SAJET

South Asian Journal of Engineering and Technology Vol.2, No.15 (2016) 145–150

ISSN No: 2454-9614

Secure Data Sharing using Attribute Based Encryption with Revocation in Cloud Computing

D. Vaduganathan[a]

[a)] *Department Of Computer Science and Engineering, Excel Engineering College, Komarapalayam, Tamilnadu, India.*

*Corresponding Author: D. Vaduganathan

E-mail:vaduganathan.kce@gmail.com

Received: 10/11/2015, Revised: 22/12/2015 and Accepted: 10/03/2016

Abstract

Cloud computing is used to providing many services like data sharing, data storage and platform, infrastructure, software. Services can be change based on the user's needs. Services can classify as public and private. Private services are used in within the organization. So that private services has the low security challenges. Public services are used by all. Security is the main challenge in public services. Data sharing is the one of the main public services used by the IT industry and many private industries. Data may be the sensitive in industry. Obviously Data sharing in cloud has the security issues. To manage the security issues in data sharing access control mechanisms are used. Attribute based encryption is one of the main access control mechanism which used to ensure the security of the data in the data sharing. Data are shared by the attributes. Here attributes are identified by the key. One of the security issues in data sharing is attributing and data sharing policies are seen by anyone. Key-escrow problem is the one of the security issue in data sharing. Key-escorw is one which is occurred by key provider itself my access the others data. Data sharing has the security issues called revocation. These are three issues in data sharing. To solve this three issues in data sharing have proposed the new attribute based encryption system. New proposed attribute based encryption uses the proxy server which is used to avoid the key- escrow problem. New attribute based encryption solves the revocation problem by re-encryption in data sharing. Attributes and policies are hidden in the new proposed attribute based encryption. So that proposed system solves the problems of attributes based encryption in data sharing. This data sharing is secured by new attribute based encryption.

Keywords– cloud computing, data sharing, access control, data storage

Reviewed by* **ICETSET'16 *organizing committee*

1. Introduction

Cloud computing is used to provide services which is used to store and retrieve the data from the cloud. Cloud services are accesses anywhere from the world. It is the one of the main advantage of cloud computing. Data sharing is the one of the services mainly used by the IT industry for store the data; access the data from the cloud

itself.

To store and access the data are done through internet. Internet is the one of cloud carrier. There is no need of additional hardware to access the data and store the data. So that many industry mostly depends on the data sharing alone. Data sharing is defined as many users can work on the same data and they can share the data. Data sharing can be done through cloud. All this data sharing can be done through cloud. Industry may use the very sensitive data. So that data sharing has many security challenges. One of the challenge is data should be shared to correct person who is belongs to the data. To avoid this challenges have choose the access control technique is attribute based encryption. ABE systems use the attributes to classify the people like HODs or Students. Attributes are like anything like dates, person's roles and time. Attributes based encryption is used to provide the secure data sharing. Data sharing gives some problems while using the attribute based encryption. Attributes systems working under the access policies. Access polices are used to share the data in between the users. Access policy is defined as who can access the particular data and who cannot access the data. This access policy is associated with data. If persons trying to access the data means access polices of the particular data should satisfy otherwise cannot access the data. In this attribute based encryption is key provider. Key providers share the key for each users based on the attributes. In this attribute based encryption there is some issues occurred in the data sharing. Revocation is one of the main in data sharing. Revocation is defined as the revoke the keys which is already given to the users. This is one of main challenge in data sharing. To resolve this problem introduce the re-encryption in the attribute based encryption. Through this re-encryption system can updates the keys. Through this can avoid the revocation in data sharing. Next issues in the data sharing are key-escrow problem which is access the data by key providers itself. To avoid this problem can introduce the proxy server. This proxy server and key provider is used to produce the keys to users. So that can avoid the key-escrow problems. Important issue in the data sharing is hiding the access policies and attributes. To avoid this can use the hashing function in new attribute based encryption.

