International Journal of Computer Science and Engineering Communications
Vol.3, Issue 3, 2015, Page.1076-1081
ISSN: 2347–8586
www.scientistlink.org

Analysis of Attribute Based Encryption Schemes

[1] R.Nitya Lakshmi, [2] R.Laavanya, [3] M.Meenakshi, [4]Dr.C.Suresh Gana Dhas
[1,2,3]UG Students, [4]HOD
Department of Computer Science and Engineering,
Vivekanandha College of Engineering for Women, Namakkal, India.
[1]nitilakshmi@gmail.com,[2]laavanyarajasekar@gmail.com,,[4]suresh.me@gmail.com

Abstract: Cloud computing is an emerging computing paradigm enabling users to remotely store their data in a server and provide on-demand services . With the emergence of sharing confidential corporate data on cloud server, data security and privacy became the critical issues for remote data storage. Secure user enforced data access control mechanism must be provided before cloud user has the liberty to outsource sensitive data to the cloud for storage. In present many cryptographic algorithms are used for encryption of the data. In this paper, we are going to analyze various schemes for encryption and possible solutions for their limitations that consist of Attribute based encryption(ABE), Key policy Attribute based encryption(KP-ABE), Cipher text Attribute based encryption(CP-ABE), non-monotonic access structure, Hierarchical Attribute based encryption(HABE), Multiple authority Attribute based encryption(MA-ABE).

Keywords
Attribute based encryption, user accountability, user revocation, collision resistance, Scalability, KP-ABE, CP-ABE, HABE, MABE.

1. INTRODUCTION

Cloud computing has rapidly becomes a widely adopted paradigm for delivering services over the internet. Cloud service provider must provide the trust and security, as there is valuable and sensitive data in large amount stored on the clouds. For protecting the confidentiality of the stored data, the data must be encrypted by using some cryptographic algorithms. In this paper we are going to discuss about attribute based encryption and its categories.

An attribute based encryption scheme (ABE) was introduced by Sahai and Waters in 2005. The goal of this scheme is to provide security and access control. Attribute-based encryption (ABE) is a public-key based one to many encryption that allows users to encrypt and decrypt data based on user attributes. Attribute based encryption scheme has various categories which are to be discussed in detail further. It includes Key policy attribute based encryption (KP-ABE), Cipher text policy attribute based encryption (CP-ABE),Attribute-based Encryption scheme with Non-Monotonic Access Structures, Hierarchical attribute-based encryption(HABE), Multi-level attribute based encryption(MABE).

2. THE CRITERIA OF AN IDEAL ATTRIBUTE-BASED ENCRYPTION SCHEMES

According to the above mentioned schemes in section I, a summary of the criteria or constraints of an ideal attribute-based encryption schemes are listed as follows:

2.1 Data confidentiality

Data Confidentiality is a set of rules or a promise that limits access or places restrictions on certain types of information. In cloud, the data was encrypted by the data owner and unauthorized parties including the cloud cannot know the information about the encrypted data hence data confidentiality is maintained.

2.2. Secured access control: Secured Access Control is any mechanism by which a cloud system grants or revokes the right to access some data, or perform some action. In cloud users are granted with different access right to access data to provide security.

2.3. Scalability

Scalability is defined as the capability to handle the user load supported, the number of transactions, the data volume etc. When the authorized users increase, the system can work efficiently. So the number of authorized users cannot affect the performance of the system.

2.4. 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.

2.5. 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.

2.6. Collision 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 conclude each other.

3. LITERATURE SURVEY

The literature survey that containing study of different scheme available on Attribute Based encryption(ABE).That are KP-ABE,CP-ABE, Attribute-based Encryption Scheme with Non-Monotonic Access Structures, ABE and MABE. Also include advantage, disadvantage and a comparison table of each of scheme based on setup, encryption, decryption, drawbacks, secured access control, efficiency, and computational overhead and collusion resistant.

3.1. Attributes Based Encryption (ABE)

Security and access control is the main goal of the Attribute Based Encryption. It is a public-key (PK)based one to many encryption that allows users to encrypt and decrypt data based on user attributes. In which the secret key (SK) of a user and the cipher text(CT) are dependent upon attributes (e.g. the country she lives, or the kind of subscription she has).In such a system, the decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text. Decryption is only possible when the number of matching is at least a threshold value. Collision-resistance (An adversary that holds multiple keys should only be access data if at least one individual key grants access.) is crucial security features of Attribute-Based Encryption.

Drawbacks

The problem with attribute based encryption (ABE) scheme is that data owner needs to use every authorized user's public key to encrypt data. The application of this scheme is restricted in the real environment because it uses the access of monotonic attributes to control user's access in the system.

