Secure Attribute Based Encryption with Revocation in Cloud Storage

Vaduganathan D,
Master Of Engineering
Department of Computer Science and Engineering
Angel College OF Engineering and Technology
Tirupur, India.

Ramasami S,
Assistant Professor
Department of Computer Science and Engineering
Angel College OF Engineering and Technology
Tirupur.India

Abstract– **Cloud computing is used to providing services which is used to satisfy the user's needs. Services has two types in cloud computing. They are public and private services. Private services are used by the already known users. So that private services ensuring the security in cloud computing. Public services are used by the people who are unknown. Security in public services is one of the main dispute in cloud computing. Cloud storage is the one of the main public services used by the IT industry. From this obviously cloud storage has the security issues. To manage the security issues 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 cloud storage. Cloud storage's data are accessed by the attributes. Here attributes are identified by the key which is offered based on the attributes. Therefore each attribute's group of users should have the same keys. In this scenario after providing the attribute keys to users, cancelling users attribute is an important issue. Such that cancelling the authorized rights from the users is an essential issue. Some point of time needs to cancel the authorization of users for the cloud storage. To do cancel the users is a very difficult in the attribute based encryption. To cancel the rights of users, key distribution center needs to update the keys or needs to do the re-encryption in attribute based encryption. This shows that each canceling of user's rights needs the re-encryption and updating of keys. To avoid this difficulty in the attribute based encryption introduces the placeholder. Placeholder used to avoid the re-encryption and updating the keys. Such that placeholder in the attribute based encryption involved as one of the part of half decryption in the attribute based encryption. So that each cancel of rights only needs update the keys that are used to do the parts of the decryption in attribute based encryption. This placeholder is used to cancel the attribute efficiently. Secure ABE system is used to ensure the avoid the key-escrow problem and policy privacy in the cloud computing.**

Keywords–Cloud computing, cloud storage, access control, cloud storage

I. INTRODUCTION

Cloud computing is mainly used by the IT industry for store the data, access the data from the cloud itself. Storing and accessing the data are done through internet from the cloud. There is no need of additional hardware and software to access the data and store the data in the organization. So that IT industry mostly depends on the cloud computing alone. Cloud computing main pillar is internet. There is no IT industry without internet. Using that internet IT industries perfectly getting the cloud services. Cloud provides the everything as services. Services are some functionality that is used to gratify the needs of IT industry. Building the cloud within the organization or IT industry should have the minimal security issues only. Such that there is chance of inside attackers in organization cloud. That attack can be identifiable. Building the cloud to public is important challenge in the cloud computing. This arises many security issues. Building the cloud in the public is depends on the others which are said as third parties. Third parties are responsible for providing the services from the cloud. But believing third party alone is an important trouble in the cloud computing. Data confidentiality is an important issue in the third party cloud services. To guarantee the data security in the third party cloud needs the encryption and decryption mechanisms. Thus mechanisms are provided by the access control methods. Access control is a functionality to assure the control over own data in the third party cloud. Many access control mechanisms that is used to ensure the security in the public cloud. Attribute based encryption a system is one of the main access control mechanism used to provide the security to data based on the attributes in the public cloud. Attribute based encryption is the enhancement of identity based encryption used to provide the access control in the cloud computing. Identity based encryption not efficient at some point of time. To improve this introduces the attribute based encryption system which working under attributes associated with the cipher texts. In ABE each users should have the keys for attributes. Thus attribute keys used to do the decryption in the cloud computing. Thus attribute keys are also called the access rights in the attribute based encryption. Provide this decryption a key to users is defined as the giving access rights to one user. Through the access rights user can access the public cloud. But one user is not always being a part of data. Some point of time need to remove the user from the authorized users list. It is an important issue in the attribute based encryption. Canceling the user's rights is very complex to do in the ABE. Because it needs the update of attribute keys every time while one of the user's rights is canceling. It is one of the main disadvantages. Such that to cancel particular user in the attribute, need to do the re-encryption in the ABE. Also need update the attribute keys. This is not efficient in the attribute based encryption. Each time while doing canceling of attribute, need a whole encryption and update the keys in ABE. It is very complex in the ABE. Need to do again and again update the keys. To improve ABE introduces our proposed system as algorithm with placeholder. Placeholder is like intermediate to the user and the cloud. Placeholder used to involve in the decryption part of ABE. Thus decryption can be done through the placeholder only. This placeholder method is used to avoid the re-encryption and update the attribute keys. Such that each time while doing the cancel of user's rights need not do the whole ABE algorithm again and no need to do the whole attribute key update through the placeholder. That is placeholder consists of part of keys to do the decryption. Through this advantage of placeholder while remove the user rights from the cloud no need do again and again key update and re-encryption in the attribute based encryption.

