IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727
PP 19-23
www.iosrjournals.org

A Survey on Attribute Based Encryption Schemes for Data Sharing

Athira Rajeev, Tina Sara Kenu, Arun R , Dr. Suvanam Sasidhar Babu
Dept. of CSE (Cyber Security) Sree Narayana Gurukulam College of Engineering Kadayiruppu, Kerala, India
Dept. of CSE Sree Narayana Gurukulam College of Engineering Kadayiruppu, Kerala, India

Abstract: *As sensitive data is stored and shared by third party sites on the Internet, there will be a need to encrypt data stored at these sites. Attribute Based Encryption (ABE) schemes is a vision of public key encryption mechanism that allows users to encrypt and decrypt messages based on user attributes. ABE takes attributes as public key and associates them with the ciphertext and user's secret key. It is an efficient way to solve open problems in access control scenarios.*

In this paper, we survey the basic Attribute Based Encryption (ABE) scheme and its two varients: Key-policy ABE (KP-ABE) scheme and the Ciphertext-policy ABE (CP-ABE) scheme.
Keywords: *Attribute Based Encryption, Key-policy, Ciphertext-policy, data sharing, security.*

I. Introduction

With the development of the Internet and the distributed computing technology, demand for data sharing and processing in an open distributed computing environment is growing. Every piece of data may legally be accessed by several different users in many access control systems. Such systems will be implemented with trusted server which stores all the data in clear. A user would log into the server and the server decides what data the user is permitted to access. But the problem is when the server gets compromised. The attacker can see all the data in clear if he can successfully log into the server. The data provider needs to provide expressive access control and data confidentiality when communicating with customers. By encrypting the data on the server with the private keys of the users who are permitted to access it can solve this problem. However using traditional public key encryption systems in handling complex access control policy can be difficult, this is because the access policy might be described in terms of attributes(e.g.: place, profession) that a valid user should have rather than in terms of actual identities of user.

Sahai and Waters [1] introduced the concept of Attribute Based Encryption (ABE) as a step to develop encryption schemes with high expressiveness. In ABE scheme, attribute plays a very important role. Attribute have been used as an access policy to control users' access. It is intended for one-to-many encryption in which who are able to fulfill certain requirements specified.

Attribute based encryption is a type of public key encryption where the secret key of a user and the ciphertext are dependent on the attributes (e.g.: the profession he as, place he lives in etc.) that is allows user to encrypt and decrypt messages based on user attributes. We can decrypt the ciphertext only if the set of attributes of the user key matches the attributes of the ciphertext. Based on the access policy, researchers can be able to classify into either as key-policy or ciphertext policy. Goyal et al. [2] proposed the first KP-ABE scheme that allows any monotone access structures and Bethencourt et al [3] proposed the first CP-ABE systems. After that, several KP-ABE [4-5] and CP-ABE schemes were proposed [5].Bounded CP-ABE scheme in the standard model is proposed by Goyal et al[6], but fully expressive CP-ABE scheme in the standard model was proposed by Waters [13]. Recently, several researches have further proposed Attribute Based Encryption with multiple authorities who jointly generate user's private keys.

The security intention of Attribute Based Encryption is collusion resistance. An adversary that holds multiple keys should only be able to access data only if at least one individual key grants access.

II. LITERATURE REVIEW

The literature survey consists of the study of Attribute Based Encryption, KP-ABE, and CP-ABE.

1.Attribute Based Encryption (Abe)

Attribute Based Encryption scheme was first propose by Sahai and Waters. Attribute Based Encryption is a type of public key cryptosystem in which the secret key of a user and the ciphertext are associated with the attributes. The ciphertext is associated with some set of user attributes, such that the decryption of ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. The scheme can be

divided into two categories: Ciphertext-Policy ABE (CP-ABE) and Key-Policy ABE (KP-ABE) [8] depending on the access policy embedded into the ciphertext or user's secret key.

1.1 Data Sharing Architecture

Data sharing architecture has four main entities which are the following:

- User

User is one who wants to access the data. If a user possesses a set of attributes satisfying the access policy of the encrypted data, and is not revoked in any of the valid attribute groups, then he will be able to decrypt the ciphertext and obtain the data.

- Data owner

Data owner is the person who owns data and who wishes to upload data into the external data-storing center for sharing or cost saving. Data owner is responsible for defining the access policy and also the one who want to encrypt the data in order to ensure security.

