International Journal Of Advancement In Engineering Technology, Management and Applied Science (IJAETMAS)
UGC APPROVED-63082

ISSN: 2349-3224 || www.ijaetmas.com || Volume 04 - Issue 08 || August-2017 || PP. 144-149

A Survey on Security Control in Cloud Computing with Attribute based Encryption Schemes

[1]THANDU NAGARAJU , [2]BETHALA SHIRISHA

[1]*Assistant Professor, MTech, Department of CSE, CMRIT, India*
[2]*Assistant Professor, MTech, Department of CSE, CMRIT, India*

Abstract

In Attribute based Encryption (ABE) scheme, attributes play a vital 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 ABE or ciphertext policy ABE. The key policy is the access structure on the user's private key, and the ciphertext policy is the access structure on the ciphertext. And the access structure can also be categorized as either monotonic or non monotonic one. The advantages of ABE schemes (1) to reduce the communication overhead of the Internet, and (2) to provide a fine grained access control. In this paper, we survey a basic attribute based encryption scheme, two various access policy attribute based encryption schemes, and two various access structures, which are analyzed for cloud environments. Finally, we list the comparisons of these schemes by some criteria for cloud environments.

1 Introduction

Web innovation is developing increasingly rapidly, and individuals can process, store, or offer with their information by utilizing its capacity. As of late, the cloud has developed to give different application administrations to fulfill clients' prerequisite [1]. In the capacity benefit application, the cloud can let the client, information proprietor, store his information, and offer this information with different clients by means of the cloud, in light of the fact that the cloud can give the compensation as you go environment [8] where individuals simply need to pay the cash for the storage room they utilize. It can cut down the cost proficiently for individuals. In any case, there is an issue that the information proprietor needs to comprehend it. The information proprietor needs to influence a palatable and adaptable access to control approach to charge clients' entrance right, with the goal that lone the approved clients can get to [6].

Additionally, to protect the privacy of the put away information, the information must be scrambled before transferring to the cloud [10]. Customary open key framework can be embraced in the information encryption process, and the information proprietor utilizes information clients' open key to encode this information before transferring to the cloud; if the information client sends through an entrance demand to the cloud, at that point the cloud would restore the relating ciphertext to the information client. A client would utilize his private key to decode this information. Be that as it may, this way would prompt a few issues: (1) to have the capacity to scramble information, the information proprietor needs to get the information client's open key to finish this; (2) a considerable measure of capacity overhead would spend in light of the same plaintext with critical lease open keys.

For enhancing these detriments, Sahai and Waters proposed a trait based encryption (ABE) plot [2] in 2005, and this paper proposed the principal idea of the quality based encryption conspire. The ABE plot utilized a client's way of life as traits, and an arrangement of ascribes were utilized to encode and unscramble information. The ABE plan can come about the issue that information proprietor needs to utilize each approved client's open key to scramble information. What's more, around the same time, Nail et al. proposed a limit property based encryption which can keep the intrigue assaults [5].

In 2006, Goyal et al. proposed a key policy characteristic based encryption (KP ABE) conspire [10] that incorporated the entrance approach with the client's private key and portrayed the encoded information with client's properties. The KP ABE plan can accomplish fine grained get to control and more adaptability to control clients than ABE conspire. Be that as it may, the burden of KP ABE is that the entrance approach is incorporated with a client's private key, so information proprietor can't pick who can decode the information aside from picking an arrangement of properties which can depict this information. What's more,

ISSN: 2349-3224 || www.ijaetmas.com || Volume 04 - Issue 08 || August-2017 || PP. 144-149

it is unacceptable in certain application in light of the fact that an information proprietor needs to put stock in the key backer. Additionally, the entrance structure in KP ABE is a monotonic access structure; it can't express the negative credit to prohibit the gatherings with whom information proprietor would not like to share information from participations.

So Ostrovsky et al. proposed a non monotonic access structure [2] in 2007, and this plan can give each ascribe a chance to append prepared word before them. What's more, Bethen court et al. additionally proposed a ciphertext approach attribute based (CP ABE) conspire [2] around the same time, and the CP ABE plot incorporated the entrance strategy with the encrypted information; an arrangement of qualities is in a client's critical. The CP ABE plot tends to the issue of KP ABE that information proprietor just trusts the key backer. From that point forward, a few plans were proposed in light of the CP ABE plot [7, 9].

Also, Muller et al. proposed a dispersed characteristic based encryption plot [3] in 2008; Yu et al. proposed a fine grained information get to control encryption plot [3], Tang et al. proposed a Verifiable property based encryption conspire [30], and Wang et al. professional represented a various leveled quality based encryption plot (HABE) [3] of every 2010 and 2011. This plan utilizes the disjunctive typical frame arrangement and produces the keys progressively. Also, this plan expected that all properties in a single conjunctive provision are directed by a similar area expert. Moreover, there are multi experts ABE plans that utilization numerous gatherings to circulate properties for clients.