II. RELATED WORKS

Attribute based encryption is used to do the encryption and decryption based on the set of access policies. Access policies used to ensure the data secrecy. But these policies not included in the attribute based encryption. To do the policies secrecy functional encryption, key policy attribute based encryptions, cloud mask, predicate based and hierarchical predicate encryptions are used. Functional encryptions are used to hide the access policies and attributes by the access policies are associated with the keys [6]. So that users cannot learn anything about the access policies. However this security depends on the authority that is providing the decryption keys. Cloud mask is used to hide the access policies in the attribute based encryption. It consists of set of roles. Important role is in the cloud mask is data manager who is responsible for handling the access policies. However single point of failure may occur in this system. Predicate based encryption is used to do the inner products encryption. So that attributes and access policies are hidden. But it is not suitable increasing the huge number of users [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 cloud computing. It has disadvantage of single point of failure. Privacy preserving attribute based encryption used to hide the access policies by the authority. But here want to fully depend authority. The attribute based encryption wants the attributes canceling or users canceling in the cloud storage. Cannot ensure particular user always have to get the services of cloud storage. Some point of time need to remove the users or attributes to limit the users who are all accessing the cloud storage. To do the attributes canceling can survey the techniques are there in the attribute based encryption. These attribute canceling is done through the following techniques. That is updating the existing keys and produces the new keys in the attribute based encryption. It is not efficient to produces canceling of attributes. Because want to update the keys again and again. Another technique to canceling of user's rights is to re-encrypt the cipher texts. It is also not efficient. In the re-encryption is defined as have to do the encryption more than one time for each data. That is called as the re-encryption. Through the re-encryption can do the canceling of attributes. However this re-encryption is not efficient [2]. Next technique in revocation is attribute keys with the version number. The public keys are associate with the version number. The version number is increasing each time while the public key of attribute is updating. This called as the updating keys. Also want to update the secret keys in the ABE. This type of key update is difficult do for each attribute canceling [3]. Here computation overhead occurred. Patient health records are uses the ABE system. So that it needs some attribute canceling in some point of time. To do so here re-encryption of cipher texts is used. Here also doing encryption for each attribute canceling. So that it is also inefficient in attribute based encryption [4]. Lazy-canceling of attribute is re-encryption that affects the updated cipher texts only late login. This is called as the lazy re-encryption. It is also not well-organized in the ABE. Because it doing the re-encryption again and again [4]. Key escrow is the one the problem in ABE. Key-escrow is defined as the authority itself may be doing the decryption of user's data. So that security will not be in the ABE. To improve the security of ABE can avoid the key-escrow problem by 2pc communication protocol in smart grid. In the 2pc protocol is used to avoid the key-escrow problem by storage center. That is KDC and the storage center both will communicate and generate the keys for each attribute. Through the 2pc ensure the secrecy of ABE. However this cannot used in the cloud computing. In cloud computing there is no paper combining these three parameters. If some ABE satisfy the data secrecy and policy secrecy. But it will not satisfy the revocation and key-escrow problem. If some ABE satisfy the canceling of attributes but it will not satisfy the policy secrecy.

III. CLOUD STORAGE ARCHITECTURE

Cloud storage is used to store and access the large amount of data in the cloud computing. Cloud storage is main functionality used by the IT industry to access the large amount of data as well as store the large amount of data. Cloud storage is the one of the services in the cloud computing. Cloud storage examples are drop box and send space. Thus are the cloud storage used to provide the storage services. But there is no data confidentiality in the cloud storage. To improve the data confidentiality needs the access control mechanisms. Fine grained access control mechanisms are widely used in the cloud storage. Fine-grain access control mechanisms are used to ensure the data confidentiality. There many types of fine grain access control mechanism. One of the efficient mechanisms is attribute based encryption system.

