Volume 5, Issue 3, March 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Survey of Various Attribute Based Encryption Schemes Used in Data Sharing System

Mangesh Gosavi[1], Tabassum Maktum[2]
[1] Student, [2] Assistant Professor
[1, 2] Department of Computer Engineering,
Terna Engineering College, Mumbai, India

Abstract*: Nowadays due to advancement in network and computing technology it is easily possible for people to share their data with others using online external servers. People can share their lives with friends by uploading their private photos or messages into the online social networks such as twitter, Facebook and MySpace etc.From recent study it was found that most of the internet user are having habit of uploading their highly sensitive personal health records (PHRs) into online data servers such as Microsoft Health Vault, Google Health for getting quick precautionary measurement from their primary doctors which is also cost saving. As people enjoy the advantages of these new technologies and services, their concerns about data security and access control also arise. Improper use of the data by the storage server or unauthorized access by outside users could be potential threats to their data. People would like to make their sensitive or private data only accessible to the authorized people with credentials they specified. Attribute-based encryption (ABE) is a promising cryptographic approach that achieves a fine-grained data access control. Attribute-based encryption is a public key based encryption that enables access control over encrypted data using access policies and ascribed attributes. In this paper, we are going to analyse various attribute based encryption schemes and their limitations like KP-ABE, CP-ABE, Attribute-based Encryption Scheme with Non-Monotonic Access Structures, HABE, MA-ABE.

Keywords-Attribute-based encryption, cipher text policy, fine-grained access control, re-encryption

I. INTRODUCTION

Nowadays there is a trend of storing sensitive data on third parties server using Internet. For example personal email, data, and personal preferences are generally stored on web portal sites such as Google and Yahoo. As peoples are enjoying benefits of these new technologies at the same time they are concern about their personal data security. Public-Key encryption is a powerful mechanism for protecting the confidentiality of stored and transmitted information. Traditionally, encryption is viewed as a method for a user to share data to a targeted user or device. While this is useful for applications where the data provider knows specifically which user he wants to share with, in many applications the provider will want to share data according to some policy based on the receiving user's credentials which can be done by using Attribute Based Encryption (ABE). In this paper we going to discuss about several attribute based encryption scheme and its categories.

II. RELATED WORK

Sahai and Waters proposed Fuzzy Identity-Based Encryption [1] in 2005, and this paper proposed the first concept of the attribute-based encryption scheme through public key cryptography. Fuzzy Identity-Based Encryption in which identities as a set of descriptive attributes. Fuzzy IBE can be used for an application that we call attribute based encryption. In this scheme in which each user is identified by a set of attributes, and some function of this attributes is used to determine decryption ability for each cipher text. M. Pirretti, P. Traynor, P. McDaniel, and B. Waters proposed Secure attribute-based systems [2] in2006. This paper gave an implementation of the ABE encryption system with more complex access policy with (AND, OR gate) based on [1]. This work also demonstrated different applications of attribute-based encryption schemes and addressed several

Practical notions such as key-revocation and optimization. However, this work is dismissed after the proposal of KPABE and CP-ABE, which is more flexible and efficient. In 2006, Goyal et al. proposed an key-policy attribute-based encryption (KP-ABE) scheme [3]. Fine grained access control provided by KP-ABE as compared with classical model. In 2007 Bethencourt et al. proposed an cipher text policy attribute based (CP-ABE) scheme [4]. Data owner only trusts the key issuer as CP-ABE scheme addresses the problem of KP-ABE. Both KP-ABE and CP-ABE are able to enforce general access policies that can be described by a monotone access structure. Later on Muller proposed an distributed attribute-based encryption scheme in 2008, Yu e. proposed a fine grained data access control encryption scheme, Tang proposed a Verifiable attribute based encryption scheme. Ostrovsky et al. proposed an enhanced ABE scheme which supports non-monotone access structures [5]. In 2008 Muller et al. proposed an distributed attribute-based encryption scheme [6] . Wang et al. proposed a hierarchical attribute-based encryption scheme (HABE) [7] in 2010. Which integrates properties in both a HIBE (hierarchal identity based encryption) model and a CP-ABE model? There after

introduce MA-ABE(multi-authorities ABE)schemes [8] that use multiple parties to distribute attributes for users. Attribute-based encryption schemes can be further categorized as either monotonic or non-monotonic based on their type of access structure.

A. Attribute Based Encryption (ABE)

In this paper we survey and analyze different schemes available in Attribute Based encryption (ABE) including Key policy attribute based encryption(KPABE), Cypher text policy attribute based encryption(CPABE), Attribute-based Encryption Scheme with Non-Monotonic Access Structures,Multi authority attribute based encryption(MAABE) and we also include their pros and cons and a comparison table of each scheme based on fine grained access control,efficiency,computational overhead and collusion resistant.The concept of attribute based encryption was first proposed by Amit Sahai and Brent Waters. 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. Using ABE schemes can have the advantages: (1) to reduce the communication overhead of the Internet, and (2) to provide a fine-grained access control. 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 d. 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 use the access of monotonic attributes to control user's access in the system.