In light of the sort of access structure, property based encryption plans can be generally ordered as either monotonic or non monotonic. What's more, in light of the entrance arrangement, these plans likewise can be generally ordered as either key strategy or ciphertext approach. In this paper, the review began from essential property based encryption plot, trailed by monotonic access structure which could be separated into key arrangement quality based encryption conspire, ciphertext strategy characteristic based encryption conspire. Characteristic based encryption plot with non monotonic structure is presented. From there on, and various leveled quality based encryption conspire as the end.

2 Related Works

In cloud situations, if an information proprietor needs to impart information to clients, he will encode information and after that transfer to distributed storage benefit. Through the encryption step, the cloud can't know the data of the encoded information. In addition, to maintain a strategic distance from the unapproved client will get the encoded information in the cloud, an information proprietor utilizes the encryption conspire for get to control of scrambled information. In existing plans, numerous encryption plans can accomplish and give security, guarantee information classified, and avoid conspiracy assault plot. One of the encryption plans is quality based encryption plot. The main idea of property based encryption was expert postured in 2005. And afterward numerous trait based encryption plans were proposed. As indicated by the entrance approach, two sorts of these plans can be ordered, the key strategy and ciphertext arrangement property based encryption plans. The key approach trait based plan is that the entrance arrangement is appended to the client's private key, and an arrangement of graphic characteristics is in the encoded information. In the event that an arrangement of characteristics fulfills the entrance strategy, the client will recuperate the message. If not, he can't acquire it. Furthermore, the ciphertext strategy property based plan is that the entrance approach is related to the encoded information, and an arrangement of enlightening properties is in the client's private key. On the off chance that a set trait fulfills the entrance approach, the client can interpret the encoded information. In this area, we will present five quality based encryption plans. Furthermore, as per the sort of access arrangement, there are monotonic access structure and non monotonic access structure.

2.1 Attribute based Encryption Scheme

Sahai and Waters proposed a characteristic based encryption conspire in 2005. There are expert, information proprietor (likewise be called sender) and information client (additionally be called recipient) in this plan, and specialist's part is to produce keys for information proprietors and clients to encode or unscramble information. In this plan, the specialist creates keys as per properties; and these traits of open key and ace key, which are produced by the expert, ought to pre characterize (implies that it will list characteristics which will be utilized as a part without bounds). On the off chance that any information client who needs to add to this framework, and he claims to characteristics do exclude pre characterized qualities. The expert will reclassify characteristics and create an open key and ace key once more. Furthermore, information proprietor's part in this plan is to scramble information with an open key and an arrangement of graphic qualities. An information client's part is to decode encoded information with his

ISSN: 2349-3224 || www.ijaetmas.com || Volume 04 - Issue 08 || August-2017 || PP. 144-149

private key sent from the specialist, and after that he can acquire the required information.

For decrypting data, attributes in data user's private key will check by matching with the attributes in encrypted data. If the number of "matching" is at least a threshold value d, the data user's private key will be permitted to decrypt the encrypted data. For example, for a set of descriptive attributes in the encrypted data, fMIS; Teacher; Student g, the threshold value is 2. If a data user wants to decrypt the encrypted data, his number of attributes in private key will need two or the more than two of attributes in the encrypted data, so that a data user has a private key with attributes, fMIS; Student g to decrypt and obtain the data.

In this scheme, there are four algorithms to be executed: Setup, KeyGen, Encrypt, and Decrypt. Let G1 and G2 be two bilinear groups of prime order p, and let g be a generator of G1. In addition , let e : G1 £G1 ¡! G2 denote the bilinear map, and let d be a threshold value.

2.2 Key Policy Attribute based Encryption Scheme

In 2006, Goyal proposed an key policy attribute based (KP ABE) scheme. This scheme uses a set of attributes to describe the encrypted data and builds a access policy in user's private key. If attributes of the encrypted data can satisfy the access structure in user's private key D, an user can obtain the message through decrypt algorithm. In addition, the KeyGen() algorithm is different from the attribute based encryption which is introduced at subsection one in this section. The user's private key is according to the access structure to generate. In this algorithm, it adopts secret sharing and chooses a polynomial qx such that qx(0) = q parent (x)(index(x)), (Note that parent(x) is x's parent node, and index(x) is the number associated with node x that is given by x's parent node.) in a top down manner which is to start from the root node r for each node x in the access structure. So qr(0) is equal to the master key y, and the master key y is distributed among the user's private key component Di which is corresponding to the leaf node (Note that the leaf node represents attribute).

