Various Security Enhanced Techniques based on attributes

Jayvir Kher[1], Narendra Singh[2]

[1]Student, Dept. of Computer Science and Engineering, Parul Institute of Engineering and Technology, Gujarat, India

[2]Ass. Professor, Dept. Of Computer Science and Engineering, Parul Institute of Engineering and Technology, Gujarat, India

---

Abstract – *Nowadays the vast amount of data and web contents are available, so the data security is more difficult. Recently the trends to store or share the data in the third party servers. But third party servers must be trust if it is not trusted then possibility to lose the confidential data. So the data should be protected. In this paper we are discuss about various security methods which is based on attribute of user and secure data sharing methods.*

Key Words: Attribute Based Encryption, security, Data Sharing, CP-ABE, KP-ABE

1. INTRODUCTION

Defending networks from computer security attack is a critical apprehension of computer security. Since the big amount of text is commonly uploaded into many sites and thus it need to be secured particularly when confidential information is uploaded. Currently network and computing are more developed technologies. This enable many users to easy share and update their confidential information with others via online storage i.e. cloud. As people love the advantages of these new technologies & services, their main fears about data security and effective access control. Incompatible access of the data by the storage server or unauthorized access by beyond users could be possible threats to their data [1].Since the data is private and needs to be made ensure from wildcat users in the network. Also the data security is made possible by providing various access policies in the network based on the attributes or identity of the users [4].

It is crucial to protected data that is transferred in to various social sites or put in online. Attribute-based encryption (ABE) is a assuring cryptographic method that reaches a fine-grained data access control [5], [6], [7], [8]. It feeds a way of determining access policies based on various attributes of the requested user, scenario, or the data object. Especially, CP-ABE enables an encryptor to set the attribute set over a universe of attributes that a decryptor needs to own in order to decrypt the ciphertext, and apply it on the contents [5]. Thus, each user with a dissimilar set of attributes is permitted to decrypt dissimilar parts of data per the security policy.

Although there are several techniques enforced for the encryption of the data in the network, one such technique is IBE. IBE is a technique which is based on the encryption of the data applying identity of users. The theme is to generate a key pairs which is based on the identity of the users and the encryption and decryption of the data is potential using these identities. Fuzzy Identity based encryption is a technique which is more efficient as compared to the existing IBE, since fuzzy Identity Based Encryption provides authentication using biometric technique and encryption based on the biometric identity of the user [5].

In ABE an encryptor will associate encrypted data with a set of attributes. An authority will fear users diverse private keys, where a user's private key is connected with an access structure over attributes and shine the access policy ascribed to the user [8]. In an ABE system, the various keys are got based on the attribute of the users and also the various cipher text. Such type of techniques needs to be more precise and efficient and error free as equated to other IBEs and is also useful for big systems [6].

CP-ABE [6] is a PKC primitive that is used to decide the exact issue of fine-grained access control on shared data in one-to-many communications. In CP-ABE, each user is allotted a set of attributes which are planted into the user's secret key. A public key element is defined for every user attribute. When encrypting the message, the encryptor takes an access structure on attributes, and encrypts the message under the access structure through encrypting with the corresponding public key elements[4].

For better security we must consider some parameters that are essential like Data confidentiality, Collusion resistance, single point of failure and Backward and forward secrecy. Unauthorized users who do not have enough attribute satisfying the access policy should be protected from accessing the plaintext of the data. Collusion resistance is one of the most important security property required in Attribute Based Encryption systems [5], [6], [7]. If multiple users get together, they may be able to decrypt a ciphertext by combining their attributes even if each of the users can't decrypt the ciphertext alone. In the context of ABE, backward secrecy signifies that some user who comes to hold an attribute (that satisfies the access policy) should be protected from accessing the plaintext of the old data distributed before he keeps the attribute [1].

2. RELATED WORK

In [1] authors proposed Improving security and efficiency in attribute-based data sharing. They offered a novel CP-ABE scheme for a assure data sharing system, which features the following achievements. Here in this paper various problems like Escrow based problem and proxy-encryption based problems are resolved using ABE techniuqes.

Second, the quick user revocation can be performed via the proxy encryption mechanism together with the CP-ABE algorithm. Attribute group keys are exclusively distributed to the legal users in each attribute group, which then are use to re-encrypt the cipher text encrypted under the CP-ABE algorithm. The immediate user revocation enhances the backward/forward privacy of the data on any membership alterations. Additionally, as the user revocation can be done on each attribute level rather than on system level additional fine-grained user access control can be achievable. Even if a user is retracted from various attribute groups, it would still be able to decrypt the shared data as long as the other attributes that he keeps satisfy the access policy of the ciphertext [1]. Data owners need not be concerned about defining any access policy for users, excluding just want to describe only the access policy for attributes as in the prior ABE schemes.

This scheme delegates most hard tasks of membership management and user revocation to the data storing center while the Key Generation Center is responsible for the attribute key management as in the previous CP-ABE schemes without leaking any sensitive information to the other users. Consequently, this scheme is the most suitable for the data sharing scenarios where users encrypt the data only one time and upload that data to the data-storing centers, and disappear the rest of the odd jobs to the data storing centers such as reencryption and revocation [1].