2. Related works

Attribute based encryption is used to do the production of data based on the set of access policies and attributes. Access policies are defined as ensures that who can access the data that cannot in data sharing. But these policies not hidden in the attribute based encryption. To do the policies secrecy provides by predicate based and hierarchical predicate encryptions are used. Predicate encryptions are used to hide the access policies and attributes **[6]**. So that users cannot learn anything about the access policies and attributes. However this method is not efficient, in this method does not support for revocation property. Cloud mask is used to hide the access policies in the attribute based encryption with data sharing. It consists of set of attributes. Important role is in the cloud mask is data manager who is responsible for hiding the access policies **[5]**. However single point of failure may occur with cloud system. Predicate based encryption is used to do the inner products encryption to avoid revealing of access policy. So that attributes and access policies are cannot see by anybody. But it is not suitable when the scaling is

increasing **[5].** To improve the large numbers of users dynamically go with the hierarchical predicate based encryption which used to manage the large numbers of users in data sharing. However It has disadvantage of single point of failure. Privacy preserving attribute based encryption is used to hide the access policies and attributes by the authority. But here want to fully depend authority. The attribute based encryption wants revocation or users cancelling in the data sharing. Cannot ensure particular user always have to get the services of data sharing. Some point of time need to cancel the users or attributes to limit the users who are all accessing the data sharing. These attribute revocation is done through the following techniques. That is updating the existing keys and creates a new key for users. It is not efficient revocation. Because want to update the keys repeatedly. Another technique to revocation is to re-encryption of cipher texts. It is also not efficient for revocation. The re-encryption is defined as have to do the encryption many times. That is called as the re-encryption. Through the re-encryption can do revocation in attributes based encryption? However this needs many times **[2].**

3. Data sharing's security requirements

3.1 Data privacy

Data privacy is defined as the secrecy of data. Such that ensuring that particular data owner access their data alone, not others data. Such that data are not access by the unauthorized persons. Also it ensures that authorized persons only accessing their data.

3.2 Access policy privacy

Access policy is heart of the attribute based encryption. It works only by access policies. It gives the more security by access polices and attributes. Access policies are defined as set of polices who can access the data and who cannot access the particular data. But these policies itself sometimes not hidden. Attribute based encryption should ensure the access policies' secrecy.

3.3 Revocation policy

Revocation policy is essential for attribute based encryption. If particular user is removed from data sharing group then should update the private keys. This is defined as the revocation policy.

4. Prerequisite of Cryptography

4.1 Prerequisite

To define the attribute based encryption, it requires the following pre-requisites.

4.2 Access structure

Attribute based encryption associates with the access policies in the form of Boolean formulas. These access policies are defined in the form of tree. This is called as the access structure. Access policies are used to provide the set of rules to access the data. The rules defined for each cipher texts in data sharing. These rules used to ensure the data privacy and access policy privacy.

4.3 General ABE algorithm

Following procedures are used in the general attribute based encryption system

Setup the (Pub_Key, Mas_Key)n and decryptio: The setup phase is used to produce the public keys and private key. These keys are used to produce the encryption and decryption.

Key_gen phase: Key_gen phase is define as the key generation phase which is used to generate the attribute keys. Attribute keys is defined as the key which produced based on the attributes produce of the users. The attribute key is used to satisfy the access policy.

Encryption phase: Encryption phase is the important phase in the attribute based encryption. It consists three elements. There are message, access policy and public key. These elements are used to do the encryption in attribute based encryption.

Decrypt (Encrypt text, Private Key) →Message. In this phase decryption can be take place. Decryption can be done by the attribute keys which are used to satisfy the access policy. If Access policy is satisfies with the private key attributes then the user will get the original message.

5. Proposed Scheme

The above survey shows that most ABE algorithm can revoke the user's authority by doing update the keys again and again. But this is not efficient ABE algorithm because it doing the updating of keys each and every time. To improve attribute based encryption algorithm efficiency proposed the new ABE algorithm by using the proxy server.

