypt using receiver's Cpr and send this partialy decrypted intermediate key and cipher text to receiver. The reciver decrypt the intermediate keys completely and obtained data encrypted key. So receiver can easily decrypt the ciphertext.

The advantages of improved sytem is that it is relatively fast compared to the above approach, and it can eliminate the overhead of data owner when the data owner has to share the same data among different users . The data owner has to encrypt the same data once when he want to send

data. The private key is encrypted by the public keys of corresponding receiver.

6. BASIC ALGORITHM

Algorithm 1 describes the detailed working of the proposed method. It includes cloud server setup, registration phase, encryption phase, and decryption phase.

Algorithm 1: Data Security Algorithm
Output: Decrypted Data for a user
Inputs: Identity and Data
1) Cloud server Setup:
a) Run the server.
2) Registration:
a) specify the identity id.
b) generate pubic key, private key pair Upu and Upr using RSA.
c) generate private key S for encryption by using AES
d) Send its identity and public key Upu to cloud
e) Cloud veryfies the identity and generate its public key Cpu and private Cpr.
f) Send public key Cpu to the corresponding used
3) Encryption:
a) Data owner send a request to cloud with identity of receiver.
b) Data owner gets Cpu,Upu of receiver
c) Data owner encrypt data
d) Generate intermediate key
e) Send cipher text and intermediate key to cloud f) Done
4) Cloud Decrypt:
a) cloud partially decrypt the data.
b) Send partially decrypted data and cipher text to corresponding user
c) Done
5) Receiver decrypt:
a) Send a request to cloud for receiving data.
b) Completely decrypt intermediate key
c) Decrypt the cipher text d) Done

7. EXPERIMENTAL RESULT

This section include the analysis of proposed system with basic techniques.

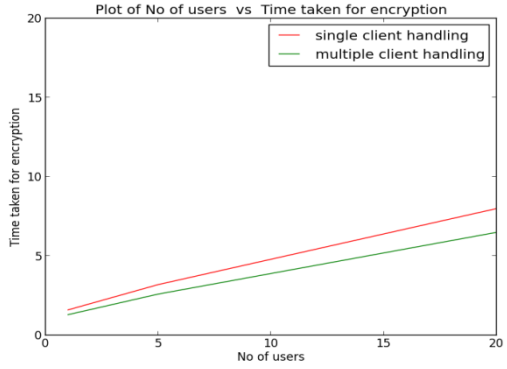

Figure 2: Experimental result on shairing Data among multiple users

The experiments were performed on a machine running 32 bits Linux kernel Intel R Core. Our prototype is implemented in python. In this chapter first make a comparison of basic approach and improved approach. Improved approach take less time for sharing same data among multiple users as compared to basic scheme.

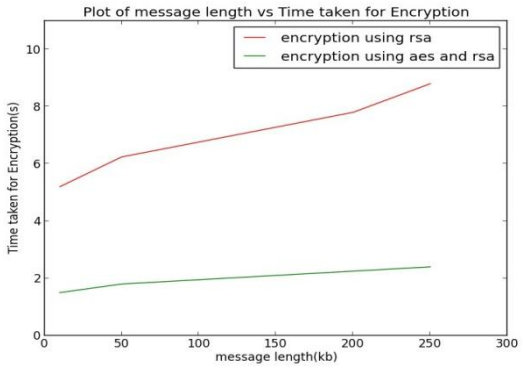

Figure 3: Encryption with RSA only and using RSAand AES

In basic scheme data owner want to encrypt the same data encryption key multiple times as compared to improved approach. And next analysis is based on RSA and AES. If we implement the system with public key cryptography, we can say that it is very slow. So inorder to overcome such shortcomings we combine AES and RSA. So we can get both advantages of AES and RSA. From the graph we can say that time taken for encryption and decryption is less as compared to algorithm use only RSA.

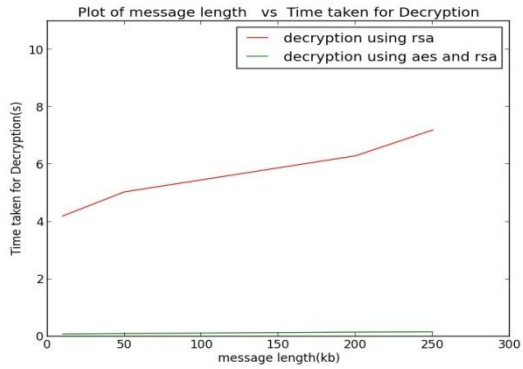

Figure 4: Decryption with RSA only and using RSAand AES

Figure 4 explain the decryption time taken for RSA only and using AES and RSA. The RSA decryption time will be high as compared to AES and RSA decryption time.

8. CONCLUSION

In this paper we have proposed a new certificateless encryption for secure cloud storage and sharing. It is implemented using AES and RSA. AES for data encryption and RSA for key encryption. Here certificate revocation in public key cryptography and key escrow problem in identity based encryption is solved. And here the overhead of data owner is reduced. Because the data owner has to encrypt the

data once when multiple user want to access the same data . And here we combine AES and RSA. We get both the advantages of AES and RSA. It seems to be relatively fast.

REFERENCES

[1] S. Al-Riyami and K. Paterson, Certificateless public key cryp- tography, in Proc. ASIACRYPT 2003, C.-S. Laih, Ed. Berlin, Germany Springer, LNCS 2894, pp. 452473.

[2] E. Fujisaki and T. Okamoto. Secure integration of asymmetric and symmetric encryption schemes. In M. J. Wiener, editor, Proc. CRYPTO 1999, LNCS vol. 1666, pp. 537554. Springer,
1999.

[3] M. Green and G. Ateniese. Identity-based proxy re-encryption.
In J. Katz and M. Yung, editors, Applied Cryptography and Network Security ACNS 2007, volume 42

[4] M. Abdalla et al., Searchable encryption revisited: Consistency properties, relation to anonymousibe, and extensions, J. Cryp- tol., vol. 21, no. 3, pp. 350391, Mar. 2008.

[5] D. Boneh, X. Ding, and G. Tsudik, Fine-grained control of security capabilities, ACM Trans. Internet Technol., vol. 4, no.
1, pp. 6082, Feb. 2004.

[6] S. S. M. Chow, C. Boyd, and J. M. G. Nieto, Security mediated certificateless cryptography, in Proc. 9th Int. Conf. Theory Practice PKC, New York, NY, USA, 2006, pp. 508524.

[7]I.Dropbox.Dropbox[Online].Available:
https://www.dropbox.com/