IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Using Certificate less Encryption for Providing Data Sharing Efficiency in Public Clouds

Ch. Dinesh

Sr. Asst. Professor, Department of Computer Science, Dadi Institute of Engineering &Tech, Andhra Pradesh, India

Abstract: Now a day's public cloud storages have more benefits to provide service to users to manage their data. However for the rapidly increase of public cloud storage, the public cloud should solve the major issue of data confidentiality. That is sharing sensitive data through all the data must be strongly secured for unauthorized access. In order to provide security of sensitive data store in public clouds, a commonly used approach is to encrypt data before upload into public clouds. So that to provide confidentiality of stored public cloud data, the encryption mechanism should also able to support the access of confidential data. In this paper we are propose public key encryption schema for generation of secret key and encrypt the data using that key. The generation of secret key we are using public key power auditing protocol. Another concept is encryption and decryption of data using data encryption standard algorithm. By implementing those concepts we can improve efficiency and security of give shared data in a cloud.

Keywords: Cloud Computing**,** Cryptography, Security Access Control, Certificate less cryptography.

1. INTRODUCTION

Implementing this concept we can reduce the problem of managing keys and also does not need to maintain the relevant keys. So that by implementing the concepts we can't generate digital certificates separately and also we can't generate secret key. Both the functions can be done by implementing new certificate less public key cryptography technique. In the certificate less public key cryptography technique contains other concepts for encryption and decryption of cloud data so that by implementing those concepts we can provide more efficiency and privacy of sharing information in the cloud.

Based on our schema we proposed a novel certificate less public key cryptography for the generation of digital certificates and also provide data encryption. By implementing those concepts we can get more confidentiality sharing information in the cloud and also get more efficiency for generation of digital certificates. In this approach we can also provide semi trusted for the authentication of users in the cloud computing. If the user is authenticated we will provide provision for the decryption of retrieving data. If the user is not authenticated it will not get the decryption process. In this schema the accessing control of data owner is to perform the encryption of data and stored the data into cloud. For the encryption of data items the data owner will use one of the symmetric cryptography techniques. The advantage of our schema is that easy generation of secret key and also provides more confidentiality of sharing information in the cloud.

2. RELATED WORK

The yang et al[1] is first to introduce the novel approach for the certificate less public key cryptosystem. But the schema is insecure against the partial decryption attack. In the Yang et al schema will face the problem of decryption process of sharing data items in cloud computing. The partial decryption attack will also face the problem of secure mediated of certificate less public key cryptography with pairing is needed. By implementing without pairing we face the problem of removing certification management problems. Since the advent of public key cryptography schema as many certificate less public key encryption schema have been proposed. The certificate less public key encryption schema is to be implemented based on bilinear pairing. By implementing bilinear pairing will be more computational and will be maintained high standard operation such as modularexponentiation in finite fields.To improve the efficiency of certificate less public key encryption Sun et al[2] proposed a strongly secure schema without pairing.

However some of previous certificate less public key encryption schema could not solve the key revocation problem. In the public key cryptography, we should implement scenarios of some private keys. So that if the private key is compromised, then it is no longer secure to use the public keys in the public key cryptography. To address this problem, Boneh et al[3] proposed the new concepts for mediated cryptography to provide support for immediate revocation. The basic concept of mediate cryptography is to provide security mediator. The security mediator will control the all control security capabilities of every transaction in the cloud. Suppose the security mediator revoke the users public key immediately it will stop the users participation in a transaction.In 2003, Al-Riyami and Paterson [4] introduced a CertificatelessPublic Key Cryptography (CL-PKC). Since each user holds a combination of KGC produced partialprivate key and an additional user-chosen secret, the key escrow problem can be resolved.

3. EXISTING SYSTEM

Due to the benefits of public cloud storage, organizations have been adopting public cloud services such as Microsoft Sky Drive and Drop box to manage their data.

DOI 10.17148/IJARCCE.2016.5222

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

However, for the widespread adoption of cloud storage services, the public cloud storage model should solve the critical issue of data confidentiality. That is, shared sensitive data must be strongly secured from unauthorized accesses. In order to assure confidentiality of sensitive data stored in public clouds, a commonly adopted approach is to encrypt the data before uploading it to the cloud.

