A Survey on Attribute-Based Access Control Mechanisms in Cloud Environments for Secure Healthcare Data Sharing and Privacy-Preserving Biomedical Systems

Dr. Hana Kim[1]
Prof. Giulia Conti[1]
[1] University of Toronto, Department of Cybersecurity and Health Informatics Systems, Toronto, Canada

,

ABSTRACT

Cloud computing is a top emerging technology in the IT industry. It is a computing mode, which provides users with services, applications, storage and so on. Due to the internet based storage of cloud computing there exist a lot of security risks for the outsourced data. Several techniques including attribute based encryption (ABE) is introduced to provide security to the outsourced data. Most of the outsourced data in cloud suffer from large complexity in implementing access policies. In Attribute-based Encryption (ABE)[4] scheme, attributes has a very important role where a set of values are treated as user identity. Encryption and decryption is done using these set of values. ABE scheme is further extended to key-policy attribute based encryption (KP-ABE)[6] and ciphertext-policy attribute based encryption (CP-ABE)[2]. Other schemes are hierarchical attribute-based encryption (HABE)[3] scheme and the hierarchical attribute-set-based encryption(HASBE)[1] scheme. In this paper we conduct a survey on various attribute based access control techniques which provides security for the data in cloud computing.

KEYWORDS: Attribute based encryption, cloud computing, cloud service provider, data owner, data user.

1. INTRODUCTION

Cloud computing, is a service that enables users to store large amount of data in their cloud servers and provide with several other services on-demand. In the last several years, cloud computing has become one of the top emerging technology. The cloud storage service helps the user to store his/her data in the cloud servers and retrieve them via the internet. The advantages of using cloud are that accessing data is fast and easy, scalable, pay per use, and no maintenance is necessary. Different service models have been proposed for cloud. IaaS, PaaS and SaaS. One of the security issues concerned with cloud is the issues in security and users privacy of the outsourced data in cloud. Due to the storage in an internet basis, cloud faces lots of security threats. In cloud, owner of the data can upload the data files into the cloud server whereas the data user can download and use the data uploaded by the owner. Along with security, the data owners must also provide flexible and efficient access control in the cloud model. That is, only the users who are authorized can access the files in the cloud. So a flexible and scalable access control policy is required. The Attribute based encryption scheme was first introduced by Sahai and Waters[4]. In this scheme some attributes exist with the encryption and the decryption key. The identity about the user is defined by a set of data which should match with the attributes that are present with the cipher text only by which the person who request can access the data. The ABE schemes are further extended to KP-ABE[6] and CP-ABE[2]. This classification is done based on how the access policies are based with the cipher text and users keys which are private. In 2006, Goyal et al. introduced a scheme that is the KPABE scheme[6]. In this scheme, the access policies are linked with the cipher text. And the attributes are attached with the users keys. The second technique is the CP-ABE scheme[2] which was proposed in 2007. In this scheme, the access policy is present with the users key which is kept private. This scheme is more closer to the traditional encryption schemes. Then a scheme similar to the CP-ABE was proposed which is the CP-ABSE[5] which uses an attribute set. In 2011 Wang, Q. Liu, and J.Wu introduced HABE[3]scheme which a combination of hierarchical identity-based encryption scheme (HIBE) and CPABE[2]. The scheme is further extended to the hierarchical attribute-set-based encryption (HASBE)[1] scheme.

2. RELATED WORKS

In this section we study different attribute based encryption schemes such as ABE, KP-ABE, CP-ABE, CPABSE, HABE, HASBE. We compare these techniques, their performance, efficiency and computational overhead.

Attribute based encryption

ABE[4] was proposed by Sahai and Waters in 2005. In this scheme some attributes are chosen as user identity which is used to authorize the user to access a particular file. There are three parties in this system. The authority, data owner, and the data user. The data owner is the person who uploads the data into the cloud. The data user uses or access the data which is uploaded by the data owner. The authorities role is to provide the

public keys to the owners for encryption and private keys to the users for decryption. The owner of data encrypts the file and the cipher text will be associated to an attribute set. Similarly an attribute set is linked with the users private key. The attributes in the users private key must satisfy or match with the set linked with the cipher text by which the user can access the data. Else the user will not be authorized or he/she cannot access the data uploaded by the owner. The advantage of this system is that suppose if a new person wants to join the system, then they will redefine a new set of values and generate the keys. The authority does not need to start a new process to add a user. Also, this scheme helps to reduce the proportion of time needed for communication and also provides better access control for the data users. One of the problem concerned with this scheme is that the data owner while encrypting the data, need to use every users public key for the encryption process. The ABE schemes are further extended to KP-ABE[6] and CP-ABE[2].