3.2. Key policy Attribute Based Encryption (KP-ABE)

It is the modified form of classical model of ABE. Users are assigned with an access structure (AS) over the data attributes.. To reflect the access structure the secret key of the user is defined. Cipher texts are labeled with sets of attribute and private keys are associated with monotonic access structure that control which cipher texts a user is able to decrypt. Key policy Attribute Based Encryption (KP-ABE) scheme is designed for one-to-many communications.

Algorithm takes input K as a security parameter and returns PK as public key and the system master secret key MK. PK is used by message senders for encryption.MK is used to generate user secret keys and is known only to the authority. For encryption algorithm takes a message M, the public key (PK), and a set of attribute as input. It outputs the cipher text (CT). Key generation algorithm takes as input an access structure (AS) and the master secret key MK. It outputs as a secret key SK that enables the user to decrypt the message encrypted under a set of attributes if and only if matches T[1]. Decryption is possible only if the attribute set satisfies the user's access structure. The KP-ABE scheme can achieve secured access control and more flexibility to control users than ABE scheme.

Drawbacks

The problem with KP-ABE scheme is encryptor cannot decide who can decrypt the encrypted data. It can only choose descriptive attributes for the data, it is unsuitable in some application because a data owner has to trust the key issuer.

3.3. Cipher text Policy Attribute Based Encryption

CP-ABE is the modified form of KP-ABE introduced by Sahai. In a CP-ABE scheme, every cipher text is associated with an access policy on attributes, and every user's private key is associated with a set of attributes[3]. A user is able to decrypt a cipher text only if the set of attributes associated with the user's private key satisfies the access policy associated with the cipher text. CP-ABE works in the reverse way of KP-ABE.

The algorithm takes as input a security parameter K and returns the public key PK as well as a system master secret key MK. PK is used by message senders for encryption.MK is used to generate user secret keys and is known only to the authority. For encryption of data algorithm takes as input the public parameter PK, a message M, and an access structure AS. it outputs the cipher text CT[4]. Key-Generation this algorithm takes as input a set of attribute associated with the user and the master key MK. It outputs a secret key SK that enables the user to decrypt a message encrypted under an access tree structure T if and only if matches T. Decryption of the data only if satisfies the access structure associated with the cipher text CT. 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 attribute to satisfy in the encrypted data

Drawbacks:

Drawbacks of the most existing CP-ABE schemes are still not fulfilling the enterprise requirements of access control which require considerable flexibility and efficiency. CP-ABE has limitation in terms of specifying policies and managing user attributes. In a CP-ABE scheme, decryption keys only support user attributes that are organized logically as a single set, so the user can only use all possible combinations of attributes in a single set issued in their keys to satisfy policies.

3.4. Attribute-based Encryption scheme with Non-Monotonic Access Structures:

Previous ABE schemes were limited to expressing only monotonic access structures and there is no satisfactory method to represent negative constraints in a key's access formula. Ostrovskyetal. Proposed an attribute-based encryption with non-monotonic access structure in 2007.Non-monotonic access structure can use the negative word to describe every attributes in the message, but the monotonic access structure cannot.

In the basic construction, a parameter d specifies how many attributes every cipher text has. To encrypt a message M under a set of d attributes, choose a random value s and output the cipher text CT[6]. Key Generation algorithm outputs a key D that enables the user to decrypt an encrypted message only if the attributes of that cipher text satisfy the access structure ~A.

Drawbacks:

The Problem with Attribute-based Encryption Scheme with Non-monotonic Access Structure is that there are many negative attributes in the encrypted data, but they don't relate to the encrypted data. It means that each attribute adds a negative word to describe it, but these are useless for decrypting the encrypted data. It can cause the encrypted data overhead becoming huge. It is inefficient and complex as each cipher text needs to de encrypted with attributes.

3.5. Hierarchical attribute-based Encryption:

Hierarchal attribute-based encryption (HABE) is derived by Wang et al. The HABE model consists of a root master (RM) that corresponds to the third trusted party(TTP),multiple domain masters(DMs) in which the top-level DMs corresponds to multiple enterprise users, and numerous users that corresponds to all personnel in an enterprise as shown in Fig.3.5.1. This scheme used the property of hierarchal generation if keys in HIBE scheme to generate keys. Then HABE scheme is defined by presenting randomized polynomial time algorithm[10]. The Root Master(RM) takes a sufficiently large security parameter K as input, and output system parameters (params) and root master key MK0.DM algorithm checks whether the RM or the DM generates master keys for the DM's directly under params and its master key and also whether U is eligible for a, which is administered by itself. If so, it generates a user identity secret key and a user attribute secret key for U, using params and its master key. Otherwise it outputs "NULL". For encryption the algorithm takes a file f, a DNF access control policy A, and public keys o all attributes in A, as inputs, and outputs a cipher text CT[12]. Decryption is done if it satisfy the j-th conjucutive clause. This scheme can satisfy the property of secured access control, scalability and full delegation. It can share data for users in the cloud in an enterprise environment. Furthermore, it can apply to achieve proxy re-encryption.