Since the KeyGen() algorithm is different, the De crypt() algorithm also be different. It use attributes of encrypted data to run decrypt node function in the decryption algorithm. And it can input encrypted data, user's private key, and nodes of the access structure in user's private key; it adopts bottom up manner in the access structure and recursive manner to decrypt the encrypted data. Beside, this scheme divides nodes of the access structure into the equal the leaf nodes. Finally, it will get a bilinear formula and use polynomial interpolation to get the message. For example, the encrypted data with attributes are fMIS Studentg, and user's private key with access structure is fMIS V(Teacher W Student)g. The encrypted data with attributes satisfies the access structure of an user's private key, and then user can get the message.

In this scheme, there are four algorithms to be executed: Setup, KeyGen, Encrypt, and Decrypt. And the parameters described in this scheme and parameters of the ABE scheme are the same. It will be depicted as follows.

2.3 Ciphertext Policy Attribute based Encryption Scheme

In 2007, Bethencourt et al. proposed a ciphertext policy attribute based scheme, and the access policy in the encrypted data (ciphertext). 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 ciphertext 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 fMIS V(Teacher W Student)g. If a set of attributes in user's private key is fMIS V Teacher g, the user can recover the data.

In the access structure of this scheme, it adopts the same method which was depicted in KPABE 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(), De crypt(). The Delegate algorithm is in addition more than above schemes, and it can input user's private key and re generate 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.

ISSN: 2349-3224 || www.ijaetmas.com || Volume 04 - Issue 08 || August-2017 || PP. 144-149

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 in crease security of this field. The CP ABE scheme can be applied in the scheme which can achieves proxy re encryption in cloud environments [6].

2.4 Attribute based Encryption Scheme with Non Monotonic Access Structures

In 2007, Ostrovsky et al. proposed an attribute based encryption with non monotonic access structure. The access formula of access structure in user's private key can represent any type through attributes such as negative ones. It is different from the previous attribute based encryption scheme. The previous schemes are like KP ABE scheme, and the access structure in user's private key has monotonic access formula. No negative at tributes exist in it. Apart from this, the access structure of this scheme is the same as the access structure of KP ABE scheme. There is a Boolean formula such as And, OR, and threshold gates in these access structures, but there is a Boolean formula, NOT in access structure of this scheme. However, other schemes do not include it. There is an example for this scheme. If a teacher in department of information management wants to share the data with students, he will set a set of attributes in the encrypted data. And there is an access structure, fMIS V Student g in students' private key. But the teacher doesn't want graduates to access this data, he adds NOT graduate to the access structure. So the access structure is fMIS V Student V NOT graduate g. It can let data not be accessed by graduates.

3. Comparisons

In this section, we compare these schemes which we survey. First, we compare these schemes by the criteria and the second, we compare these schemes by the length of their user's private key and ciphertext, and by the operation of the encrypt and decrypt algorithm.

3.1 Security Analysis

These schemes which we survey were compared by the criteria listed in Section 1. The criteria contain C1 fine grained access control, C2 data confidentiality, C3 scalability, C4 user accountability, C5 user revocation, and C6 collusion resistant. This comparison table is listed. We can know that these schemes almost cannot satisfy the criteria of scalability and user accountability, and they all can achieve the data confidentiality. The ABE scheme only satisfies one criteria. Because it uses the attributes in the user's private key to match the attributes in the encrypted data, it only achieves the basic security requirement. But it provides the first concept to develop the attribute based encryption scheme. After that, these schemes cannot satisfy all the criteria except HABE. Besides, the criteria of user accountability are hard to achieve.

Preventing the problem of illegal key sharing among users is difficult to solve, because it is hard to trace who shares the key. So almost all ABE schemes that we introduce cannot achieve two criteria.

3.2 Performance Analysis

LG1 denotes the bit length of element in G1, LG2 denotes the bit length of element in G2, Ce denotes a pairing op eration, G1; G 2 denotes two bilinear group operation, m denotes least node of the tree which can satisfy the access structure, and j ¤ j denotes the number of the element. Table list the comparison result [9]. We can found out, the length of user's private key and the ciphertext are corresponding to the number of attributes; if the number of attributes is too many, the length would increase. Moreover, the length of user's private key in ABE with a non monotonic access structure scheme is more than other schemes, because the component of the user's private key in this scheme is including non negated and negated attributes. If the scheme is based on the CP ABE scheme, the decryption computation time is more than basic ABE scheme and KP ABE scheme. In addition, the policy in ABE with a non monotonic access structure is different, because it can use the negated word to describe attributes. But it causes a problem that the length of user's private key is longer than other schemes.