In order to assure confidentiality of sensitive data stored in public clouds, a commonly adopted approach is to encrypt the data before uploading it to the cloud. Since the cloud does not know the keys used to encrypt the data, the confidentiality of the data from the cloud is assured. However, as many organizations are required to enforce fine-grained access control to the data, the encryption mechanism should also be able to support fine-grained encryption based access control. a typical approach used to support fine-grained encryption based access control is to encrypt different sets of data items to which the same access control policy applies with different symmetric keys and give users either the relevant keys or the ability to derive the keys. Even though the key derivation-based approaches reduce the number of keys to be managed, symmetric key based mechanisms in general have the problem of high costs for key management.

4. PROPOSED SYSTEM

The proposed system of Certificate less Public Key Cryptography mainly contains three concepts i.e. Generation of group key, generation of signature, encryption and decryption of shared data in a cloud. By implementing those concepts we can improve the performance and security of shared data. The implementation procedure of those concepts as follows.

Generation of group key:

The Trusted Authority will generate group key and sent to all group members. The generation of group key is as follows.

1. Each group member will register into group by entering he/she details. After registering Trusted Authority will give username and password for each user.
2. The user will login using those username and password. After login the each group member will choose two prime number(P,G) and also choose one private key a.
3. By using those value each group member will calculate public key and send it to Trusted Authority. The calculation of public by using given formula.
   Public key= G^a mod p
4. The group members also sent his prime numbers to Trusted Authority.
5. The Trusted Authority will retrieve those value and generate another public key by using give formula. Before generating public key the Trusted Authority will generate individual private keys of group members.
   Pub key_i= public $key_i^{privatekey_i}$ **mod** p_i
6. After generating pub key of each member and Trusted Authority will sent to those keys to each group member.
7. Each group member will retrieve pub key and again generate shared key by using give formula.
   $sharedkey_i=pub\ key_i^a$ mod P
8. After calculating shared keys each member will send those keys to Trusted Authority.
9. The Trusted Authority will retrieve shared keys and will generate secret key by using following formula

$$publickey=pub_1 \circledR pub_2 \circledR \ldots\ldots pub_i$$

$$Pval=P_1 \circledR P_2 \circledR \ldots\ldots P_i$$

$$Secretkey_i=publickey^{sahredkey1 \circledR sharedkey2\ \ldots.sharedkey_i} \textbf{mod} Pval.$$

After generating secret key the Trusted Authority will generate signature for the each group member. The generation signature is as follows.

Signature Generation:

The Trusted Authority will generate signature for authentication of each group member. The generation of signature as follows.

$$Val=publickey_i \circledR sharedkey_i$$

$$Sig_i= hash(val)$$

After that the Trusted Authority will send signature and key to individual group members. The group members will retrieve signature and secret key again generate signature by using same formula. After generating signature if both signatures are equal that group member is authenticated user. By implementing this technique we can't generate any certificate for authentication purpose. So this is one of the advantages of proposed system. After completion of authentication each user will get secret key. By using the secret key each group member will decrypt the shared data in the cloud. Before sending the secret key to group member the trusted center will also send the secret key to data owner for the purpose encryption of shared data and stored into cloud.

Encryption and Decryption Shared data:

In the encryption and decryption shared data can be performed by the two types of users. They are encryption process can be performed by data owner and decryption process can be performed by group member. The encryption and decryption of data is by using data encryption standard algorithm. Before storing the data into cloud the data owner will encrypt the shared data and stored into cloud. After that if any user wants that data it will retrieve the cipher data and decrypt it by using decryption process of data encryption standard algorithm

For the implementation of proposed system we cannot generate digital signature separately and also the secret key. In the proposed system by using public and private keys we can generate signature and also perform the modulo operation based on those values we can generate the secret key. In this paper the generation of signature we are using one way hash function i.e. message digest five. After generating individual digital signature of users the Trusted Authority will generate secret key and send to all users. After sending signature and secret key to users, each and every user will verify authentication status. If the users are authenticated then they get the secret key. Before sending signature and secret key to users the Trusted

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 2, February 2016

Authority also send only secret key to data owners. The data owner will retrieve the secret key from the Trusted Authority and choose the file to be stored into cloud. Before storing the file the data owner will encrypt file by using the data encryption standard and stored into cloud.