- Key generation center

It is a key authority that generates public and secret parameters. It is in charge of issuing, revoking and updating attribute keys for users. It will honestly execute the assigned tasks in the system. Based on the attributes of individual users KGC grants differential access rights.

- Data-storing center

Data storing center stores data for the users. Data sharing service is provided by this entity. It is another authority that generates personalized user key with KGC, and issues and revokes attribute group keys to valid users per each attribute, which are used to enforce a fine-grained user access control like KGC it is also semi trusted.

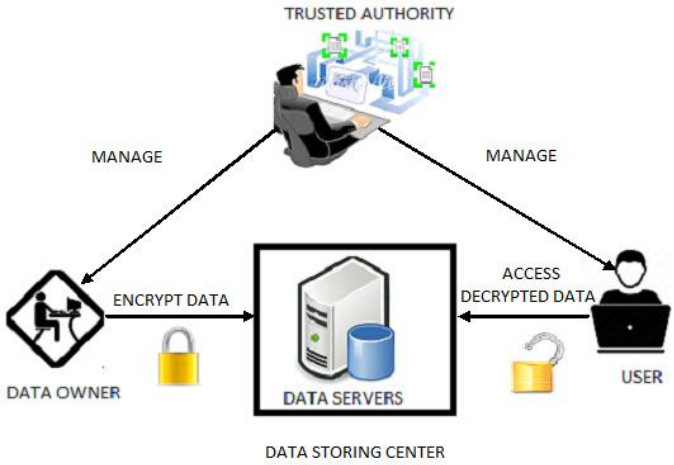

Fig 1. Architecture of Data Sharing

1.2 Abe Algorihtm Model

ABE schemes usually consist of four fundamental algorithms. In basic ABE schemes, the user's secret key and the cipher text are labeled with a set of descriptive attributes. A particular key can decrypt a particular ciphertext only if there are at least a specific number of attributes overlapped between the attributes of the ciphertext and the user's key. The decryption condition in a KP-ABE or CP-ABE schemes is that the attributes set satisfies the access structure specified in the secret key or ciphertext.

The four algorithms are Setup, Encryption, Decryption, Key generation and it has a sender, an authority and some receivers as participants.

Setup: (K, U)->(PP,MSK)

This algorithm takes as input a security parameter K and returns a public key PP and system master secret key MSK. PP is used by message senders for encryption. MSK is used to generate user secret key and is only known to the authority.

Key Generation: (K,PP,MSK,S)->SK

The authority executes this algorithm for the purpose of generating a secret key SK. The algorithm takes as inputs the public parameter PP, the master secret key MSK , set of attributes S and outputs a decryption key SK that enables the user to decrypt a message encrypted under an access tree structure T if and only if matches T.

Encryption: (K,PP,M,T)->CT

This algorithm is performed by a sender who wants to encrypt a message M, with the public parameter PP, a set of attributes S, an access structure T. This algorithm outputs the ciphertext CT.

Decryption: (K,PP,SK,CT)->M

This algorithm takes as the input the ciphertext CT and secret key SK for an attribute set. IT returns the message M if and only if satisfies the access structure associated with the ciphertext CT.

2. Key-Policy Attribute Based Encryption (Kp-Abe)

It is a modified encryption scheme of ABE scheme. First key-policy scheme is proposed by Goyal el al. in 2006 [2].KP-ABE helps in fine-grained sharing of encrypted data and is designed for one-to-many communications. In this scheme every ciphertext is associated with a set of descriptive attributes and the user's secret key is issued by trusted authority captures access structure is also called policy. This specifies which type of ciphertexts the key can decrypt, i.e. A user is able to decrypt a ciphertext only if the set of attributes associated with the ciphertext satisfies the access policy associated with the user's private key.

KP-ABE is suitable for structured organizations with rule about who may read particular documents.KP-ABE prevents any unauthorized users from accessing of data, even if the data were stores data in an untrusted server.

3. Ciphertext-Policy Attribute Based Encyption (Cp-Abe)

Another form of ABE scheme is the CP-ABE scheme. One thing we do all time is to store our files on remote servers. There are a number of reasons why we do so.

