Encryption Based Access Control Model In Cloud: A Survey

Rachana Chavda, Rajanikanth Aluvalu
Department of C.E, School of Engineering, R.K. University, Rajkot
e-mail: chavda.rachana@gmail.com, rajnikanth.aluvalu@rku.ac.in

Abstract

Cloud computing is known as "Utility". Cloud computing enabling users to remotely store their data in a server and provide services on-demand. Since this new computing technology requires user to entrust their valuable data to cloud providers, there have been increasing security and privacy concerns on outsourced data. We can increase security on access of the data in the cloud. Morever we can provide encryption on the data so third party can not use the data. In this paper we will be reviewing various encryption based access control model for enhancing cloud security along with their limitations. We will be concluding with a proposed access control model to enhance cloud security.

Keywords*: Cloud Computing, Access Control, Security Encryption, Encryption Techniques*

1. Introduction

Cloud computing is an internet based model that enable convenient on demand and pay per access to pool of shared resources. It is a new technology that satisfies a users requirement for computing resources like networks, storage, servers, services and application without physically acquiring them. Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a utility over a network (typically the Internet).

Cloud computing refers to the application and service that run on a distributed system using virtualized resources and access by common internet protocol and networking standard. Cloud computing virtualizes system by pooling and sharing resources. System and resources can be monitored from central infrastructure as needed. Its required High security.

The cloud environment is a large open distributed system. It is important to preserve the data, as well as, privacy of users. Access Control methods ensure that authorized users access the data and the system. Access control is generally a policy or procedure that allows, denies or restricts access to a system. It may, as well, monitor and record all attempts made to access a system. Access Control may also identify users attempting to access a system unauthorized. It is a mechanism which is very much important for protection in computer security supported by cloud. [9]

Access control is the selective restriction of access to a place or other resources, the act of accessing may mean consuming, entering, or using. Permission to access a resource is called authorization. Locks and login credentials are two analogous mechanisms of access control.

The major problem In cloud computing is, The data owners and service providers are not in the same trusted domain in cloud computing. So there is a need to prevent the data by encrypt it in some format that is not understood by third party. So here we will discuss various encryption techniques of access control model. [2]

2. Encryption Techniques

There are various type of access control techniques that utilizes cryptographic algorithms depending upon the availability of the computing resources. The system model of the cryptographic based access control is shown in Figure 1. [15]

Received December 19, 2014; Revised February 5, 2015; Accepted February 22, 2015

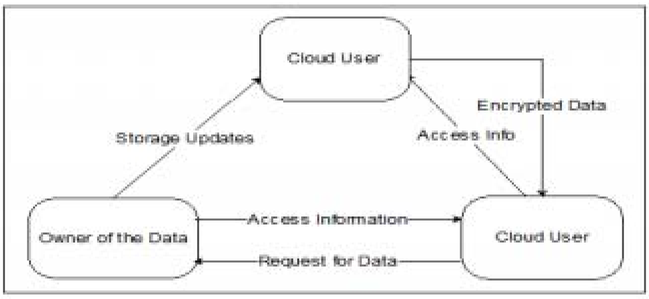

Figure 1. Encrypted Data Access Model [15]

In paper [7] says that file encryption mechanism includes metadata attached to the protected object that contains information about how to decrypt the protected object. This metadata is part of the encrypted file header and is always inserted at the beginning of the file. This metadata allows individual users to access the file. Two keys used for encrypting a file:
(1) Symmetric Key (2) Encrypted Symmetric Keys (ESK).
Let us understand various Encryption Techniques.
Bilinear maps
Bilinear maps are the pairing based crypto, it can Establish relationship between cryptographic groups. [6] It is used in encryption.

Table 1. Bilinear Mapping [6]

Let G_1, G_2, and G_t be cyclic groups of the same order
Bilinear map from :$G_1 \times G_2$ to Gt is a function
e: $G_1 \times G_2 \Rightarrow G_t$
G_t such that for all u belongs to G_1, v belongs to G_2, and a, b belongs to Z

The above table is the definition of the bilinear map algorithm and the figure 3 shows the working architecture of the bilinear mapping techniques

