Survey on Fine-Grained Access Control with Efficient Data Sharing of Cloud Storage in Cloud Computing

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.

Santhiya C
Master Of Engineering
Department of Computer Science And Engineering
Angel College OF Engineering and Technology
Tirupur. India.

Vanishree K A
Master Of Engineering
Department of Computer Science and Engineering
Angel College OF Engineering and Technology
Tirupur, India.

***Abstract*—Cloud computing storage has either files or software. Here the data are shared for authorized persons only. To ensure this confidentiality, data sharing is an important thing. To do efficient data sharing access control is applied to subject and objects. In cloud storage, access control is an important issue while sharing data with others. Main motto of this paper is to provide efficient access control with others through the fine-grained access control. Access control provides access rights for set of object entity to the exact subject. Fine grained access control provides set of rights to the specific authorized persons. Access control is of different types. In fine grained access control many encryption mechanism is used. They are Broadcast encryption, attribute based encryption, attribute-set based encryption, Hierarchical based encryption, Hierarchical attribute-set based encryption, Key-policy attribute based encryption, cipher text-policy attribute based encryption, cipher text-policy attribute-set based encryption, and patient controlled encryption. In the encryption systems the keys are forwarded to the particular user. So that the particular user can access the set of object by that user. The Access rights may be forwarded to others and cannot control the Access rights. In the existing access control encryption a lot of disadvantages are found. Thus the implementation of efficient access control is done in fine-grained access control.**

Keywords*– Cloud computing, data sharing, data storage, encryption scheme.

I. INTRODUCTION

Cloud computing is defined as the on-demanding service provided by the specific providers like Google, Amazon, Salesforce.com through the internet. It is done by a new service's interface and this is called as front end of the cloud computing. The storage cannot be viewed by the user and its maintenance depends upon the providers. i.e. Google maintains their servers in USA, The Salesforce.com maintains their servers other than USA and is called as back end of the cloud. The main advantage of cloud is back end and front end of the cloud can be accessed from anywhere in the world only by internet connection. The stored data of cloud are viewed by the interface and that is accessible from cloud. But confidential data should not be accessed by any other by providing protection over here. For this purpose, access control is applied to the data. The access control will be provided based on data and users. Data can be classified as private, public and hybrid where private data should have only the confidential information. So that it always has the access control for those data. Public data will be having non-confidential information and there is no need of high access control. Hybrid data will have combination of both the above data. Here security dependency is needed for the data. [1]

A. Cloud Storage

Cloud storage is a server managed by the hosting company. For instance, EMC corporation's ATMOS is an object storage for cloud computing. Here the data is stored as an object and those objects will be accessed from anywhere from the cloud.

B. Data sharing

It is impossible to send the cloud data from one place to another place. Then cloud loses the value of the storage. For this purpose, we go for the data sharing in cloud computing. Sharing is an important issue in cloud computing. For efficiently sharing the data, access control is used.

C. Access control

It is used to provide control to the subject for object. This is called as the access control. Here subject may be any person or people. The object entity may be either be a file or software or any type of resources.

D. *Fine-grained Access control*

In the existing system, servers contain data and the software will control who are all having access to the particular data. It will check whether the user have authorization for accessing the piece of data or not. Software is a malicious one and the people who access the server may leak the information. To avoid the above disadvantages from the server we go for fine-grained access control.

Fine-grained access control is one type of access control. Here different person will have the different access rights for the files. That is one file may be accessed by the first person, but cannot be accessed by the second person based on the identity. Identity will be admin, other than the admin different access rights are provided to each individual.

Fine-grained access control ensures that the person will access the piece of data from the server and is called the fine-grained access control. Fine-grained access control is used in all areas like personal health records, encrypted attribute searching. There are many access controls but the fine-grained access control is an efficient one for decrypting.

II. ATTRIBUTE–BASED ENCRYPTION

Attribute based encryption is one of the encryption technique used to implement the fine-grained access control in cloud computing. Attribute based encryption is used to overcome the disadvantages for each user who wants to encrypt the cipher text. This will make the performance to degrade.

To avoid the above disadvantage, attribute based encryption is used. In this encryption system, text is encrypted with public key and each user uses a decryption key to decrypt particular user's attributes and is called as the attribute based encryption. The decryption key should be matched with the attributes of cipher text and the key will decrypt the cipher text.