SECURITY REQUIRMENTS:

DATA PRIVACY

Data privacy is the one of the requirements that is used to ensure the secrecy of data. Such that ensuring the data are not access by the unauthorized persons. That is called as the data Attribute based secrecy. Encryption should satisfy the access policy in every access and ensure the privacy of the data.

Ensure that while access policy is not satisfied then cannot decrypt the data.

Access Policy Privacy
Access policy is used to associate with the each cipher texts in the attribute based encryption. These access policies are ensuring that data are accessed by the authorized attributes only. But thus access policies are not hidden in the some of the attribute based encryption. Through these policies revealing some of the useful information gathered about the data owner and attributes. To avoid this type of non-privacy policies needs privacy for each cipher texts policies.

Involvement Conflict
Involvement conflict is one of the security requirements that is used to ensure that unauthorized users or attributes cannot decrypt the data by consolidate the every keys. Consolidate of keys occur only when access tree is not use the efficient secret sharing scheme. These type of consolidate are avoided in the attribute based encryption. Ensuring that involvement of multiple keys will not decrypt the data.
That is called as the involvement conflict. That should be removed from the attribute based encryption. These are the important requirement in ABE.

IV. PREREQUISITE OF CRYPTOGRAPHY PREREQUISITE

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

Access Structure:
Attribute based encryption has the access policies in the form of Boolean formulas. These access policies are defined in the form of access tree. This is called as the access structure of access policy. Access policies are used to provide the set of rules. The rules defined for each cipher texts in cloud storage. These rules used to ensure the data privacy such that data are accessed only by the authorized users.

Bilinear Pairings
G2 and G3 is the group. Then the bilinear pairings is used to define as g2 is the generator of G2 and g3 is the generator of G3 then the G2 and G3 generators used to produces the third group G4 which contains the generator g. That is called as the bilinear pairing.

Secret Sharing Scheme
Secret sharing scheme is used share the keys in attribute based encryption. ABE consists of access tree which is used to define the policies. These access trees are used to generate the keys for each attribute. Access tree consists of different nodes. Leaf nodes are used to denote the access tree. From the root node have to create the keys for each leaf node by secret sharing scheme. That is called as the secret sharing scheme. Hence secret sharing scheme is used to create the secret keys for each attribute in the access tree. Planned algorithm uses the polynomial function which is used to generate the keys for leaf nodes which consists set of attributes.

General Abe Algorithm:
Attribute based encryption system consists of following phases.

Setup the (PublicKey, MasterKey).In this phase general public key and master keys are produced which used to generate the cipher texts and decrypt the cipher texts

Key generation phase: In this phase takes input as the set of attributes and produces the output as the keys for each attribute which is used to satisfy the access policies in the cipher texts. Such that these keys are called as the attribute keys which is used to do the decryption in the ABE.

Encryption: In this phase ABE system will produces the cipher texts. This phase is belongs to the data owner. Before upload the data into the cloud, data owner should run this phase to ensure the data privacy. This phase takes the public key, message and access policies. Here a cipher text consists of access policies which are used to ensure who can access the data and who cannot access the data. This phase produces the output as the cipher texts.
Decrypt (Cipher texts, Secret key)→Message. In this phase after access the cipher texts using the attribute key which is provided for only authorized persons alone. This phase takes the cipher texts and secret keys and it produces the message.

V. PROPOSED SCHEME

The above literature survey shows that most ABE algorithm can cancel the user's authority by doing the re-encryption and update the keys again and again for each canceling of user's authority. But this is not efficient ABE algorithm because it doing the updating of keys each time. To improve ABE algorithm efficiency following steps are done in the proposed algorithm.

Access Tree
Access tree is used to define the set of access rules in the attribute based encryption. Access rules is defined as the Boolean formula which consists of attributes and threshold values. These threshold values are used to ensure to satisfy the access policies. Root node consists of polynomial a value which is used to share the polynomial to the multiple attributes in the root node by secret sharing method. Secret sharing scheme is can be represented formally for each attributes (A) formally as (x, Z(x)) is one of the polynomial shares of xth attribute. In the access tree consists of root node, its polynomial values can be represented by the Lagrange formula defined by,

$$\text{Z(root)} = \sum \lambda_x Z(A)$$

Where λ is the coefficient which is calculated by the difference between two attributes of index is used to divide the attribute of one index. It can be represented formally as,