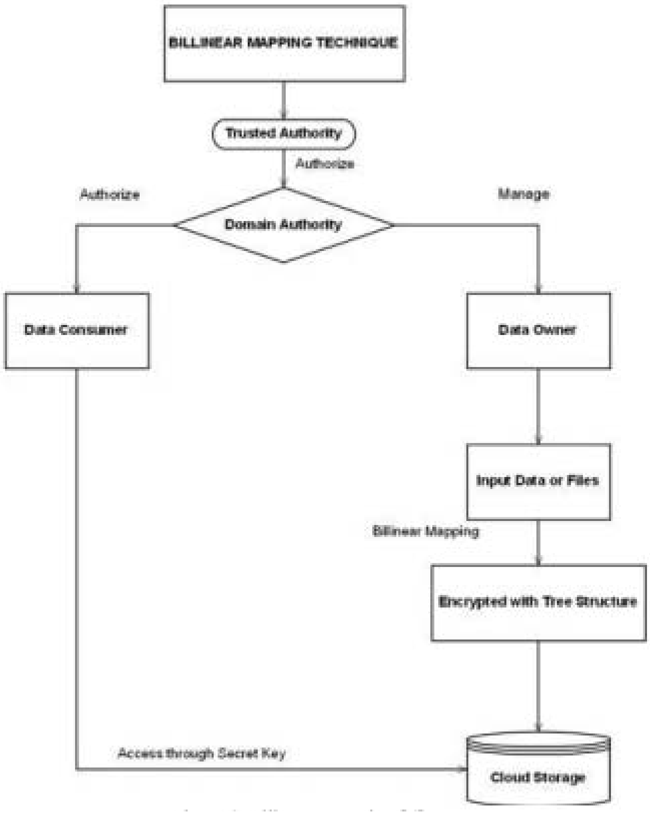

Figure 2. Bilinear Mapping [6]

A. ABE (Attribute Based Encryption)

Users need to share sensitive objects with others based on the recipients ability to satisfy a policy in distributed systems. One of the encryption schemes is Attribute Based Encryption (ABE) which is a new paradigm where such policies are specified and cryptographically enforced in the encryption algorithm itself. [2]

Sahai and waters first introduce ABE scheme to enforced access control through public key cryptography. At that time main goal of these model was provide security and access control. [14] Data Encrypt in does not require a trusted data server. The server directly upload the encrypted file without knowing plaintext. But here server know the encryption pattern of the usres which allows it to infer some information about the queries.

Issues of ABE:

It use single trusted authority (TA) in the system. Trusted authority (TA) creates a load bottleneck and have key escrow problem since the TA can access all the encrypted files.

B. KP-ABE (Key Policy Attribute Based Encryption)

Key Policy Attribute Based Encryption was proposed in paper [16]. It is the modified form of the classical model of ABE. This scheme enables a data owner to reduce most of the computational overhead to cloud servers. In this technique file or message is encrypted with a symmetric data encryption key (DEK), which is again encrypted by a public key corresponding to a set of attributes in KPABE, which is generated corresponding to an access structure.

[2] Message or the data file that is encrypted is stored with the corresponding attributes and the encrypted DEK. Only if the corresponding attributes of a file or message stored in the cloud satisfy the access structure of a user's key, then the user is able to decrypt the encrypted DEK, which is used to decrypt the file or message.

Issues of KP-ABE:

The main drawback of the scheme is that the data owner is also a Trusted Authority (TA) at the same time. If this scheme is applied to a PHR system with multiple data owners and users, it would be inefficient because then each user would receive many keys from multiple owners, even if the keys contain the same set of attributes.

C. CP-ABE (Ciphertext Policy Based Encryption)

Another modified form of the ABE is CP-ABE which is introduced by Sahai in paper [16]. Previous ABE systems used to the outsourced data can be described and built policies into users keys. While in this system attributes are used to describe a users credentials, and a party encrypting data determines a policy for decrypt. In ciphertext-policy attribute-based encryption (CP-ABE), depends how attributes and policy are associated with cipher texts and users decryption keys. The confidentiality of the data will be compromised, if any server storing the data is compromised. The storage server is untrusted if the data can be confidential by this technique. In this scheme the ciphertext is encrypted with a tree access policy chosen by an encryptor, while the decryption key is genenerated with respect to a set of attributes. [2]

Issues of CP-ABE:
Basic CP-ABE schemes are not enough to support access control in modern enterprise environments, require considerable flexibility and efficiency in specifying policies and managing user attributes.

D. CP-ASBE (Ciphertext Policy Attribute Set Based Encryption)

In the CP-ABE scheme decryption key has support to known attributes arrangement in only one set. So users can use all possible combinations of the attributes from the single set itself to satisfy Ciphertext policy. To deal with this drawback, Bobba et al Ciphertext attributes set encryption scheme is introduced. This organizes user attributes into a recursive set structure. [17]
{Employee: Ifica, Post: Auditor, Business Analyst,
{Project Id: 121, Post: Auditor}
{Project Id: 230, Post: Business Analyst}}

ASBE can support dynamic constraints on combining attributes to satisfy a policy so that it provide greater flexibility in access control. As a recursive attribute set is assigned to a user in the ASBE scheme, attributes from the same set can be easily combined, while attributes from different sets can only be combined with the help of translating items using ASBE. This problem can be solved simply by assigning multiple values of the group of attributes in different sets. Existing ABE schemes are not suitable for some applications where efficient ciphertext policy encryption of ABSE is more effectively used. ASBE's capability of assigning multiple values for the same attribute enables it to solve the user revocation problem efficiently, which is difficult in CP-ABE [10]

Issues of CP-ABE:

The challenge in constructing a CP-ASBE scheme is in selectively allowing users to combine attributes from multiple sets within a given key while still preventing collusion, i.e., preventing users from combining attributes from multiple keys.