B. Key Policy Attribute Based Encryption (KP-ABE)

Goyal et al. provided a more expressive modification to ABE, called Key-Policy Attribute-Based Encryption (KPABE) which modified the original ABE scheme to allow the user's private key to contain the access structure of multiple levels of properties, while the encrypted texts contain a set of attributes or flags that are used to check if the key's access tree is satisfied. For example, if Alice's key in KPABE contains "X AND Y" as the access policy, the only files she can decrypt are those that have both attributes X and Y.A cipher text with only attribute X could not be decrypted by Alice, as the access tree would not be satisfied. Similar to that of the original ABE scheme, the keys given to users are also collusion resistant, meaning that two users could not use an overlap of attributes within their keys in order to decrypt files neither would be able to decrypt on their own. This is done through levels of secret sharing over the access tree, with values associated with each attribute in the key, just like the ABE designs.

KP-ABE scheme consists of the following four algorithms:

Setup: Algorithm takes input K as a security parameter and returns PK as public key and 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.

Encryption: Algorithm takes a message M, the public key PK, and a set of attributes as input. It outputs the cipher text E.

Key Generation: Algorithm takes as input an access structure T and the master secret key MK. It outputs a secret key SK that enables the user to decrypt a message encrypted under a set of attributes if and only if matches T.

Decryption: It takes as input the user's secret key SK for access structure T and the cipher text E, which was encrypted under the attribute set . This algorithm outputs the message M if and only if the attribute set satisfies the user's access structure T.

The main issue with KPABE is the fact that the control of the access to the encrypted data is only controlled by the attributes given to the file, and not a controlled access tree . A user encrypting a text in a KPABE scheme has no control over sets of attributes given to the users, and this makes fine control of access requiring multiple properties challenging.

C. Cipher Text Policy Attribute Based Encryption(CP-ABE)

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.In this scheme whenever we are encrypting a message M, the encryptor specifies an access structure which is expressed in terms of a set of selected attributes for M. The message is then 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 the cipher text even if they collude. A CP-ABE scheme consists of the following four algorithms:

Setup: This is a randomized algorithm that takes a security parameter as input, and outputs the public parameters PK and a master key MK. PK is used for encryption and MK is used to generate user secret keys and is known only to the central authority.

Encryption: This is a randomized algorithm that takes as input a message M, an access structure T, and the public parameters PK. It outputs the cipher text CT.

KenGen: This is a randomized algorithm that takes as input the set of a user (say X)'s attributes SX, the master key MK and outputs a secret key SK that identifies with SX.

Decryption: This algorithm takes as input the cipher text CT, a secret key SK for an attribute set SX. If SX satisfies the access structure embedded in CT, it will return the original message M.

Drawbacks of the most existing CP-ABE schemes are they still not fulfilling the enterprise requirements of access control which require considerable flexibility and efficiency. CPABE 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.

D. Attribute-based Encryption Scheme with Non- Monotonic Access Structures

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 attributes 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. This scheme proposes the first method that can add negative constraints to describe attributes. And it is flexible to use access policy for a data owner. This scheme contains four algorithms: Setup(), KeyGen(), Encrypt(), and Decrypt(), and they will be introduced as follows.

Setup(d): In the basic construction, a parameter d specifies how many attributes every ciphertext has. ***Encryption (M, γ,PK)***: To encrypt a message M ε GT under a set of d attributes γ C Zp, choose a random value s ε Zp and output the ciphertext E.

Key Generation (˜A,MK,PK): This algorithm outputs a key D that enables the user to decrypt an encrypted message only if the attributes of that ciphertext satisfy the access structure ˜A

Decrypt(CT;D): Input the encrypted data CT and private key D, if the access structure is satisfied it generate the original message M.

The problem with Attribute-based Encryption Scheme with Non- Monotonic Access Structures 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 each ciphertext needs to be encrypted with d attributes, where d is a system-wise constant.

E. Hierarchical attribute-based Encryption

Hierarchical attribute based encryption scheme is based on HABE model which integrates properties of both a HIBE model and a CP-ABE model. It consists of a root master (RM) and multiple domains, where the RM functions as the TTP, and the domains are enterprise users. More precisely, a domain consists of many domain masters (DMs) corresponding to the ITPs and numerous users corresponding to end users. The RM, whose role closely follows the root PKG in a HIBE system, is responsible for generation and distribution of system parameters and domain keys. The DM, whose role integrates both the properties of the domain PKG in a HIBE system and AA in a CP-ABE system, is responsible for dele-gating keys to the DMs at the next level and distributing secret keys to users. Specially, we enable the leftmost DM at the second level to administer all the users in a domain, just as the personnel office administers all personnel in an enterprise, and not to administer any attribute. Notice that other DMs administer an arbitrary number of disjoint attributes, and have a full control over the structure and semantics of their

attributes. In the HABE model, we first mark each DM and attribute with a unique identifier (ID), but mark each user with both an ID and a set descriptive attributes, where ID is an arbitrary string corresponding to some unique information about an entity. Then, as Gentry and Silverberg (2002), we enable each entity's secret key to be extracted from the DM administering itself. Each entity's public key, which denotes its position in the model, is an ID tuple consisting of the public key of the DM administering itself and its own ID.