We may want to provide scalable access to our files to others using additional resources available elsewhere. We may want more reliability in case of failures. In this case we replicate our files in different data centers or with different organizations. But we want security. We may have requirements on who can access which files. The interesting thing is, there is a tension between security and the other properties. The more we replicate our files, the more we introduce potential points of compromise and the more trust we require. It's this tension which makes this sort of problem interesting, and provides a context in which CP-ABE can vary be useful.

CP-ABE can be viewed as a generalization of identity-based encryption. So as in identity-based encryption, there is a single public key, and there is a master private key that can be used to make more limited private keys. However, CP-ABE is much more flexible than plain identity-based encryption, in that it allows complex rules specifying which private keys can decrypt which ciphertexts. Specifically, the private keys are associated with sets of attributes or labels, and when we can decrypt, we encrypt to an access policy which specifies which keys will be able to decrypt.

In CP-ABE [2] each user is associated with a set of attribute and her private key is generated based on this attributes. When encrypting a message M, the encryptor specifies an access structure which is expressed in terms of set of selected attributes for M. The message is the encrypted based on the access structure such that only those whose attributes satisfy this access structure can decrypt the message. Unauthorized users are not able to decrypt this cipher text even if they collude. 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 similar to traditional access control schemes.

III. Abe Security Analysis

The functionalities in an ideal ABE scheme according to the existing schemes is listed as follows:

1. Data Confidentiality:

Unauthorized user is prevented from accessing the plaintext of the data ie. Unauthorized participants cannot know the information about the encrypted data. In this case the unauthorized users do not have enough attributes satisfying the access policy. Thus, unauthorized access from the KGC as well as the data-storing center to the plain text of the encrypted data should be prevented.

2. Collusion Resistance:

The dishonest users cannot combine their attributes to decrypt the encrypted data. Collusion resistance is one of the important security property required in the ABE systems. If multiple users collude, they may be able to decrypt a ciphertext by combing their attributes even if each of the user's cannot decrypt the ciphertext alone.

3. User/attribute revocation:

The schemes can revoke the access right of the person who quit the system.

4. Scalability:

The number of authorized user's cannot affect the performance of the scheme ie the scheme can deal with the case that the number of authorized user's increases dynamically.

IV. Comparison Between Key Policy And Ciphertext Policy

CP-ABE scheme is highly efficient when compared with the KP-ABE scheme. The CP-ABE is more appropriate for the data sharing system because it keeps the access policy decisions in the hand of the data owners. 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 use's private key is in the 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. But there are still some disadvantages for the CP-ABE scheme. 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 limitations 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 users can only use all possible combinations of attributes in a single set issued in their keys to satisfy policies.

SCHEMES:	PROPERTIES			
	FINE GRAINED ACCESS CONTOL	SECURITY	COLLUSION RESISTANT	EFFICENCY
ABE	LOW	AVERAGE	LOW	AVERAGE
KP-ABE	LOW	AVERAGE	HIGH	AVERAGE
CP-ABE	AVERAGE	HIGH	HIGH	HIGH

Fig 2. Comparison

V. Conclusion

In recent years, attribute based encryption is a relatively attractive research topic and has many attracting properties. It provides a fine-grained and non interactive access control mechanism of encrypted data and has great potential applications in many fields. In this paper, firstly we expound the emergence and development of ABE schemes and then the two of ABE schemes: KP-ABE and CP-ABE.

REFERENCES

[1]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," inProc.EUROCRYPT, 2005, pp. 457473.
[2]. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06), pp. 89–98, November 2006.
[3]. J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in Proceedings of the IEEE Symposium on Security and Privacy (SP '07), pp. 321–334,May 2007. 4) R. Ostrovsky, A. Sahai, and B.Waters, "Attribute-based encryption with non-monotonic access structures," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), pp. 195–203, November 2007.
[4]. N. Attrapadung, B. Libert, and E. de Panafieu, "Expressive keypolicy attribute-based encryption with constant-size ciphertexts," in Public Key Cryptography—PKC 2011, vol. 6571, pp. 90– 108, Springer, 2011.
[5]. V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute based encryption," in Automata, Languages and Programming: Part II, vol. 5126 of Lecture Notes in Computer Science, pp. 579–591, Springer, Berlin, Germany, 2008.
[6]. L. Cheung and C. Newport, "Provably secure ciphertext policy ABE," in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), pp. 456–465,November 2007.