$$\lambda_x = \prod \frac{A_j}{A_j - A_i}$$

Proposed Scheme Construction

Proposed scheme is used to construct the ABE algorithm which uses the placeholder to do the efficient dynamic user rights canceling. This used to improve the attribute based encryption as well as satisfying the security requirements. A dynamic user right canceling is done through the placeholder. Placeholder which is used to do the partial decryption in ABE. Each authority should have the placeholder. Placeholder has the partial decryption keys. So that decryption is not fully depends on the secret keys. Each user canceling the placeholder keys will be updated. So that can easily assure that already canceled user cannot decrypt the message through their secret keys. This is main concepts of placeholders. The placeholder will be placed for each authority in a distributed manner. The algorithm has the following phases to canceling the users dynamically,

Setting Up Public And Private Keys

In this phase public keys and master keys are generated. This public key and master keys is used to encrypt the message. Master key is further used to generate the attribute keys for every user. Here random groups G3, G4 are generated by the generator g3, g4 which are public keys. Then random values of α, β are the random keys used to generate the public key and master keys. G3, G4, α, β are the components of public key and private key. Polynomial values also the one of the master key component. Then the master key and public keys can be represented formally,

Pub_key = (group1, group2, generator of group1, generator group2, generator of group2 power random components, bilinear pair power random component)

Example of public keys can be represented as,

Pub_key = (G3, G4, g3, g4, g_4^{β}, e $(g_3, g4)^{\alpha}$)

Master key can represent by the following components,

Master_key = (random component, generator of group4 power random component, polynomial_values)

Example of master key can be represented by following,

Master_key = (β, g4α, poly_value)

Key Generation For Attributes

KDC is responsible for generating the keys for attributes by the secret sharing method. Secret sharing method is one of the methods which used to generating the shares of keys in the access trees. Polynomial values are the shares of attribute keys are shared by the secret sharing method. These secret keys are generated also by the master keys and the public keys used in the Attribute based encryption. It can be represented by following,

Attribute_key = (each attribute keys by polynomial values)

Encryption

Encryption is done through the access policy. Access policies are associated with the cipher texts. Cipher texts are produced by the data and access policies. Access polices consists of attributes which is used to satisfy with the attribute keys. Public keys and master keys are used to generate the cipher texts. Encryption can represent by the following formula,

Cipher_texts = (Access_policies, data)

Placeholderkey Generation

Placeholderkey is used to generate for each time canceling the attributes. These keys are used to do the partial decryption in the attribute based encryption. Placeholderkey are generated dynamically. This Placeholderkey is used to generate the decryption. Without this Placeholderkey cannot produce the cipher texts with secret keys. This advantage is used to do the efficient canceling user's rights through the Placeholderkey values. There is no canceling means no need to do the Placeholderkey update in the attribute based encryption. This phase is used in the cloud computing. So that can do the efficient attribute canceling the in the dynamic cloud computing. These are used to improve the attribute based encryption in the cloud computing environment. These proxies also avoid the single point of failure. Because these proxies are distributed for each authority. So that it is efficient one compared to all other attribute based encryption. These Placeholderkey of attribute based encryption in cloud computing can be represented formally by following,

Placeholder_key = (x, Z(x))

Where Z is the polynomial values for attribute and x denotes the indexes of attributes. Using this Placeholder key that generates the keys values that is used for the partial decryption.

Conversion of Placeholder Key

The Placeholderkey generation phase is used to generate the keys which his for each attribute. While doing the user's rights canceling for cloud storage Placeholder key want to update then only can assure that only non-canceling users can do the decryption. Even though the already canceled users may have the secret keys of attributes, they cannot perform the decryption operation from the cloud storage. It is one of the main phases of attribute based encryption to do the decryption efficiently in the cloud storage. So that this phase is very important phase in attribute based encryption. Because this phase of keys used to restrict the users who are having canceling rights. No need to change the attribute key for each canceling of user's rights or no need to do the re-encryption for cipher texts. These both are the advantages of Proposed ABE scheme.

Update_Placeholder_key = conversion (Placeholder _key)

The above statement shows that the new Placeholder key is used to do the dynamic canceling of user's rights.

