Access Control: Ciphertext Policy - Attribute Based Encryption in Cloud Computing

Norhidayah Muhammad 1, Jasni Mohd Zain 2

1Departme Faculty of Computer & Mathematical Sciences, Universiti Teknologi Mara, 40450, Shah Alam, Selangor, Malaysia.

Email: hidayahmuhd@unisza.edu.my

Abstract. Access control and confidentiality is important features for cloud storage. The cloud service allows data owner to outsource their data to the cloud and through which provide the data access to the users. Although cloud computing brings many benefits, it may suffer from conventional distributed systems’ security attacks. Because the cloud server and the data owner are not in the same trust domain, the semi-trusted cloud server cannot be relied to enforce the access policy. However, storing the data in the untrusted cloud server leads the privacy and access control issues in the cloud. The traditional encryption schemes such as symmetric and asymmetric schemes are not suitable to provide the access control due to lack of flexibility and fine-grained access control. One of the prominent cryptographic technique to provide privacy and fine-grained access control in cloud computing is Attribute Based Encryption. In this paper, access control ABAC framework will be introduced for cloud storage systems that achieves fine-grained access control based on an adapted Ciphertext-Policy Attribute-based Encryption (CP-ABE) approach.

1. Introduction

These Cloud services is a key focus in many areas today, especially in business, banking, health, education and more. This is because all daily business today uses a computer system because all information is digitally stored, and this will involve large data and requires large storage. Therefore, cloud computing is an option for users to store data. This is because cloud computing makes it easy for users to manage large data. Using cloud services, consumers can save on costs because they only need to cover the cost of used storage only, and it's lower than the cost of setting up their own servers since server handling is costly. Cloud provides a lot of benefits such as cost savings in investments, less maintenance, flexibility, less environment impact, scalability, and access anywhere. However, it raises security concerns relating to the shared data, since the cloud storage servers and data owners are not in the same domain [1]. The problem with cloud storage is data privacy and access control, because storing data in the cloud means it is stored in third party Cloud Service Provider (CSP) who may not trusted. Therefore, it makes access control over the shared data a challenging issue in cloud computing security.

As shown in figure 1, four security features need to be present in cloud computing to prevent invasion of client data. These four are access control, authentication, confidentiality, and reliability. The access control model is implemented to ensure that their data stored in cloud storage servers are accessed by legitimate users. Access control is significantly more than just enabling people to access the building, access control also helps to protect the data from various types of intruders and it is up to organization’s access control policy to address which method works best for the organization. Access control is more
than just controlling which users (subjects) can access which computing and network resources. In addition, access control manages users, files and other resources. It controls user’s privileges to files or resources (objects). In access control systems various steps like, identification, authentication, authorization and accountability are taken before actually accessing the resources or the object in general.

2. Access Control
There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data. As shown in Figure 2, there are four familiar logical access control model used in cloud computing:

2.1. Role-based access control (RBAC):
RBAC is a natural way to provide security because it only allows employees to access information they need to do their jobs based on role that was assigned. RBAC can minimizes the damage of information by intruders. Disadvantage of RBAC is based on the privilege of role change, permissions associated with each role can be deleted or changed. RBAC also does not consider the time and location constraints, it does not support active responsibilities as it does not separate tasks form roles, it has to deal with a lack of sophisticated semantic models.

2.2. Discretionary access control (DAC):
DAC is an access control method in which owners or administrators of the protected system, data or resource set the policies defining who or what is authorized to access the resource. Many of these systems enable administrators to limit the propagation of access rights. Disadvantage of DAC is a lack of centralized control or deal with Trojan horses that can inherit access permissions and that can violate the integrity and confidentiality of objects. DAC model is generally less secure than MAC model, so it not require a high level of protection.

2.3. Mandatory access control (MAC):
MAC is a security model in which access rights are regulated by a central authority based on multiple levels of security. Often used in government and military environments, classifications are assigned to system resources and the operating system or security kernel, grants or denies access to those resource objects based on the information security clearance of the user or device. Disadvantage of MAC is very
expensive and difficult to deploy and does not support: separation of duties, least privilege, and delegation or inheritance principles. Also dynamic activation of access rights for certain tasks is not supported. Moreover, it also does not support time and location constraints as RBAC.

2.4. Attribute-based access control (ABAC):
ABAC is a methodology that manages access rights by evaluating a set of rules, policies and relationships using the attributes of users, systems and environmental conditions. An attribute can be a user’s work start date, a location of a user, a role of a user, or all of them. Attributes may or may not be related to each other.

![Access Control Models](image)

**Figure 2:** Access Control Models

There are two access control model often used by an organization to secure data in cloud storage, which is RBAC and ABAC models. In RBAC model, a user will be assigned with a specific roll and each roll was assigned with permission or access. RBAC more implemented in big organization with more job scope. With RBAC, every action that can be carried out in a system is tied to a complex set of role combinations. If a new role is introduced, every action that this new role can access must be updated. There are two access control model often used by an organization to secure data in cloud storage, which is RBAC and ABAC models. In RBAC model, a user will be assigned with a specific roll and each roll was assigned with permission or access. RBAC more implemented in big organization with more job scope. With RBAC, every action that can be carried out in a system is tied to a complex set of role combinations. If a new role is introduced, every action that this new role can access must be updated.

