ISSN:0975-9646

Privacy-Preserving Decentralized Key Policy Attribute-Based Encryption

Girija Patil

MCT's Rajiv Gandhi Institute of Technology
Department of Computer Engineering
Andheri(W), Mumbai-53, India.

Abstract— **In Attribute-based Encryption (ABE) scheme, attributes play a crucial role. Attributes have been utilized 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 divided as either key-policy or cipher text-policy. The key-policy is the access structure on the user's private key, and the cipher text-policy is the access structure on the cipher text. And the access structure can also be further divided as either monotonic or non-monotonic one. Using ABE schemes one can have the advantages: (1) to reduce the communication overhead of the Internet, and (2) to provide fine-grained access control.**

Keywords— ***ABE; Decentralized ABE scheme; privacy-preserving; GID.***

I. INTRODUCTION

In old access control schemes, a central authority can have control a user's access to sensitive and important data. Following drawbacks in these schemes are observed, specifically in distributed systems. Firstly, since a user's identity needs to be updated by the authority, in a large distributed system, it is a not possible task to manage numerous users' identities. Furthermore, all users must trust the central authority. If the authority is harmful, he can give access any user without being detected. Being different from the traditional access control schemes, attribute-based access control are the schemes that allow users to be validated by the analyzing attributes instead of their unique identities. Furthermore, a user can share his data by giving an access structure so that all the users whose attributes satisfy it can access the data without having any knowledge about their identities. Therefore, attribute-based access control schemes are systematic primitives to exchange data with multiple users without knowing their identities.

In order to minimize the trust on the central authority, some of the decentralized and distributed access control schemes are taken into consideration. Although, decentralized attribute based access control schemes denote lots of metrics, they are rarely consider for the user's privacy. Hence, a user's attributes could be exposed to the harmful authorities. . Also, to provide a sound solution for sharing delicate data with various users in distributed systems, the scheme for a decentralized attribute-based access control with privacy preserving scheme should be put forward. In an open source communication surrounding, for example Internet, delicate data must be encrypted before being transmitted. To attain this, encryption schemes can be used to protect the confidentiality of the sensitive data. Nonetheless, customary encryption schemes cannot express a complex access policy, and furthermore, the sender must have all the public keys of the receivers.

Attribute-based encryption (ABE) introduced by Sahai and Waters is a more systematic encryption scheme and it can express a complex access structure. In an ABE scheme, the user's secret private keys and the cipher text are labelled with sets of attributes. The encrypter can encrypt a message by using a set of attributes. Before decrypting the cipher text, the receiver must receive the secret keys from the central authority (CA). The receiver can decrypt the cipher text and get the data if and only if match between his secret keys and the attributes listed in the cipher text if obtained. The central idea of ABE is to construct a fuzzy (error-tolerant) identity-based encryption (IBE). Since its influential introduction, ABE as a special primitive has engaged a lot of attention in the research community.

Fundamentally, there are two kinds of ABE schemes: Key-Policy ABE (KP-ABE): In these schemes, the private keys are related with an access structure, while the cipher text is labelled with a set of attention in the research community. Fundamentally, there are two kinds of ABE schemes: Key-Policy ABE (KP-ABE): In these schemes, the private keys are related with an access structure, while the cipher text is labelled with a set of attributes .Cipher text-Policy ABE (CP-ABE): In these schemes, the cipher text is associated with an access structure, while the secret keys are associated with a set of attributes. In an ABE scheme, an access structure is selected by the authority (in KP-ABE) or the encrypter (in CP- ABE) to control who can decrypt the cipher text. First CP-ABE scheme was proposed by Bettencourt, Sahai and Waters, and it proved to be secure in the generic group model. In opposite with KPABE, the access structure in CP-ABE is decided by the encrypter, instead of the CA. Hence, the encrypter can take decision of who will decrypt the cipher text; while, this is decided by the CA in the KP-ABE schemes.

II. TYPES OF ENCRYPTION TECHNIQUES.

A. Multiple Authority Attribute Based Encyption

In their innovative work, Sahai and Waters left an open question that whether it is possible to construct an ABE scheme where the secret keys can come from various authorities. Chase answered this question positively by

proposing the idea of a multi-authority KP-ABE scheme. In this scheme, there are various authorities, from which one is called central authority. The central authority has information about the secret keys of the other authorities. The user needs to extract secret keys from all these authorities. Being dissimilar from one authority ABE, it is difficult to resist collusion attacks in multi-authority ABE schemes. If the multiple authorities can work separately, the scheme is profound to this attack. Chase mastered this problem by introducing the global identifier (GID) to the multi-authority ABE scheme. All the user's secret keys from multiple authorities must be tied to his GID. In order to let the cipher text is separate of the user's GID, the central authority must calculate a special secret key for the user using his secret key and the other authorities' secret keys. Even though this scheme is not a decentralized ABE scheme, Chase made an influential step from one authority ABE to multi-authority ABE. Chase and Chow proposed one more multi-authority KP-ABE scheme which enhanced the previous scheme and removed the need of a central authority.