B. Key-Policy Attribute-based Encryption

In 2006 oyal introduced the KP-ABE[6] scheme. Here a set of attributes are used with the cipher text. The access rule is defined in the user's private key. When the data owner encrypts the data he uses a set of values which is linked with the cipher text. The user's key has an access policy which has a monotonic tree structure. If the user wants to access the data then the tree structure must satisfy the values that are linked with the encrypted data. The tree access structure consists of nodes where the nodes represent the threshold gates and the leaves represent the values. In this scheme the data owner defines the attributes linked with the cipher text. The data owner does not know who decrypts the data because the access policies are defined in the user's key. This is one of the drawbacks of this scheme that the data owner will have to trust the issuer of the key without the concern about the decryptor. So this scheme is not suitable to apply in real cases. The disadvantage of this scheme is overcome in the CP-ABE.

C. Ciphertext-Policy Attribute-based Encryption

In 2007, Bethencourt et al. introduced a CP-ABE[2] scheme. The CP-ABE scheme is similar to the KP-ABE and also it overcome the disadvantage in the KP-ABE. In this scheme an access policy is linked with the cipher text where the access policy is represented as a tree structure. The tree access structure consists of nodes where the nodes represent the threshold gates and the leaves represent the values. The users key is linked with a set of values which define some unique user identity. The attributes must satisfy the access policy linked with the cipher file. Thus the user can decrypt the required data. Else the required person cannot get the data. In this scheme the authority distributes the public and master keys to the data owner and user. The data owner converts the data to cipher text using this public key and the data user decrypts using the private key got from the authority. Here the data owner decides the access policies thus the owner of the data has the authority about the encryption policy. This scheme provides better access control over other methods and can be implemented in real time environments.

D. Ciphertext Policy Attribute-Set-Based Encryption

CP-ASBE[5] is a scheme which is almost similar to the CPABE but in this scheme it supports multiple value assignments for the attributes within a single key. In real time cases an attribute may have two or more different values where all the values are valid. The scheme allows the data owner to combine compound attributes or apply different combinations of attributes. Here attributes are arranged in recursive sets. A single set may contain many subsets which define the attributes within them. This scheme helps to solve complex access control policies and use the scheme for real time applications. The system contains four parties. Cloud Service Provider, Data owner, Data user and Attribute Authority. The attribute authority authorizes the user and provides keys to the data owner and user for encrypting and decrypting the data. The authority allows multiple value assignments for the same attributes. The model in Figure 1 shows the access control mechanism in the CP-ASBE scheme. Here the attribute authority is the root authority and maintains the recursive key set.

Fig.1. System model

E. Hierarchical Attribute Based Encryption

HABE[3] scheme was proposed by Wang et al. In 2011. This scheme is a combination of two other schemes. They are the HIBE and CP-ABE scheme. This scheme proposes a hierarchical structure of key generation. The structure consists of the Root master, the Domain authority, Data owner, Data users and the cloud storage provider. The outsourced data is stored in the cloud storage provider. The data owner encrypts and stores the data into the cloud storage. The access policies defined at the time of encryption is similar to CP-ABE. The root master controls the domains under it. It distributes the security parameters and keys to the domains in the level just below it. The domains manage those domains which are in the levels below it. They manage the data owners and data users. Each level in this system is provided with a public key and a master key. It is the task of the domain to provide the secret keys to the users. The authorization of the users takes place using this secret key. The structure of this model is shown in fig.2. This model provides one-to-many communications and also provides better access control. The system has more advantages out of the other schemes due to its hierarchical structure which divides the task of the root to the domains below it.

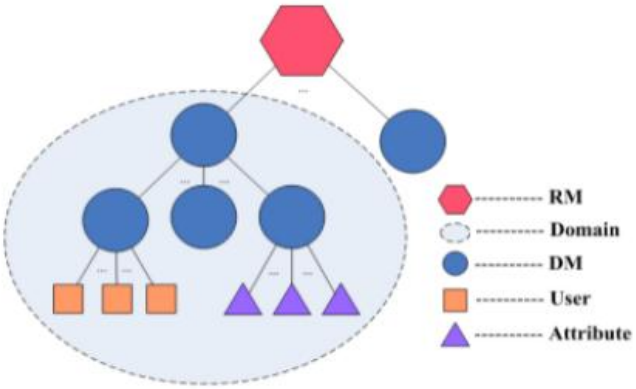

Fig. 2. HABE model

Hierarchical Attribute-set-Based encyption

HASBE[1] was introduced by Zhiguo Wan in 2012. This scheme is extended from the HABE scheme and uses the CP-ASBE scheme for the encryption technique. The scheme proposes a hierarchical structure or a model and along with it allows multiple value assignments for the attributes. It uses a recursive set of attributes as the key structure. The system model consists of five components. They are the cloud service provider (CSP), a trusted root authority, domain authorities, data owner and the data users. The system model is shown in the figure 3. The CSP provides the space for data storage. The root authority is completely trusted and this authority manages the multiple domain authorities. The root authority distributes the security parameter to the domain authorities under it. The domain authorities manage the data owners and authorize the data users. The domain authorities

