

A Novel Approach for Attribute Based Encryption in Cloud Computing

¹S.Sailaja, ²Sayyed Nagul Meera

^{1,2}Dept. of CSE, St.Mary's Group of Institutions, Chebrolu Village, Chebrolu Mandal, Guntur, AP, India

Abstract

In Attribute-Based Encryption (ABE) scheme, attributes play a very important role. Attributes have been exploited to generate a public key for encrypting data and have been used as an access policy to control users' access. The access policy can be categorized as either key-policy or cipher text-policy. In this paper, we describe a CP-ABE based encryption scheme that provides fine-grained access control. In a CP-ABE scheme, each user is associated with a set of attributes based on which the user's private key is generated. Contents are encrypted under an access policy such that only those users whose attributes match the access policy are able to decrypt.

Keywords

Cloud Computing, Access Control, Data Security, Key Generation

I. Introduction

Internet technology is growing more and more quickly, and people can process, store, or share with their data by using its ability. Recently, the cloud has emerged to provide various application services to satisfy users' requirement [1]. In the storage service application, the cloud can let the user, data owner, store his data, and share this data with other users via the cloud, because the cloud can provide the pay as you go environment [8] where people just need to pay the money for the storage space they use. It can bring down the cost efficiently for people. But, there is a problem that the data owner has to solve it. The data owner needs to make a flexible and scalable access control policy to command users' access right, so that only the authorized users can access [6].

Besides, for protecting the confidentiality of the stored data, the data must be encrypted before uploading to the cloud [9]. Traditional public key infrastructure can be adopted in the data encryption process, and the data owner uses data users' public key to encrypt this data before uploading to the cloud; if the data user sends through a access request to the cloud, then the cloud would return the corresponding cipher text to the data user. An user would use his private key to decrypt this data. But this manner would lead to some problems: (1) to be able to encrypt data, the data owner needs to obtain the data user's public key to complete this; (2) a lot of storage overhead would spend because of the same plaintext with different public keys.

For improving these disadvantages, Sahai and Waters proposed an Attribute-Based Encryption (ABE) scheme [7] in 2005, and this paper proposed the first concept of the attribute-based encryption scheme. The ABE scheme used an user's identity as attributes, and a set of attributes were used to encrypt and decrypt data. The ABE scheme can result the problem that data owner needs to use every authorized user's public key to encrypt data. And in the same year, Nail et al. proposed an threshold attribute-based encryption which can prevent the collusion attacks [5].

A. The criteria of the Attribute-based Encryption

1. Data confidentiality

Before uploading data to the cloud, the data was encrypted by the data owner. Therefore, unauthorized parties including the cloud cannot know the information about the encrypted data.

B. Fine-Grained Access Control

In the same group, the system granted the different access right to individual user. Users are on the same group, but each user can be granted the different access right to access data. Even for users in the same group, their access rights are not the same.

C. Scalability

When the authorized users increase, the system can work efficiently. So the number of authorized users cannot affect the performance of the system.

D. User Accountability

If the authorized user is dishonest, he would share his attribute private key with the other unauthorized user. It causes the problem that the illegal key would share among unauthorized users.

E. User Revocation

If the user quits the system, the scheme can revoke his access right from the system directly. The revocable user cannot access any stored data, because his access right was revoked.

F. Collusion Resistant

Users cannot combine their attributes to decipher the encrypted data. Since each attribute is related to the polynomial or the random number, different users cannot collide each other.

II. Related Works

In cloud environments, if a data owner wants to share data with users, he will encrypt data and then upload to cloud storage service. Through the encryption step, the cloud cannot know the information of the encrypted data. Besides, to avoid the unauthorized user accessing the encrypted data in the cloud, a data owner uses the encryption scheme for access control of encrypted data. In existing schemes, many encryption schemes can achieve and provide security, assure data confidential, and prevent collusion attack scheme. One of the encryption schemes is attribute-based encryption scheme.