Here the private keys are constructed by the Access tree as in ABE system root node. The gateway is used for accessing the set attributes of child node. Let 'x' be a node means parent and is identified by the function parent(x). The attributes of the 'x' will be identified by the function attr(x).

Attribute based encryption is used in many applications. One of the applications is electronic health records management (HER). In this, each user will have the decryption key to access the cipher text of HER data. These data are accessed by the doctors. So that, the doctor will pass the access rights to other doctors as there is only single authority. This means multi-owner principle. If one doctor does modifications with the data or adds the data means cipher text grows linearly.

In the ABE system, attribute access rights are delegated to others. So that it will not support for the revocation policy and the cipher text are grows linearly, such that cost of the cloud storage is increasing. In many search-based applications the attributes are passed from the database owner. Through this, attacker may have a chance to learn all the attributes stored in the cloud server. So that attributes will not hide from the attackers. To provide a security ABE audit-logs are used. In the audit-logs, source IP address, destination IP address, L3 protocol type, source port, destination port, TOS byte and Input logical interface should be maintained. For each flow this should be maintained. So performance degradation will occur. From these fields attacker may learn about the flow. Hence, this flow attributes should be hidden from every analysts.

Data integrity in cloud service provider (CSP) is maintained by the ABE system. But it will not provide efficient integrity of data. If we use the ABE system it will have insufficient performance, data security, and flexible access control. It will mainly depend on the external level security maintenance. The audit log is an example for maintaining the security to the system.

III. MULTI AUTHORITY ATTRIBUTE–BASED ENCRYPTION

A single authority ABE is called as the single owner authority. This single authority will not control the attributes for each user and all access rights. In single authority, ABE performance degradation occurs. To cope-up the disadvantages of single authority ABE, the multi ABE system is introduced.

Multi Authority ABE is defined as the multiple monitoring systems for multiple users' attributes. Hence, multiple key issuing and monitoring improves the system performance. Exact example of this includes giving driving license by multiple authorities. This will enable the system to work in a concurrent manner. Each authority is responsible for protecting or monitoring some attributes. Each should have the unique identity to maintain consistency. The unique identification is given by the unique global identifier (UGI). In the UGI the chance of collusion will occurs in-between the authority. So that the particular user can get the complete attributes. To avoid this, attribute authorities (AA) are enabled. AA cannot learn about the other authorities' attributes. So AA makes sure about the privacy between the authorities of users. AA uses the pseudonyms to generate the unique decryption keys for each set of attributes.

Here every authority should maintain equal or considerable number of attributes. If not then it may go like a single authority scheme. Equally it should have the subset of attributes. Attribute keys may be forwarded to the others.

III. KEY-POLICY ATTRIBUTE–BASED ENCRYPTION

KP-attribute based system is defined as the private key in the form of access tree structure; through access structure, such that the tree should specify what are the cipher texts decrypted by the key and is called as the KP-policy attribute based system. Here cipher texts are associated with the set of attributes.

The KP-attribute based system is based on the predefined set of attributes and cannot handle the dynamic changes in the access structure. In KP-ABE, the keys will be forwarded to others to access same level attributes in the tree structure. But it will not satisfy the scalability and also it will not satisfy the full security. The defined KP-attribute system is a static one. Revocation is also a complex one, because we cannot predict who are all having access rights.

Here the only solution for the KP-ABE is that, it should be combined to the lazy re-encryption algorithm. Lazy re-encryption is defined as the symmetric data encryption key used to encrypt each file. The public key is used to encrypt the set of attributes which is associated to the keys. Here even the public key may be hacked by attackers. But for symmetric decryption, data encryption key should be known. So that, it may be secure. Because of this re-encryption the system will degrade its performance.

IV. CIPHERTEXT-POLICYATTRIBUTE BASED ENCRYPTION

The KP-ABE decryption key has the access structure policy. Cipher texts are associated with the set of attributes. CP-attribute based encryption is entirely opposite to the KP-ABE systems because CP-ABE is defined as the cipher texts following the access structure policy. The decrypt key is associated with set of attributes.