E. IBE (Identity Based Encryption)

In an identity-based encryption scheme, an arbitrary key is used as the key for data encryption and for decryption, a key is mapped by a key.
authority. [13]

Issues of IBE:
Key management overhead. [3]

F. HIBE (Hirarchical Identity Based Encryption)

It is the extended form of IBE. The concept of HIBE scheme help to explain security. In a regular IBE (1-HIBE) scheme; there is only one private key generator (PKG) that distributes private keys to each users, having public keys are their primitive ID (PID) arbitrary strings. A two-level HIBE (2-HIBE) scheme consists of a root PKG, domain PKGs and users, all of which are associated with PID's. A user's public key consists of their PID and their domain's PID (in combine, called an address). In a 2-HIBE, users retrieve their private key from their domain PKG. Private key PK of any user in their domain can be computed by Domain PKGs, provided they have previously requested their domain secret key -SK from the root PKG. Similarly, is for number of sub-domains. There also includes a trusted third party or root certificate authority that allows a hierarchy of certificate authorities: Root certificate authority issues certificates for other authorities or users in their respective domains. The original system does not allow for such structure. However, a hierarchy of PKGs is reduces the workload on root server and allows key assignment at several levels. [13]

G. HABE (Hirarchical Attribute Based Encryption)

It is designed to achieve fine-grained access control in cloud storage services. It is a combination of HIBE and CP-ABE. In the HABE scheme, there are multiple keys with different usages. HABE uses disjunctive normal form policy. It assumes all attributes in one conjunctive clause those are administrated by the same domain master.

Issues of HABE:
Issues with multiple values assignments.

H. Distributed Attribute - Based Encryption

In DABE, there will be an arbitrary number of parties to maintain attributes and their corresponding secret keys. There are three different types of entities in a DABE scheme [9] 1. The master is responsible for the distribution of secret user keys. However, master is not involved in the creation of secret attribute keys. 2. Attribute authorities are responsible to verify whether a user is eligible of a specific attribute; in this case they distribute a secret attribute key to the user. An attribute authority generates a public attribute key for each attribute it maintains; this public key will be available to all the users. Eligible users receive apersonalized secret attribute key over an authenticated and trusted channel. 3. Users can encrypt and decrypt messages. To encrypt a message, user should formulate the access policy in Disjunctive Normal Form (DNF). To decrypt a ciphertext, a user needs at least access to some set of attributes which satisfies the access policy. The main advantage of the solution is each user can obtain secret keys from any subset of the Trusted Authorities (TAs) in the system.

Limitations of DABE:

It requires a data owner to transmit an updated ciphertext component to every non-revoked user. While sharing the information the communication overhead of key revocation is still high. [3]

I. HASBE (Hirarchical Attribute Set Based Encryption):

The HASBE scheme extends the ASBE scheme to handle the hierarchical structure. The trusted authority is responsible for managing top-level.domain authorities. It is root level authority. A HASBE scheme for scalable, flexible, and finegrained access control in cloud computing. The HASBE scheme consists of hierarchical structure of system users by using a delegation algorithm to CP-ASBE. HASBE supports compound attributes due to flexible attribute set combinations as well as achieves efficient user revocation because of attributes assigned multiple values. Thus, it provides more scalable, flexible and fine grained access control for cloud computing. [2]

Limitations of HASBE:

Compared with ASBE, this scheme cannot support compound attributes efficiently and does not support multiple value assignments.

3. Proposed System

The proposed scheme HASBE on security features in implementing access control for cloud computing. [13]

A. Scalability

We extend ASBE with a hierarchical structure to effectively delegate the trusted authority's private attribute key generation operation to lower-level domain authorities. By doing so, the workload of the trusted root authority is shifted to lower-level domain authorities, which can provide attribute key generations for end users. Thus, this hierarchical structure achieves great scalability. Only has one authority to deal with key generation, which is not scalable for large-scale cloud computing applications.

B. Flexibility

HASBE organizes user attributes into a recursive set structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. So HASBE can support compound attributes and multiple numerical assignments for a given attribute conveniently.

C. Fine-grained access control

Based on HASBE, our scheme can easily achieve fine-grained access control. A data owner can define and enforce expressive and flexible access policy for data files as the scheme.

D. Efficient User Revocation

To deal with user revocation in cloud computing, we add an attribute to each user's key and employ multiple value assignments for this attribute. So we can update user's key by simply adding a new expiration value to the existing key. We just require a domain authority to maintain some state information of the user keys and avoid the need to generate and distribute new keys on a frequent basis, which makes our scheme more efficient than existing schemes.