The system uses the following algorithm:
***Setup* :** A randomized algorithm which must be run by some trusted party (e.g.central authority). Takes as input the security parameter. Outputs a public key, secret key pair for each of the attribute authorities, and also outputs a system public key and master secret key which will be used by the central authority.
Attribute Key Generation : A randomized algorithm run by an attribute authority. 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. (We will assume that the user's claim of these attributes has been verified before this algorithm is run). Output secret key for the user.
Central Key Generation : A randomized algorithm run by the central authority. Takes as input the master secret key and a user's GID and outputs secret key for the user.
Encryption : A randomized algorithm run by a sender.
Takes as input a set of attributes for each authority, a message, and the system public key. Outputs the ciphertext.
Decryption : A deterministic algorithm run by a user. Takes as input a cipher-text, which was encrypted under attribute set AC and decryption keys for an attribute set Au.
Features:

1. No trusted central authority
2. User privacy
3. Distributed pseudo random functions are used in the system
4. Collusion resistance for any number of colluding users.

The scheme also defines an anonymous key issuing protocol. This protocol provides improved user privacy.

B. Attribute Based Encryption

An attribute based encryption scheme discovered by Sahai and Waters in 2005 and the final goal is to provide security and access control. Attribute-based encryption (ABE) is a public-key based one to many encryption that lets users to encrypt and decrypt data based on user attributes. In which the secret key of a user and the ciphertext 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 ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. Decryption is only possible when the number of matching is at least a threshold value . Collusion-resistance is important security feature of Attribute-Based Encryption .An adversary that holds multiple keys should only be able to access data if at least one individual key grants access. The drawback 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.

C. Cipher Text Policy Attribute Based Encryption.

Another enhanced form of ABE called CP-ABE invented by Sahai. In a CP-ABE scheme, every cipher text is related with an access policy on attributes, and every user's private key is related with a set of attributes. A User is able to decrypt a cipher text only if the set of attributes related with the user's private key satisfies the Access policy associated with the cipher text. CP-ABE executes in the reverse way of KP-ABE. The access structure of this scheme or algorithm, it inherits the same method which was used 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 similar to the traditional access control schemes. The encryptor who specifies the threshold access structure for his interested attributes while encrypting a message. Based on this access structure message is then encrypted such that only those whose attributes satisfy the access structure can decrypt it. The most existing ABE schemes are obtained from the CP-ABE scheme.
CP-ABE scheme consists of following four algorithms
Setup : This 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.
Encrypt : This algorithm takes as input the public parameter PK, a message M, and an access structure T. It outputs the ciphertext CT.
Key-Gen : This algorithm takes as input a set of attributes associated with the user and the master secret key MK. It outputs a secret key SK that enables the use

D. Key-Policy Attribute Based Encyption.

It is the modified form of classical model of ABE. Users are assigned with an access tree structure over the data attributes. Threshold gates are the nodes of the access tree. The attributes are associated by leaf nodes. To reflect the access tree Structure the secret key of the user is defined. Ciphertexts are labelled with sets of attributes and private keys are associated with monotonic access structures that control which ciphertexts a user is able to decrypt. Key

Policy Attribute Based Encryption (KP-ABE) scheme is designed for one-to-many communications.
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 ciphertext 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 ciphertext 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 KP-ABE scheme can achieve fine-grained access control and more flexibility to control users than ABE scheme. The problem with KP-ABE scheme is the 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.

E .Privacy Preserving Decentralized Key-Policy Attribute Based Encryption.

In this section, a decentralized KP-ABE scheme based on the DBDH assumption is explained. After that description of a privacy-preserving extract protocol for the secret keys is explained. In this privacy-preserving decentralized KP-ABE scheme, a user executes a 2-party secure computation protocol with an authority to gain his secret keys. Hence, the user can gain his secret keys unknowingly without releasing anything about his identifier to the multiple authorities. As pointed in, an unknown credential system can be used by the user to satisfy the authorities that he holds the corresponding attributes without revealing his identifier. In an unknown credential system, a user can gain a credential and prove the possession unknowingly. The user can interact with various partners with different pseudonyms such that no partner can link the pseudonyms to the same user. Moreover, the user can prove that he has gained multiple credentials which correspond to the same identifier without revealing it.
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 KP-ABE scheme can achieve fine-grained access control and more flexibility to control users than ABE scheme. The problem with KP-ABE scheme is the 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.

F. Cipher Text Policy Attribute Based Encryption

Another enhanced form of ABE called CP-ABE invented by Sahai. In a CP-ABE scheme, every cipher text is related with an access policy on attributes, and every user's private key is related with a set of attributes. A User is able to decrypt a cipher text only if the set of attributes related with the user's private key satisfies the Access policy associated with the cipher text. CP-ABE executes in the reverse way of KP-ABE. The access structure of this scheme or algorithm, it inherits the same method which was used 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 similar to the traditional access control schemes. The encryptor who specifies the threshold access structure for his interested attributes while encrypting a message. Based on this access structure message is then encrypted such that only those whose attributes satisfy the access structure can decrypt it. The most existing ABE schemes are obtained from the CP-ABE scheme.