Then, HABE scheme is defined by presenting randomized polynomial time algorithms as follows:

Setup (K)→(params,MK0): The RM takes a sufficiently large security parameter K as input, and outputs system parameters params and root master key MK0.

CreateDM(params,MKi, PKi+1) → (MKi+1): Whether the RM or the DM generates master keys for the DMs directly under it using params and its master key.

CreateUser(params,MKi, PKu, PKa) → (SKi,u, SKi,u,a):The DM first checks 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". ***Encrypt(params; f ;A; {PKa|a E A})→(CT):*** A user takes a file f, a DNF access control policy A, and public keys of all attributes in A, as inputs, and outputs a ciphertext CT.

Decrypt(params,CT,SKi,u,{SKi,u,a|aECCj}→(f):A user,whose attributes satisfy the j-th conjunctive clause CCj, takes params, the ciphertext, the user identity secret key, and the user attribute secret keys on all attributes in CCj, as inputs, to recover the plaintext.

E. Multi-Authority Attribute Based Encryption

A multi-authority ABE system consists of any number attribute authorities and any number of users. A set of global public parameters is defined in the system. A user can select an attribute authority and obtain the corresponding decryption keys. The authority executes the corresponding attribute key generation algorithm and the result is returned to the user. The encryption process uses the global public parameters and an attribute set to produce the cipher text. Decryption is performed using the decryption keys for the attribute set. Chase proposed a multi-authority attribute-based encryption system to overcome the drawbacks of a single authority attribute-based system. This system uses a central authority (CA) and multiple attribute Authorities (AAs). The problem with the Chase multi-authority attribute-based encryption system is that the CA can decrypt every cipher text which reduces the user privacy and confidentiality of user data. This system consists of the following five algorithms.

Setup: The algorithm generates a public key, secret key pair for each of the attribute authorities, and also outputs a system public key and master secret key.

Attribute Key Generation: The algorithm generates a private key for the user.

Central Key Generation: The algorithm generates a central secret key for the user.
Encryption: The sender encrypts the message and outputs the cipher text.
Decryption: The user executes the decryption algorithm and decrypts the cipher text.
The scheme can provide collusion resistance against any number of colluding users. With this feature, multi-authority attribute based encryption as proposed by Chase becomes one of the powerful attribute-based encryption schemes used in cloud computing. However, each authority's attribute set must be disjoint. To overcome this problem, we can create a separate copy of each attribute for each clause. The CA can decrypt every cipher text so that the user privacy and confidentiality of the data is less in this system.

III. COMPARASION

In this section, we compare these schemes based on data confidentiality, fine grained access control, scalability, user accountability, user revocation and collusion resistant.

Table 1: Comparison of schemes based on various criteria

Criteria	ABE	KP-ABE	CP-ABE	ABE with no monotonic	HABE
User Revocation	NS	S	S	S	S
Collusion Resistant	S	S	S	S	S
Fine Grained Access control	S	S	S	S	S
Scalability	NS	NS	NS	NS	S
User Accountability	NS	NS	S	NS	S

****Note- S-Satisfactory NS-Not Satisfactory***

IV. CONCLUSION

The comparative study of different attribute based encryption schemes like KP-ABE,CP-ABE,ABE with non monotonic access structure,HABE,MABE based on various parameters suggest that these schemes are classified according to their access policy and after analyzing these schemes we found that the main access policies are KP-ABE and CP-ABE and further policies are derived using either of these policies as a base. We further found that CP-ABE removes key escrow problem of KP-ABE because of its unique key issuing mechanism and enhances data privacy and confidentiality in the data sharing system. Thus we demonstrated that cipher text policy based ABE schemes are more efficient and scalable to securely manage user data in the data sharing system.

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in Proc.EUROCRYPT, 2005, pp. 457473.
[2] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. "Secure attribute-based systems". In Proceedings of the 13th ACM conference on Computer and communications security, pages 99{112. ACM Press New York, NY, USA,2006.
[3] 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, pp. 89{98, 2006}
[4] J. Bettencourt, A. Sahai, and B.Waters"Ciphertext-policy attribute based encryption "in Proceedings of IEEE Symposium on Security and Privacy, pp. 321V334,2007.
[5] R. Ostrovsky and B. Waters. "Attribute based encryption with nonmonotonic access structures".In Proceedings of the 14th ACM conference on Computer and communications security, pages 195{203. ACM New York, NY,USA,2007.
[6] Muller, S. Katzenbeisser, and C.Eckert, "Distributed attribute-based encryption," in Proceedings of ICISC, pp. 20{36, 2008}.
[7] M. Chase. "Multi-authority attribute based encryption". In TCC, pages 515-534, 2007
[8] G. Wang, Q. Liu, and J.Wu,"Hierachical attibute- based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM conference on Computer and communications security.
[9] V Bozovic, D Socek, R Steinwandt, and V. I. Vil-lanyi, "Multiauthority attribute-based encryption with honest-but-curious central authority" International Journal of Computer Mathematics, vol. 89,pp. 3, 2012.