For the big scale organization, CP-ABE is not an efficient one. Because the key management is done by the authorized groups. There is a need for the multi authorization. Cipher texts are managed as the tree structure. Hence it should be a static one. It is not used for the dynamic delegation of access rights. We cannot do the dynamic revocation also. So that decryption key storage size is not a flexible one. Here the known attributes are logically ordered in only one set. It will not be applicable for large-scale application because of following reasons,

(i) Cloud can be used at anytime from anywhere in the world. But the memory, CPU, bandwidth are limited. Encryption system should be a high performance one.

(ii) While giving delegation of secret keys to attributes, the decision is made by the attribute authorities (AA).

(iii) In large-scale application dynamic revocation is must. CP-ABE system usually depends on the AA.

(V) CIPHER TEXT-POLICY ATTRIBUTE SET BASED ENCRYPTION

To avoid the disadvantages of CP-ABE, CP-ASBE is introduced. CP-ASBE is defined as the cipher text-policy attribute set based encryption that uses the recursive attribute sets where the user attributes are arranged in a recursive attribute set form.

{Employee name: Nathan Position: staff, developer}
{Project id: 114, position: staff}
{Project id: 115, position: developer}

The above scheme is called as the CP-ASBE. Here multiple attribute set is used for the users to support the flexibility. Through this the dynamic constraints is introduced by adding additional recursive attribute sets. All this attribute set is combined to implement the information for the users. The combining attributes from the same set can be done easily. But attribute from the different attribute set can be combined by the translation only. This problem can be overcome by the multiple values, being assigned to the different set of attributes. Through this the advantage of dynamic revocation is improved. Here the dynamic revocation can be improved to overcome the CP-ABE.

(VI) HIERARCHICAL ATTRIBUTE-BASED ENCRYPTION

Hierarchical ABE is managed by the set of hierarchical roles by providing keys to the users in the form of disjoint manner. This is called as the hierarchical-ABE system. It is used to eliminate the disadvantages of CP-ABE system. Set of roles maintained in the H-ABE system are,

(A) Role manager(RM)
(B) Domain Master(DM)
(C) User
(D) Attributes
(E) Domain

(A) Role Manager

RM is a parent of multiple domain master (DM). It's responsible is to provide keys to all domain keys. It is similar to the private key generator. It will provide the distinct keys to the domain master. It will provide the parameter for generating keys for domain master.

(B) Domain Master

Domain master is a child of Role manager (RM). The keys of each domain master are gathered from RM. Domain master provides distinct keys to the users to ensure the disjoint attributes that are accessed by the users. Domain master is responsible for managing the set users with attributes. DM is like an administrator for users and attributes. The components included are,

(i) User
(ii) Attributes

(C) Domain

Domain is an admin for whole domain masters and it is called as the domain. It has the following components,

(i) Domain Master
(ii) User
(iii) Attributes

Domain is defined as the combination of above three components. In other terms, it is like organizing people like DM, User, Attributes that are managed by the admin called domain.

There are two main disadvantages:

(i) All attributes are managed or administered by same domain master.

(ii) All admin will manage same attribute clauses. They cannot be implemented.

(iii) It will not support for multiple value assignment for attributes.

(VII) HIERARCHICAL ATTRIBUTE SET BASED ENCRYPTION

Hierarchical–ASBE is defined as the hierarchical attribute set based encryption that is used to implement multiple values assigned to the attributes and are called as the H-ASBE system. Hierarchical-ASBE is a combination of H-ABE system and the Attribute set based encryption (ASBE) system that is used to avoid the disadvantages of hierarchical attribute based encryption (H-ABE) system.

{Employee name: Nathan Position: staff, developer}
{Project id: 114, position: developer}
{Project id: 115, position: developer}

Through this implement the dynamic constraints by adding additional recursive attribute sets. Hence it is possible to implement the dynamic revocation.

However, being difficult to manage the multiple values for attributes, it improves the storage complexity. At the same level, hierarchical level persons may leak the information.

(VIII) IDENTITY BASED ENCRYPTION

Identity based encryption system (IBE) is defined based on the identity keys that are provided to decrypt the cipher texts. In the IBE, system depends on the third party trust that is PKG.PKG is used to provide the secret keys for each user based on the identity. The identity or individuality is based on the certificates. Identity is like Email address, IP address etc.,

If one person wants to send his message to another he will encrypt using public keys then send through the email. Then the receiver will decrypt using PKG. Receiver will prove his identity in PKG by getting the secret keys and decrypt the message.