distribute the security parameter to the data owners and users. In this model every domain authority and users have a set of public key and master key. The user's key is linked with a recursive set of keys. The number of subsets in the key set is the depth parameter of the key. The cipher text is linked to a policy which is an access tree structure which consists of nodes where nodes are the threshold gates. And leaf nodes are values. The recursive key structure must match the tree structure only then the user can access the data. In real time cases an attribute may have two or more different values where all the values are valid. The scheme allows the data owner to combine compound attributes or apply different combinations of attributes. Because of its hierarchical structure and attribute structure it gives flexibility and proper access control to the users.

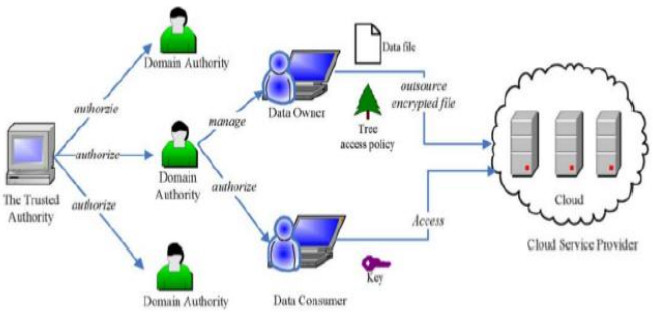

Fig. 3. HASBE system model

Access Structure : The system uses an access structure which defines the access policies. The tree structure is in the form of a tree structure where nodes represent the threshold gates and leaf nodes represent the attributes. The key structure must satisfy this access policy only then a user can decrypt the data. Thus this scheme overcomes the disadvantages of the CPABE, CP-ABSE and HABE schemes.

3. COMPARISON

In this section, we compare all the above mentioned methods. We compare the ABE, KP-ABE, CP-ABE, HABE and HASBE schemes. The ABE scheme is efficient in reducing the overhead while in this scheme, the data owner need to use each authorized users key to encrypt data which is more complex. In the KP-ABE scheme, it is used for one to many communications but it has several disadvantages that the owner of the data cannot decide who can get the encrypted data which is a drawback of this scheme. The CP-ABE scheme overcomes this drawback of KP-ABE where the data owner can define the access policies. The CP-ASBE supports multiple value assignment for attributes and compound attributes which can be used for real time applications, but is difficult to implement with a single authority. HABE Support enhanced access control over attributes. The HASBE extends the HABE scheme. The workload of the root authority is distributed to the domain authorities. So a single authority does not need to manage all the users. It provides better access control with multiple value assignments for some values but requires heavy computation overhead.

4. CONCLUSION

In this paper we conduct a study on different access control policies which are attribute based. ABE, KP-ABE, CP-ABE, HABE and HASBE schemes. We study and compare their schemes in terms of their efficiency and flexibility. These access control policies are mainly classified according to their implementation of access policies. The KP-ABE and CPABE schemes where the first implemented ABE techniques. These schemes had certain disadvantages which were overcome by the CP-ABSE scheme. Then a hierarchical model was developed from which they proposed the HASBE scheme. So this scheme had its advantages over all the other schemes. As the HASBE scheme is extended from the CP-ABE scheme its security is same to that of the CP-ABE scheme. Because of its hierarchical structure and attribute structure it gives flexibility and proper access control to the users. Out of the existing schemes, the HASBE scheme can be considered as the most efficient and can be used for real time applications.

REFERENCES

[1] Zhiguo Wan, June Liu, and Robert H. Deng,HASBE: A Hierarchical Attribute Based Solution for Flexible and Scalbale Access Control in Cloud Computing ,IEEE Transactions On Information Forensics and Security,Vol 7 , No 2, April 2012

[2] J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-policy attribute-based encryption, IEEE Transactions On Networking Vol:21 No 3 April 2007.

[3] G. Wang, Q. Liu, and J.Wu Hierarchical attribute-based encryption for fine-grained access control in cloud storage services, 2010.

[4] V. Goyal, O. Pandey, A. Sahai, and B.Waters, Attribute-based encryption for fine-grained access control of encrypted data in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Alexandria 2006.
[5] Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran, Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption July 27, 2009.
[6] Parmar Vipul Kumar J, RajaniKanth Aluvalu, Key Policy Attribute Based Encryption (KP-ABE): A Review,International Journal of Innovative and Emerging Research in Engineering Volume 2, Issue 2, 2015.