Decryption

Decryption can be performed by the placeholders' key and the secret key. This both decryption used to get the original data from the cloud storage. This two level of decryption is used to ensure the data security and confidentiality in the cloud storage. Updated_placholder_key is used to produce the partial decryption. After that using the secret key can do the full decryption. From this can infer that two level decryption is performed in the attribute based encryption of cloud storage. Through the secret key alone cannot do anything in attribute based encryption. This type of decryption is used to ensure the efficient dynamic attribute canceling in the cloud storage.

Message= (cipher_texts, placholder_key, attribute_key)

VI SCHEME COMPARISON

SCHEME	POLICY PRIVACY	KEY ESCROW	REVOCATION
AREA:CLOUD COMUTING			
ABE-SCHEME	NO	NO	NO
RE-encryption	NO	NO	YES
LAZY-encryption	NO	NO	YES
UPDATE KEYS	NO	NO	YES
KP-ABE	Yes	NO	NO
2PC	NO	YES	NO
PE	Yes	NO	NO
PP-ABE	YES	NO	NO
Proposed Scheme	Yes	YES	YES

The above table shows that our proposed scheme is used to satisfy the secrecy of the attribute based encryption. That is ABE ensures the data secrecy and the policy secrecy. Policy secrecy is ensured by the polynomial values in the proposed scheme. Key escrow problem is avoided by the placeholder's keys. That is not just having the secret keys cannot do the decryption. Through this can ensure the prevention of key-escrow problem. Even though ABE supporting policy secrecy and the key-escrow it will not support the canceling of attributes. But our proposed scheme is support the secrecy of ABE as well as efficient canceling of attributes. Therefore can infer that proposed scheme is efficient compared to the all other schemes in the table

VI SCHEME IMPLEMENTAION

Proposed scheme is used to implement in the cp-abe toolkit which is working under the concepts of PBC library. PBC is defined as the pair wise crypto library used to use attribute based library.

VIII SCHEME SECURITY

In this paper, three security requirements such as data secrecy, policy secrecy and key-escrow are considered.

Data Privacy

Data privacy ensures that authorized person can access the data from the cloud storage. It is impossible for the unauthorized persons to access the data. This is one of the primary security requirements in the attribute based encryption system.

Access Policy Privacy

Access policy privacy ensures that access policy which is associate with cipher texts are not visible by the any users. Therefore that is called as the Access Policy privacy. Access policy privacy is ensure by our proposed algorithm uses the polynomial values. Polynomial values are used to hide the attributes. Through this can assure policy privacy in the attribute based encryption.

KEY ESCROW

Key escrow problem is defined as the authority try to access the data through the attribute keys. To avoid this proposed algorithm is used to do the decryption in the form of two levels. That is placeholder level and the secret key level. Placeholder level has the key which used for the partial decryption. After this can perform the full decryption by the secret keys. Through this can ensure that proposed algorithm does not have the key-escrow problem.

IX CONCLUSION

The above proposed scheme shows that there is no efficient algorithm in cloud computing of attributes based encryption. That is key escrow and policy hiding problems are security requirements in ABE that satisfied. Efficient user's rights canceling done without the key update and re-encryption.

REFERENCES

[1] SushmitaRuj,Milos Stojmenovic,Amiya Nayak, Jia Mo, "Decentralized Access Control with Anonymous Authentication of data stored in clouds," in IEEE Feb 2014..

[2] Shucheng Yu, Cong Wang, Kui Ren,Wenjing Lou "Attribute Based Data Sharing with Attribute Revocation," in. IEEE

[3] Guojun Wang,Qin Liu,jie Wu "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services,"

[4] Yanbin Lu and Gene Tsudik, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption," in IEEE 2013.

[5] Fugeng Zeng, "Predicate Encryption for Inner Product in Cloud Computing,".

[6] Dan Boneh, and Amit Sahai and Brent Waters, "Functional Encryption: Definitions and Challenges,".

[7] Junbeom Hur and Dong Kun Noh“Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems,” IEEE 2011.

[8] Ming Li, “Authorized Private Keyword Search over Encrypted Data in Cloud Computing,”.

[9] Shucheng Yu, Cong Wang,Kui Ren and Wenjing Lou“Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing,” IEEE.2010.

[10] Ming Li, “Authorized Private Keyword Search over Encrypted Data in Cloud Computing,”

[11] Hongjiao LI, Shan WANG, Xiuxia TIAN, Weimin WEI, Chaochao SUN,Daming LIU, “A Survey of Privacy-preserving Access Control in Cloud Computing,”.in JCIS.