IBE is not fully secure because of the following reasons and the secret approval occurs without the knowledge of the PKG. Each decryption keys gather from PKG.

(i) No key revocation

(ii) Inherent key escrow

(iii) PKG requires extremely high level of assurance

(iv) Since it holds all private keys it needs user to remain online.

(v) PKG with management of certificates

(IX) HIERARCHICAL IDENTITY BASED ENCRYPTION

Hierarchical identity based encryption includes multiple authorities that are maintained in each level. It is used to avoid the PKG distribution and the centralized key management.

The Hierarchical IBE is used for the large scale applications. Scalability is satisfied dynamically in the Hierarchical IBE systems. The above diagram shows that, the school is responsible for providing keys to math and computer science (CS) department. CS and math are responsible for providing keys to Alice and Bob. School is authorized to access the Bob's message, whereas reverse is impossible.

(i) Here same level of hierarchy may forward the keys to others.

(ii) Keys are provided by parent of child. Parent node can access all child.

(iii) Revocation is missed here.

(X) BROADCAST ENCRYPTION SYSTEM

Broadcast encryption system is defined as the numbers of recipients that are already registered. The users who have registered will receive message at a time and is called as the broadcast encryption system. Here the secret approval is avoided. That is the number of users to receive this message is limited. Algorithm consists of following,

(i) Setup
(ii) Encryption
(iii) Decryption

(i) Setup

Setup defines the number of users from 1 to n to receive the message.

.

(ii) Encryption

The (M, PK) is used to encrypt the message using the public key.
M is a message
PK is a Public key

(iii) Decryption

Decryption is defined as,
Decrypt(S, i, di, Hdr, PK) where,
S is a subset
i is a unique id
$d_{\text{iis a}}$ unique id with decryption key
Hdr is the header for broadcast message
PK is the public key

However this scheme will leak the keys information to others since, no timestamp of keys is maintained. Once received, the key can be ceased continually. There is no running out time for the keys and it will not provide the full security.

(XI) PATIENT CONTROLLED ENCRRYPTION SYSTEM

Patient controlled encryption system refers to the sharing of health care data partially to others. It improves the privacy of healthcare information. Here, on decomposing the medical data, patient controlled encryption consists of three steps where first step generates the root key, second produces the subcategory name with encryptions and the third produce the decryption with name of the category and its secret key.

(X) CONCLUSION

The above survey shows that the fine-grained access control. Fine-grained access control has Broadcast encryption, attribute based encryption, attribute-set based encryption, Hierarchical based encryption, Hierarchical attribute-set based encryption, Key-policy attribute based encryption, cipher text-policy attribute based encryption, cipher text-policy attribute-set based encryption, and patient controlled encryption techniques. Through this can get the overall view of fine-grained access control system.

REFERENCES

[1] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted data, "in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS ’06). ACM, 2006, pp. 89–98.

[2] M. Chase and S. S. M. Chow, “Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,” in ACM Conference on Computer and Communications Security, 2009, pp. 121–130.

[3] Jinguang Han, Willy Susilo, and Yi Mu, “Privacy-Preserving Decentralized Key-Policy Attribute Based Encryption,” in. IEEE, 2012.

[4] Suhair Alshehri, and Stanisław P. Radziszowski, and Rajendra K. Raj, “Secure Access for Healthcare Data in the Cloud Using Ciphertext-Policy Attribute-Based Encryption,” in IEEE ,2012.

[5] Guojun Wang, Qin Liu and Jie Wu, “Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services,” in *Proceedings of IEE*, pp. 121–130..

[6] N.krishna and L.Bhavani, “HASBE: A Hierarchical Attribute Set Based Encryption For Flexible,Scalable And Fine Grained Access Control In Cloud Computing” Appears in International Journal of Computer & Organization Trends –Volume 3 Issue 9 – Oct 2013.

[9] Dan Boneh, Matthew Franklin, “ Identity-Based Encryption from the Weil Pairing” Appears in SIAM J. of Computing, Vol. 32, No. 3, pp. 586-615, 2003.

[10] Seung-Hyun Seo, O. Xiaoyu Ding, “Server-Aided Hierarchical Identity-Based Encryption, "Fourth International Conference on Emerging Intelligent Data and Web Technologies.2013

[11] Dan Boneh, Craig Gentry,“Collusion Resistant Broadcast Encryption With Short Ciphertexts and