5.1 Access Policy vs. Access tree

Access tree is defined as set of access formulas which is used to ensure authorized users are accessing the data. Access tree consists of Boolean formulas which are defined by the attributes. Also access tree consists the threshold values. These threshold values are used to define the access policy. Root node consists polynomial a value which is shared by sub-nodes. Secret sharing scheme is can be represented formally for each attributes (Att) formally as (y,Pol(y)) is one of the sub-node share of y^{th} attribute . In the access tree consists of root node, and root node's values can be represented by Lagrange formula defined by,

$$\text{Pol(root)} = \sum \lambda_x P(Att)$$

Where λ is the coefficient which is calculated by the difference between two attributes's index represented formally by,

$$\lambda_x = \prod \frac{Att_j}{Att_j - Att_i}$$

5.2 Proposed ABE scheme

Proposed new ABE algorithm which consists of proxy server to do the efficient revocation. This used to ensure the all security requirements in data sharing scheme. Revocation is done through the proxy server by changing the keys proxy server alone. Such that no need to change the entire public and private keys.

Setting up public and private keys

This is the first phase used to produce private and public keys. These public and private keys are used to produce the encryption and decryption. Attribute keys are also called as private keys which is used for each attribute. Here random groups G1, G2 are produced by the generator g1, g2. Then random key of a,b used to generate the public and private keys.

Example public keys can be defined by

$$Pub\_key = (G1, G2, g1, g2, g_2^{\beta}, e(g_1, g_2)^{\alpha})$$

Example of master key can be defined by,

$$Mas\_key = (a, g_2^{\alpha}, P)$$

Key generation for attributes

Key Distribution Centre is responsible for provide the keys for each attributes.

Secret key = (K,for all j € S: (Kj,Kj1,Kj2)

$$K = g1^{(a+r)/b}\ ,\ Kj = g_1^{\ r}.H(j)^{\ rjP(0)}$$

$$Kj1 = g0^{r} \qquad Kj2 = (Kj1)^{\ P(0)}$$

Encryption

Encryption is done through the data with access policies. Access policies are defined by Boolean formulas. To do the encryption access policies, data and public keys are used.

Cipher texts = $(Tree, Msge(g0,g1)^{as}, H(att(j))^{qj})$

Proxy key generation

Proxy key is defined as the key which has the revocation list that are all want to revoke from the existing groups. If want to revoke the particular user then want to add a user into the revocation list

Proxy key =($User_j$, Revocation List)

Decryption

Decryption produces the original message by the attribute key also called as private key. If Attribute key is matching with the access policy then it produces the original message. If Access policy is not satisfy by the attribute key then user is unauthorized person. Through these access policies ensure the security in the data sharing. To do decryption user also needs the proxy key

Message= (Encrypt text, Tree, Attribute key, Proxy key)

6. Conclusion

The above proposed scheme is efficient compared to all existing attributes based encryption. That is it ensures the revocation, policy and attributes hiding and finally key-escrow property.

References

[1] Hongjiao LI, Shan WANG, Xiuxia TIAN, Weimin WEI, Chaochao SUN,Daming LIU, "A Survey of Privacy-preserving Access Control in Cloud Computing,".in JCIS.
[2] Guojun Wang,Qin Liu,jie Wu "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services,"
[3] Yanbin Lu and Gene Tsudik, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption," in IEEE 2013.
[4] Fugeng Zeng, "Predicate Encryption for Inner Product in Cloud Computing,".
[5] Dan Boneh, and Amit Sahai and Brent Waters, "Functional Encryption: Definitions and Challenges,".
[6] Junbeom Hur and Dong Kun Noh"Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," IEEE 2011.
[7] Ming Li, "Authorized Private Keyword Search over Encrypted Data in Cloud Computing,".
[8] Shucheng Yu, Cong Wang,Kui Ren and Wenjing Lou"Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing," IEEE.2010.
[9] Ming Li, "Authorized Private Keyword Search over Encrypted Data in Cloud Computing,"