III. Proposed System

A. Cipher Text-Policy Attribute-Based Encryption Scheme

In 2007, Bettencourt et al. proposed a cipher text policy attribute-based scheme, and the access policy in the encrypted data (cipher text). The access control method of this scheme is similar to the key policy attribute-based encryption. In key policy attribute-based encryption, the access policy is in user's private key, but the

access policy is switched to the encrypted data in cipher text policy attribute-based encryption. And a set of descriptive attributes are associated with the user's private key, and the access policy is built in the encrypted data. The access structure of the encrypted data is corresponding to the user's private key with a set of descriptive attributes. If a set of attributes in user's private key satisfies the access structure of the encrypted data, the data user can decrypt the encrypted data; if it cannot, the data user cannot obtain the message. For example, the access structure in the encrypted data is {MISV(TeacherV Student)g}. If a set of attributes in user's private key is {MIS V Teacher} the user can recover the data.

In the access structure of this scheme, it adopts the same method which was depicted in KP-ABE to build. And the access structure built in the encrypted data can let the encrypted data choose which key can recover the data; it means the user's key with attributes just satisfies the access structure of the encrypted data. And the concept of this scheme is very close to the traditional access control scheme. There are five algorithms in this scheme, Setup (), KeyGen (), Encrypt (), Delegate (), Decrypt (). The Delegate algorithm is in addition more than above schemes, and it can input user's private key and regenerate the new one with another attributes which are in a set of attributes of the original user's private key. And this key is equal to the key generated from the authority.

Notation Signification

Gx $\rightarrow$ The bilinear group of prime order p, x = 1, 2

g $\rightarrow$ A generator of G1

AU $\rightarrow$ Attributes of data user U in private key

ACT $\rightarrow$ Attributes with the encrypted data CT

AU-KP $\rightarrow$ The access structure in user's private key

ACT $\rightarrow$ CP The access structure in the encrypted data

ACT $\rightarrow$ HA The DNF access control policy in the encrypted data

AU $\rightarrow$ The non-monotonic access structure in user's private key

D $\rightarrow$ User's private key

M $\rightarrow$ The message

The CP-ABE builds the access structure in the encrypted data to choose the corresponding user's private key to decipher data. It improves the disadvantage of KP-ABE that the encrypted data cannot choose who can decrypt. It can support the access control in the real environment. In addition, the user's private key is in this scheme, a combination of a set of attributes, so an user only use this set of attributes to satisfy the access structure in the encrypted data. Moreover, the CP-ABE scheme is applied in the proxy re-encryption field to increase security of this field. The CP-ABE scheme can be applied in the scheme which can achieves proxy reencryption in cloud environments.

Algorithm:

- 1) Setup: The authority chooses two random numbers α, β from Z_q as exponents, and generates the public key, $PK = (G_0, g, h = g^\beta, f = g^{\frac{1}{\beta}}, e(g, g)^\alpha)$. The master key is $MK = (\beta, g^\alpha)$.
- 2) KeyGen(MK, A_U): The authority chooses a random number s from Z_q , and random s_j for each attribute

j in a set of attributes in user's private key. The user's private key, $D = (DK = g^{\frac{(\alpha+s)}{\beta}}, \forall j \in A_U : D_j = g^s \cdot H(j)^{s_j}, D_j^* = g^{s_j})$ is output.