Amit Sahai and Brent Waters proposed Fuzzy IBE. They present two constructions of Fuzzy IBE schemes. This construction can be viewed as an IBE of a message under various attributes that compose a identity. This Identity Based Encryption schemes are both error-tolerant and safe against collusion attacks. Additionally, our basic construction does not use random-oracles. They prove the security of this method under the Selective-ID security model. They first introduced ABE for ciphered access control. In an Attribute Based Encryption system, both the user secret key and ciphertext are associated with a set of attributes. Only if threshold number of attributes match between the ciphertext and his secret key, can the user decrypt the ciphertext [5].

V. Goyal et al. [4] first introduced the concept of CPABE based on Attribute Based Encryption. The idea is to develop a much richer and secure type of ABE system. In this system each ciphertext is labeled by the encryptor with a set of attributes.KP-ABE, since the access structure is specified in the private key, while the ciphertexts are simply marked with a set of descriptive attributes. A user is able to decrypt a ciphertext if the attributes related with a ciphertext satisfy the access structure of key. Their construction supports delegation of private keys which related Hierarchical Identity-Based Encryption (HIBE) [6].

Bethencourt et al [7] suggested CP-ABE and give the first construction of such a scheme. In this system, a user's private key will be related with an arbitrary number of attributes carried as strings. On the other hand, when a party encrypts a message in this system, they specify an related access structure over attributes. A user will only be allow to decrypt a ciphertext if that user's attributes pass through the cipher texts access structure. At a mathematical level, access structures in our system are identified by a monotonic access tree, where nodes(access tree's) of the access structure are wrote of threshold gates and the leaves describe attributes. This system appropriates for a new type of encrypted access control where user's secret keys are assigned by a collection of attributes and a client encrypting data can specify a policy over these attributes assigning which users are capable to decrypt. This system allows policies to be showed as any monotonic tree access structure and is tolerant to collusion attacks in which an attacker might obtain more than one private keys. Finally, they provided an implementation of this system, which admitted various optimization methods.[7].

R. Ostrovsky et al [8] proposed Attribute-Based Encryption with Non-Monotonic Access Structures. They present a new ABE scheme where private keys can stand for any access formula over attributes. In particular, our construction can handle any access structure that can be shown by a Boolean formula involving OR, AND, NOT, and threshold operations. At a high level, the technical novelty in our work lies in determining a way to make a share "available" to the decryptor only if a given attribute is not present between the attributes of the cipher text. In designing this construction several challenges come up from adapting these negation techniques while protecting the collusion resistance features that are necessary for ABE systems. They achieved this through a modern application of revocation methods into existing ABE schemes. In addition, the execution of our scheme compares very favorably to that of existing, less-expressive ABE systems. An significant goal in ABE systems is to create even more expressive systems [8].

3. COMPARATIVE STUDY OF DIFFERENT METHODS

Table 1 shows the comparison among the different ABE methods.

Table -1: Comparison of various ABE methods

Sr.No	Paper	Association of Attributes	Association of access policy	Computational overhead	Single point of failure	Collusion resistance
1	[1]	With key	With ciphertext	average	Yes	Average

2	[3]	With key	With ciphertext	high	Yes	average
3	[5]	With ciphertext	With key	Low	Yes	Below average
4	[6]	With ciphertext	With key	average	Yes	average
5	[4]	With key	With ciphertext	average	Yes	average

4. CONCLUSIONS

Nowadays Computer Science technologies have pulled more and more people to store and share their sensitive data on third party servers for cost saving. Data confidentiality achieving by the attribute based encryption methods because outside user have not sufficient attribute to compromise. The survey about various ABE scheme that provide more security but contain some limitations like they not provide more resistance against single point of failure. For this several methods were proposed by researchers. In this paper we introduce some of them.

REFERENCES

[1] Hur, Junbeom. "Improving security and efficiency in attribute-based data sharing", IEEE Transactions On Knowledge And Data Engineering, Vol. 25, No. 10, pp. 2271 – 2282, October 2013.

[2] Minu George1, Dr. C.Suresh Gnanadhas2, Saranya.K3,” A Survey on Attribute Based Encryption Scheme in Cloud Computing”, IJARCCE November 2013.

[3] Sanjam Garg Craig Gentry Shai Halevi Amit Sahai Brent Waters,” Attribute-Based Encryption for Circuits from Multilinear Maps”, 2012.

[4] Yu, Shucheng, Cong Wang, Kui Ren, and Wenjing Lou. "Attribute based data sharing with attribute revocation." In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, pp. 261-270. ACM, 2010.

[5] A. Sahai and B. Waters, “Fuzzy Identity-Based Encryption,” Proceedings International Conference on Theory and Applications of Cryptographic Techniques (Eurocrypt ’05), pp. 457-473, 2005.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-BasedEncryption for Fine-Grained Access Control of Encrypted Data,”Proceedings of ACM Conference on Computer and Communication Security, pp. 89-98, 2006.

[7] J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-PolicyAttribute Based Encryption,” Proceedings IEEE Symposium Security andPrivacy, pp. 321-334, 2007.

[8] R. Ostrovsky, A. Sahai, and B. Waters, “Attribute-Based Encryptionwith Non-Monotonic Access Structures,” Proceedings ACM Conference Computer and Comm. Security, pp. 195-203, 2007.

[9] Boldyreva, Alexandra, Vipul Goyal, and Virendra Kumar. "Identity-based encryption with efficient revocation." In Proceedings of the 15th ACM conference on Computer and communications security, pp. 417-426. ACM, 2008.