Drawbacks:

In practice, it is unsuitable to implement. Since all attributes in one conjunctive clause in this scheme may be administered by the same domain authority, the same attribute may be administered by multiple domain authorities.

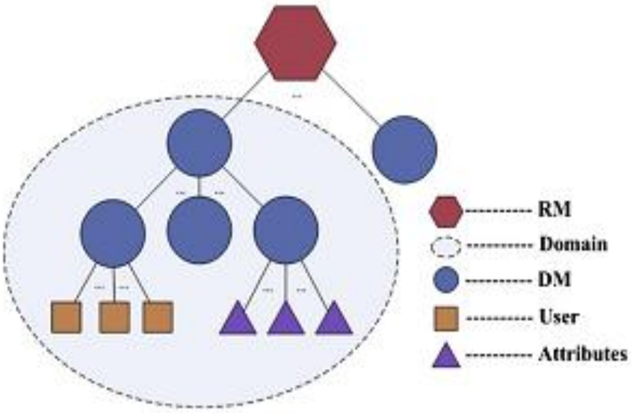

Figure 1. HABE Model

3.6. Multi-Authority Attribute Based Encryption:

Multi-authority attribute-based encryption scheme uses multiple parties to distribute attributes for users. A Multi Authority ABE system is composed of K attribute authorities and one central authority. Each attribute authority is also assigned a value dk.

A randomized algorithm which must be run by some trusted party (e.g. central authority).Takes as input the security parameter K. Outputs a public key, secret key pair for each of the attribute authorities(PKa , SKa), and also outputs a system public key and master secret key which will be used by the central authority(PKca , SKca). For Attribute Key Generation algorithm takes as input the authority's secret key, the authority's value dk, a user's GID , and a set of attributes in the authority's domain AkC and outputs secret key for the user. Encryption is done by randomized algorithm run by a sender it takes a set of attributes for each authority, a message, and the system public key as input and outputs the cipher text.

A decryption algorithm run by a user takes a cipher text as input, which was encrypted under attribute set A and decryption keys for an attribute set Au. Outputs a message M. It allows any polynomial number of independent authorities to monitor attributes and distribute private keys and tolerate any number of corrupted authorities. In this model, a recipient is defined not by a single string, but by a set of attributes.

Drawbacks:

Complication in multi-authority scheme required that each authority's attribute set be disjoint.

4. COMPARISION

The below table 4.1 gives the comparison of attribute based encryption schemes which include KP-ABE, CP-ABE, non-monotonic access structure, HABE,MABE based on algorithms such as setup, encryption, decryption and drawbacks, added technique and also parameters such as efficiency, computation overhead, user accountability, user revocation, scalability, collision resistant. Based on the compared data, we proposed applicable technique in next section.

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

Table 1. COMPARISON TABLE OF ABE SCHEMES

5. PROPOSED SOLUTION/FUTURE WORK

Issues such as scalability in key management, flexible access and efficient user revocation, has remained the most important challenges towards achieving secured cryptographically enforced data access control. For improving the limitation of the above discussed schemes we propose few techniques which we are going to use in developing new scheme, are as follows:

- **ABE without sourced decryption** largely eliminates the decryption overhead for users.
- **Priority can be given to the user based on security they want to their data**, instead of giving same security for all, and provide re-encryption technique for over sensitive data its reduces the overhead and increase efficiency. **Alert and notification system to give both providers and users ability to track their data.**
- **User can be categorized into domains (public ,private)which allows a user to choose set of attribute instead of a single string representing the user identity.**

CONCLUSION

In this paper, we have analyzed five different attribute-based encryption schemes: ABE, KP-ABE, CP-ABE, ABE with non-monotonic access structure, and HABE,MABE and compared their security ,schemes and efficiency. The main access policies are KP-ABE and CP-ABE, further schemes are obtained based on these policies .Based on the their type of access structure the schemes are categorized as either monotonic or no-monotonic. Computation overhead ,secured access control, security remained major challenges which can be eliminated by the techniques such as categorized domain, providing security priority to users, re-encryption and alert and notification system stated in above section.

REFERENCES

[1] M. Armbrust, A. Fox, R. Gri±th, A. D. Joseph,R. Katz, A. Konwinski, G. , 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 andPrivacy, 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,pp. 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 accesscontrol 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,pp. 456{465, 2007}.

[8] M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis,and Athena Vakali,Cloud computing: Distributedinternet 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, andM. 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}.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters,Attribute-based encryption for ¯ne-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security, pp. 89{98, 2006.

[12] M. S. Hwang and I. C Lin, \Introduction to Infor-mation and Network Security (4ed, in Chinese)," in Mc Graw Hill. In Taiwan, 2011.

[13] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, \Mediated ciphertext-policy attribute-based encryption and its application," Information Security Applications, vol. 5932 of LNCS, pp. 309{323, of LNCS, pp. 62{91, 2010}.