After storing the cipher format data into cloud if any user want particular file then the user will be select file and retrieve the cipher format data. So that the user will generate secret key and using that secret key we can get original plain format data. Getting plain text we perform the decryption process of data encryption standard. By implementing this concept we can reduce time complexity for the generation digital signature and reduce relevant type of keys. In this process we can also reduce the generation digital signature concepts and separation process of the secret key generation. Both concepts of generation signature and secret key can be implemented in the proposed system.

5. EXPERIMENT RESULT

In this section we present experiment result of our proposed system. In the implementation of our proposed we are using the language of Java and we use the encryption, decryption of data using data encryption standard.

The above diagram specifies user can enter Prime number p, g and private for the calculation of public key. After entering those values the user will calculate public key.

The above specify the calculation of public and send that value to Trusted Authority. y calculation of public key we are using the private Key of user and also use the user choosing values of p and q.

The above diagram specifies retrieving of public keys of users. The Trusted Authority will retrieve public keys from the users and use that key for generation of user's public keys.

The above diagram specifies the generation of public keys of users. In this page the trusted center will retrieve public keys of each users and generate private keys of individual users. After generating private keys of each user the trusted Authority will generate public keys for users and send those public keys to individual users

The above diagram specifies generation of signature and secret key. The Trusted Authority will retrieve all shared keys of users and generate signature. In the generation of signature we are using message digest five hash function. After generating digital signature the trusted also generate secret for the users. After that both signatures and secret key send to individual users. Before transferring signature and secret key the Trusted Authority will send secret key to DATA OWNER.

The above diagram specifies choose the upload file by the data owner. The data owner will upload file and encrypt the upload file before storing data into cloud. After encryption of data the data owner will store the file into cloud. Before encryption of data the data owner will retrieve the secret key and using that secret key we can encrypt the file.

The above diagram specifies decryption process retrieving file from the cloud. Before decrypt the file the user will perform the authentication and get secret key. By using secret key the user will decrypt the data and get original plain format data.

DOI 10.17148/IJARCCE.2016.5222

6. CONCLUSION

In this paper we have proposed the concept of Certificate less Public Key Cryptography. Using the Certificate less Public Key Cryptography scheme as a key building block, we proposed an improved approach to securely share sensitive data in public clouds. Our approach supports three implementation processes those are the generation of secret key, generation of signature, data encryption and decryption. By implementing that concept we can't generate any certificate for the authentication purpose. We can also share the data throughout group member with securely.Our experimental result shows more efficiency and also provides more security of shared data.

REFERENCES

[1]. C. Yang, F. Wang, and X. Wang,"Efficient mediated certificates public key encryption scheme without pairings," in AINAW, Niagara Falls, ON, May. 2007, pp. 109–112.

[2]. Y. Sun, F. Zhang, and J. Baek, "Strongly secure certificateless public key encryption without pairing," in Proc. 6th Int. Conf. CANS, Singapore, 2007, pp. 194–208.

[3]. D. Boneh, X. Ding, and G. Tsudik, "Fine-grained control ofsecurity capabilities," ACM Trans. Internet Technol., vol. 4, no. 1,pp. 60–82, Feb. 2004.

[4] S. Al-Riyami and K. Paterson, "Certificateless public key cryptography," in Proc. ASIACRYPT 2003, C.-S.Laih, Ed. Berlin, Germany: Springer, LNCS 2894, pp. 452–473.

[5]. S. S. M. Chow, C. Boyd, and J. M. G. Nieto, "Securitymediatedcertificateless cryptography," in Proc. 9th Int.Conf. Theory Practice PKC, New York, NY, USA, 2006,pp. 508–524.

[6] S. Coull, M. Green, and S. Hohenberger, "Controlling access toan oblivious database using stateful anonymous credentials," inIrvine: Proc. 12th Int. Conf. Practice and Theory in PKC, Chicago, IL,USA, 2009, pp. 501–520.

BIOGRAPHY

C. Dinesh, M.Tech (C.S.E), Sr.Asst.Professor, Dadi Institute of Engg .& Tech., Anakapalli, Visakhapatnam District-531002.