Attribute Based Access Control (ABAC) is a scheme that provides logical access control. It is distinguishable because it controls access to objects by checking the rules against the attributes of object, operations, and the environment related to a request. The access control policies that can be implemented in ABAC are restricted only by the computational language and the bounty of the available attributes. Figure 3 show ABAC process. User attribute must match with access policy to get the permission to access the data.
3. Attribute Based Encryption
Sahai and Waters [2] made some initial steps to improve the primitives existing encryption scheme with one-to-one communication features by introduced the concept of Attributed Based Encryption (ABE). The idea of ABE is grouping technique, means that user or decryptor will be scale in group. Therefore, one ciphertext can be decrypted by one group of users with certain attribute, stated in access policy by encryptor. ABE scheme has obvious advantages in terms of efficiency and is fit for large scale network environment, such as cloud systems. In an ABE system, a user’s keys and ciphertexts are labeled with sets of descriptive attributes and a particular key can decrypt a particular ciphertext only if there is a match between the attributes of the ciphertext and the user’s key.

The ABE scheme is allowed for decryption when at least k attributes overlapped between a ciphertext and a private key. While this primitive was shown to be useful for error-tolerant encryption with biometrics, the lack of impressibility seems to limit its applicability to larger systems. Attribute-based encryption (ABE) enforces encrypted data to be decrypted with a secure access control mechanism that the assigned attributes must satisfy the access policies associated with ciphertext and private keys [3]. ABE has become a promising cryptographic primitive providing one-to-many encryption.

4. Ciphertext Policy – Attribute Based Encryption
After the notion of Attribute-based Encryption (ABE) was introduced by Sahai and Waters (Sahai and Waters 2005), After that [4] has proposed the first KP-ABE system, in which ciphertexts are associated with attributes, and secret keys are associated with access policies. Then BSW [5] has proposed CP-ABE scheme contrast with KP-ABE where attribute is associated with private key and access policy is associated with ciphertext and become better than Key Policy-Attribute Based Encryption (KP-ABE) based on specification of CP-ABE provide fine-grained access control, CP-ABE scheme in which the data owner hold direct control on access policy and decide who should or should not have access to the ciphertext [6].

Then, Cheung and Newport [7] proposed another CP-ABE in which the access structures are AND gates. Both scheme is based on bilinear map and pairing based cryptography practically implementing fine grained access control for data owner to control deep security and very usable in cloud system.

The second algorithm is encryption. After the master public key is generated, the data owner can apply from the key authority and can encrypt the data using the master public key that is given and also defines the access policy for the ciphertext. Only the attributes mentioned in the access policy that will successfully access the ciphertext.

The third algorithm is keygen. Keygen algorithm operates to generate decryption key or private key for the user to decrypt the ciphertext. The key authority will validate user attribute and then use the master secret key and combined with user attribute to create user private key.

The fourth algorithm is decryption. In this algorithm, the user will use the private key that has been generated in the keygen algorithm to decrypt the ciphertext. If the attribute contained in the private key match with the attribute in the access policy then the process decrypt will succeed.

![Figure 3: Attribute Based Access Control Process](image-url)
4.1. Attribute

Each user has their own attribute. The total attribute of each user can be the same or not, it depends on the role being held. For example A an attribute. Let \{ A_1, A_2, ..., A_n \} be the set of all attributes. Therefore, it could be attribute for John = \{A_1, A_3, A_4\}, and attribute for Bella = \{A_2, A_3, A_4\}. A can decrypt a ciphertext under any access policy P satisfying P \subseteq A [8].

4.2. Access Policy

Access policy is important component in ABAC and CP-ABE scheme. It because access policy used by data owner to setup or determine group of user that can be access the data. In this CP-ABE, access policy will be associated with ciphertext and attribute will be combine with private key. Several types of access structure have been proposed to represent access policies, including threshold gates [5], the LSSS matrix [9], AND gates [7] and the distribution matrix [10].
5. Conclusion

Access control decisions are very important for any shared system such as cloud storage. However, for a large distributed system like a cloud system, access decision needs to be more flexible and scalable. This paper highlights features of attribute based access control features, which are important for designing an attribute based access control. ABAC is suitable to implemented in cloud because has a find grain access control. CP-ABE is secure scheme that using attribute and access policy as a component to control assessment of the data.

[1] Wang, Z. Security and privacy issues within the Cloud Computing Computational and Information Sciences (ICCIS), 2011 International Conference on. 2011. IEEE.

[2] Sahai, A. and B. Waters Fuzzy identity-based encryption Annual International Conference on the Theory and Applications of Cryptographic Techniques. 2005. Springer.

[3] Zhang, Y., D. Zheng, and R.H. Deng Security and privacy in smart health: efficient policy-hiding attribute-based access control IEEE Internet of Things Journal 2018 5(3): p 2130-2145

[4] Goyal, V., et al. Attribute-based encryption for fine-grained access control of encrypted data Proceedings of the 13th ACM conference on Computer and communications security. 2006. Acm.

[5] Bethencourt, J., A. Sahai, and B. Waters Ciphertext-policy attribute-based encryption IEEE Symposium on Security and Privacy. 2007. IEEE.

[6] Vaanchig, N., W. Chen, and Z. Qin Ciphertext-Policy Attribute-Based Access Control with Effective User Revocation for Cloud Data Sharing System International Conference on Advanced Cloud and Big Data (CBD). 2016. IEEE.

[7] Cheung, L. and C. Newport Provably secure ciphertext policy ABE Proceedings of the 14th ACM conference on Computer and communications security. 2007. ACM.

[8] Liu, Z., Z. Cao, and D.S. Wong Efficient generation of linear secret sharing scheme matrices from threshold access trees Proc. IACR. 2010.

[9] Waters, B. Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization International Workshop on Public Key Cryptography. 2011. Springer.

[10] Balu, A. and K. Kuppusamy An expressive and provably secure ciphertext-policy attribute-based encryption Information Sciences 2014 276: p 354-362