- 3) Encrypt(PK, M, A_{CT-CP}): Data owner executes this algorithm to encrypt the message M with the access structure A_{CT-CP} . Choose a random number $y \in Z_q$, set $q_r(0) = y$, where r is the root node, and let I be the set of leaf nodes in A_{CT-CP} . The message is encrypted with access structure A_{CT-CP} , and then outputs the encrypted data, $CT = (A_{CT-CP}, \tilde{C} = Me(g, g)^{\alpha y}, C = h^y, \forall i : C_i = g^{q_i(0)}, C_i^* = H(att(i))^{q_i(0)})$.
- 4) Delegate(D, $\tilde{A}_U$): This algorithm takes the user's private key D and a set of attributes whose each attribute is in A_U to create a new user's private key $\tilde{D}$.
- 5) Decrypt(CT, D): When data user receives the encrypted data, he can execute this algorithm. The user's private key D and the encrypted data are input in this algorithm and the recursive function, and decryptnode is called. If the node x is a leaf node and let $k = att(x)$, where $k \in A_U$, the decryptnode can be called, then it computes $decryptnode(CT, D, x) = \frac{e(D_k, C_x)}{e(D_k^*, C_x^*)} = e(g, g)^{sq_x(0)}$. If k is not in A_U , decryptnode will output invalid. If x is not the leaf node, the decryptnode function can be called and all children nodes of node x , z can be input to execute. It use Lagrange coefficient to compute and obtain $e(g, g)^{sq_x(0)}$. Hence, if the access structure A_{CT-CP} satisfies A_U , the CT, D, s are input to compute $decryptnode(CT, D, s) = e(g, g)^{sy}$. The algorithm can decrypt by computing $\frac{\tilde{C}}{e(C, DK)/e(g, g)^{ys}} = M$ to recover the message M.

IV. Conclusion

We propose an access control scheme which is based on the Cipher text Policy Attributed-Based Encryption (CP-ABE) approach. Our scheme provides a flexible fine-grained access control such that the encrypted contents can only be accessed by authorized users. Two unique features our scheme provides are: (i) the incorporation of dynamic attributes whose value may change over time, and (ii) the revocation feature.

References

- [1] M. Armbrust, A. Fox, R. Grieth, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, M. Zaharia, "A view of cloud computing", Communications of the ACM, Vol. 53, pp. 50-58, 2010.
- [2] J. Bethencourt, A. Sahai, B. Waters, "Ciphertext-policy attribute-based encryption", In Proceedings of IEEE Symposium on Security and Privacy, pp. 321-334, 2007.
- [3] V. Bozovic, D. Socek, R. Steinwandt, V. I. Vil-lanyi, "Multi-authority attribute-based encryption with honest-but-curious central authority", International Journal of Computer Mathematics, Vol. 89, pp. 3, 2012.

- [4] M. Chase, "Multi-authority attribute based encryption", In Proceedings of the Theory of Cryptography Conference, pp. 515-534, 2007.
- [5] M. Chase, S. S. M. Chow, "Improving privacy and security in multi-authority attribute-based encryption", In Proceedings of the 16th ACM conference on Computer and communications security, pp. 121-130, 2009.
- [6] C. C. Chang, I. C. Lin, C. T. Liao, "An access control system with time-constraint using support vector machines", International Journal of Network Security, Vol. 2, No. 2, pp. 150-159, 2006.
- [7] L. Cheung, C. Newport, "Provably secure cipher-text policy ABE", In Proceedings of the ACM conference on Computer and communications security, pp. 456-465, 2007.
- [8] M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis, Athena Vakali, "Cloud computing: Distributed internet computing for it and scienti^c research", IEEE Internet Computing, Vol. 13, pp. 10 -13, 2009.
- [9] K. Emura, A. Miyaji, A. Nomura, K. Omote, M. Soshi, "A ciphertext-policy attribute-based encryption scheme with constant ciphertext length", In Proceedings of the Information Security Practice and Experience, pp. 13-23, 2009.
- [10] V. Goyal, A. Jain, O. Pandey, A. Sahai, "Bounded ciphertext policy attribute based encryption", In Proceedings of the ICALP, pp. 579-591, 2008.



S. Sailaja was born in ponnur Guntur District, Andhra Pradesh, India. She received MCA from Nagarjuna University, Guntur, Andhra Pradesh, India. Presently, she is pursuing MTech in C.S.E from St. Mary's Group of Institutions, Chebroluvillage, Chebrolu Mandal, Guntur District, Andhra Pradesh, India. Her Research interest includes Cloud Computing, Data security and Network Security.



Sayyed Nagul Meera, Assistant Professor, Computer Science Engineering Department, St. Mary's Group of Institutions, Guntur, AP, India.