E. Expressiveness:

In HASBE, a user's key is associated with a set of attributes, so HASBE is conceptually closer to traditional access control methods such as Role-Based Access Control (RBAC). Thus, it is more natural to apply HASBE, instead of KP-ABE, to enforce access control.

Table 2. Comparison of Various ABE Based Access Control Techniques [13]

Techniques	Access Control	Scalability	Efficiency	Flexibility	Security
ABE	High	High	Low	High	Low
KPABE	High	Low	Low	Low	Low
IBE	Low	Low	Low	Low	High
HABE	High	High	Low	Low	Low
DABE	Low	Low	High	Low	High

4. Conclusion

This paper gives brief introduction about cloud computing and access control and various encryption techniques. Here we conclude that the HASBE scheme seamlessly incorporates a hierarchical structure of system users by applying a delegation algorithm to ASBE. HASBE scheme enforce the realization of scalable, flexible, and fine-grained access control in cloud computing.

References

[1] D Hephzi Rachel, S Prathiba. "An Enhanced HASBE for Cloud Computing Environment". *IJCSMC*. 2013; 2(4): 396 –401.

[2] Vahidhunnisha J, Ramasamy S, Balasubramaniam T. "Survey on Multi Authority Attribute Based Encryption for Personal Health Record in Cloud Computing". *International Journal of Latest Trends in Engineering and Technology (IJLTET)*. 2013; 3(2).

[3] Minu George, Dr C Suresh Gnanadhas, Saranya K. "A Survey on Attribute Based Encryption Scheme in Cloud Computing". *International Journal of Advanced Research in Computer and Communication Engineering*. 2013; 2(11).

[4] Zhibin Zhou, Dijiang Huang. “On E±cient Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption”.

[5] S Seenu Iropia, R Vijayalakshmi. “Decentralized access control of data stored in cloud using key policy attribute based encryption”. *International Journal of Inventions in Computer Science and Engineering*. 2014; 1(2).

[6] Bibin K Onankunju. “Access Control in Cloud Computing”. *International Journal of Scientific and Research Publications*. 2013; 3(9).

[7] Sonam Chugh, Sateesh Kumar Peddoju. “Access Control Based Data Security in Cloud Computing”. *International Journal of Engineering Research and Applications (IJERA)*. 2012; 2(3).

[8] Md Akram Ali, Ch Pravallika, PVS Srinivas. “Multi-Attribute Based Access Control Policy Enforcement for File Accesses in Cloud”. *International Journal of Engineering Science and Innovative Technology (IJESIT)*. 2013; 2(5).

[9] Natarajan Meghanathan. “Review of Access Control Models for Cloud Computing”. *ICCSEA, SPPR, CSIA, WimoA*. 2013: 77–85. © CS & IT-CSCP 2013

[10] VS Dhumal, Prof DN Rewadkar. “Hierarchical CP-ASBE Scheme in Cloud Computing for fine-Grained Access Control with Scalability and Flexibility”. *International Journal of Advanced Research in Computer Science and Software Engineering*. 2013; 3(11).

[11] D Hephzi Rachel, S Prathiba. “An Enhanced HASBE for Cloud Computing Environment”. *IJCSMC*. 2013; 2(4): 396 –401.

[12] S Gokuldev, S Leelavathi. “HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control by Separate Encryption/Decryption in Cloud Computing”. *International Journal of Engineering Science and Innovative Technology (IJESIT)*. 2013; 2(3).

[13] N Krishna, L Bhavani. “HASBE: A Hierarchical Attribute Set Based Encryption for Flexible, Scalable and Fine Grained Access Control in Cloud Computing”. *International Journal of Computer & Organization Trends*. 2013; 3(9).

[14] Rajesh Gaikwad, Prof Dhananjay M Dakhane, Prof Ravindra L Pardhi. ”Implementation and Analysis of Network Security using HASBE*”. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*. 2014; 3(2).

[15] Sultan Ullah, Zheng Xuefeng Zhou Feng. “TCLOUD: A Multi–Factor Access Control Framework for Cloud Computing”. *International Journal of Security and Its Applications*. 2013; 7(2).

[16] V Goyal, O Pandey, A Sahai, and B Waters. “*Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data*”. Proc.13th ACM Conf. Computer and Comm. Security (CCS ’06). 2006: 89-98.

[17] R Bobba, H Khurana, and M Prabhakaran. “*Attribute-sets: A practically motivated enhancement to attribute-based encryption*”. In Proc. ESORICS, Saint Malo, France. 2009.

[18] A Sahai and B Waters. “*Fuzzy Identity-Based Encryption*”. Proc. Of Eurocrypt’05, Aarhus, Denmark. 2005.