CP-ABE scheme consists of following four algorithms.
Setup : This 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.
Encrypt : This algorithm takes as input the public parameter PK, a message M, and an access structure T. It outputs the cipher text CT.
Key-Gen : This algorithm takes as input a set of attributes associated with the user and the master secret key MK

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. Drawbacks of the most existing CP-ABE schemes are 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. After that cipher text-policy attributes based encryption (CP-ASBE or ASBE for short) is introduced by *Bobba, Waters et al* [7]. ASBE is an extended form of CP-ABE. It organizes user attributes into a recursive set based structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. The CP-ASBE consists of recursive set of attributes. The challenge in constructing a CP-ASBE scheme is inselectively allowing users to combine attributes from multiple sets within a given key. There is challenge for preventing users from combining attributes from rmultiplekeys.

G. Hierarchical Attribute-Based Encryption Scheme

In 2011, Wang et al. proposed a hierarchical attribute-based encryption scheme composed of a hierarchical identity-based encryption scheme (HIBE) and a cipher text-policy attribute-based encryption scheme. This scheme used the property of hierarchical generation of keys in HIBE scheme to generate keys. Moreover, it used disjunctive normal form (DNF) to express the access control policy, and the same domain authority in this scheme administered all attributes in one conjunctive clause. There are ¯ve roles in this scheme: the cloud storage service, data owner, the root authority, the do-main authority, and data users. The role of cloud storage service is that let a data owner can store data and share data with users. The role of data owner is encrypting data and sharing data with users. The role of the root authority is generating system parameters and domain keys, to distribute them. The role of domain authority is managing the domain authority at next level and all users in its domain, to delegate keys for them. Besides, it can distribute secret keys for users. And users can use their secret keys to decrypt the encrypted data and obtain the message. The key generation in this scheme adopts a hierarchical method. The root authority generates a root master key for domain authority at the ¯rst level. The system public key and the master key of the domain authority at high level are used to create the master keys for the domain authorities at the next level by the root authority or the domain authority at the ¯rst level. In addition, the do-main authority generates the user identity secret key and the user attribute secret key for the authorized user.

III. CONCLUSION

Different attribute-based encryption schemes: ABE, KP-ABE, CP-ABE, ABE with non-monotonic access structure, HABE and MA-ABE is described in paper. The main access polices are KP-ABE and CP-ABE, further schemes are obtained based on these policies. Based on their type of access structure the schemes are categorized as either monotonic or non-monotonic. CHABE an adaptation of Attribute Based Encryption (ABE) for the purposes of providing guarantees towards the provenance the sensitive data, and moreover towards the anonymity of the data owner. It is unrealistic to assume there is a single authority which can monitor every single attribute of all users. Multi-authority attribute-based encryption enables a more realistic deployment of attribute-based access control, such that different authorities are responsible for issuing different sets of attributes. The original solution by Chase employs a trusted central authority and the use of a global identifier for each user, which means the confidentiality depends critically on the security of the central authority and the user-privacy depends on the honest behavior of the attribute-authorities.

REFERENCES.

[1]. 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.

[2]. Q. Liu, G. Wang, and J. Wu, “Time based proxy re-encryption scheme for secure data sharing in a cloud environment," Information Sciences In Press, 2012.

[3]. Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran, “AttributeSets: A Practically Motivated Enhancement to Attribute-Based Encryption”, July 27, 2009.

[4]. A. Lewko, T. Okamoto, A. Sahai, K. Takashima, and B. Waters, “Fully secure functional encryption: Attribute- based encryption and (hierarchical) inner product encryption,” in *Proceedings: Advances in Cryptology-EUROCRYPT’10* (H. Gilbert:, ed.), vol. 6110 of *Lecture Notes in Computer Science*, (French Riviera), pp. 62–91, Springer, May 30 - June 3 2010.

[5]. B. Waters, “Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization,” in *Proceedings: Public Key Cryptography - PKC’11* (D. Catalano, N. Fazio, R. Gennaro, and A. Nicolosi, eds.), vol. 6571 of *Lecture Notes in Computer Science*, (Taormina, Italy), pp. 53–70, Springer, March 6-9 2011.

[6]. A. Rial and B. Preneel, “Blind attribute-based encryption and oblivious transfer with fine-grained access control,” in *2010th Benelux Workshop on Information and System Security- WISSec’10*, pp. 2010

[7]. S. Yu, K. Ren, and W. Lou, “FDAC: Toward fine- grained data access control in wireless sensor networks,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 22, no 4, pp. 673–686, 2011.

[8]. J. Hur and D. K. Noh, “Attribute-based access control with efficient revocation in data outsourcing systems,” *IEEE Transactions on Parallel and Distributed Systems*, vol. 22 no 7, pp. 1214–1221.2011.