International Journal Of Advancement In Engineering Technology, Management and Applied Science (IJAETMAS)
UGC APPROVED-63082
ISSN: 2349-3224 || www.ijaetmas.com || Volume 04 - Issue 08 || August-2017 || PP. 144-149

S.NO	ALGORITHM	KP-ABE	CPABE	NON-MONOTONIC	HABE	MABE
1	setup	(K) (PK ,MK)	(K) (PK ,MK)	D	RM(K) (Params,MK)	(K) (PKa,SKa,SPKca MSKca)
2	encryption	(M,PK,A) (CT)	(M,PK,AS) (CT)	(M,A,PK) (CT)	(f,DNF,AS,PK) (CT)	(A ,M,SPK) (CT)
3	key generation	(MK,AS,PK) (SK)	(A, MK) (SK)	(~A,PK,MK) (SK)	DM(PK,MKi,PKi+1) (MKi+1). USER(P K; MKi; P Ku; PKa) SKu	AKG(SKa,dk,GID,AKC) (SKu) CKG(MSKca,GID) (SKu)
4	decryption	(SK,CT,PK) (M)	(CT,SK) (M)	(CT,SK) (M)	(Params,CT,SK,A) (M)	(CT,DK) (M)
5	limitation	It cannot decide who can encrypt data.	Decrypt key only support user attribute that are organized logically.	In sufficient and complex	Unsuitable to implement	Each authority attribute set should be disjoint
6	component	Data is associated with an access policy.	CT is associated with an access policy .	Represent negative constraints.	Hierarchical generation of key.	Multiple authorities
10	efficiency	Average	Average	High	Better	Scalable
11	secured access control	Low	Average	Average	High	Average
12	computational overhead	High	Average	More	More	More
13	data confidentiality	no	yes	yes	yes	yes
14	user accountability	no	no	yes	no	yes
15	scalability	no	yes	no	no	yes
16	user revocation	no	no	yes	yes	yes
17	collusion resistent	yes	yes	yes	yes	yes

Fig : COMPARISON TABLE OF ABE SCHEMES

4.Conclusions

In this paper, we survey five different attribute based encryption schemes: ABE, KP ABE, CP ABE, ABE with non monotonic access structure, and HABE, and illustrate their schemes and compare them. These schemes can be classified according to their access policy. The access policy in the user's private key is KP ABE, and the access policy in the encrypted data is CP ABE. Besides, we can find these schemes that are hard to satisfy user ac countability. Moreover, the access structure is pre defined in these schemes; if a new user wants to access data and his attributes are not in the access structure, these encrypted data will be re generated.

Thus, based on the discussion above, these existing attribute based encryption schemes have properties: (1) These schemes

ISSN: 2349-3224 || www.ijaetmas.com || Volume 04 - Issue 08 || August-2017 || PP. 144-149

are encrypted with attributes, so a data owner just needs to predefine these attributes that he would use, he doesn't need to care about the number of users in the system; (2) Each attribute has public key, secret key, and a random polynomial, so different users cannot combine their attributes to recover the data, and different users cannot carry out collusion attacks; (3) Only the user who possesses the authorized attributes can sat isfy the access policy to decrypt data; (4) The access policy contains a boolean formula such as AND, OR et al. which can let the access structure be flexible to control users' access. However, almost all schemes exist that the authority is used to generate keys. Since these schemes contain the authority that just suits the private cloud environments, the authority should be removed in the future. Furthermore, ABE schemes (like KP ABE or CP ABE scheme) are generally applied in the field of proxy re encryption.

References

[1] M. Armbrust, A. Fox, R. Gri±th, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, A view of cloud computing," *Communications of the ACM*, vol. 53, pp. 50{58, 2010.

[2] J. Bethencourt, A. Sahai, and B. Waters, Ciphertext policy attribute based encryption," in *Proceedings of IEEE Symposium on Security and Privacy*, pp. 321V334, 2007.

[3] V Bozovic, D Socek, R Steinwandt, and V. I. Vil lanyi, Multi authority attribute based encryption with honest but curious central authority," *Interna tional Journal of Computer Mathematics*, vol. 89, 3, 2012.

[4] M. Chase, Multi authority attribute based encryp tion," in Proceedings of the Theory of Cryptography Conference, pp. 515{534, 2007.

[5] M. Chase and 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, and 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 and C. Newport, \Provably secure cipher text policy ABE," in Proceedings of the ACM con ference on Computer and communications security, 456{465, 2007.

[8] M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis, and Athena Vakali, Cloud computing: Distributed internet computing for it and scientific research," IEEE Internet Computing, vol. 13, pp. 10 {13, 2009.

[9] K. Emura, A. Miyaji, A. Nomura, K. Omote, and 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, and A. Sahai, \Bounded ciphertext policy attribute based encryption," in Proceedings of the ICALP, pp. 579{591, 2008.