An Assessment on Attribute Based Encryption Techniques in Cloud Computing

R.Nallakumar, S.Ayyasamy, M.Nithya

Abstract— **Nowadays cloud computing is a rapidly growing technology, in which it enables users to store their data remotely in a cloud server and it provides on-demand access to a shared pool of resources in the cloud server. Sharing of data in cloud server and providing data security and privacy is a critical issue in the cloud server. In order to make data to be secure, it is necessary to implement any efficient and secure data access control method. Attribute Based Encryption is a technique which will provide data security and data access control. ABE's encryption method is based on public key with a set of user attributes and access policies associated with it [3]. In this paper, we survey various encryption schemes including ABE, KP-ABE, CP-ABE, ABE with Non-monotonic Access Structures and HABE and listed out the comparisons of the above schemes. This paper will help to determine the differences in various encryption techniques and to make future improvements among those techniques.**

Index Terms— **Attribute Based Encryption, Key policy, Cipher text policy, Access control.**

I. INTRODUCTION

The National Institute of Standards and Technology has categorized cloud computing into two types such as Service Model and a Deployment Model [1]. The Service Model contains Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).The Iaas Layer will provide the services to the consumers to utilize the hardware only. The Platform as a Service layer will provide the application environment to the consumer. The application environment will provide the libraries and software for developing the application. The top layer is Software as a Service. In this layer, consumers can utilize the applications which can be provided by the cloud providers and the consumer has no access to the infrastructure of this platform.

The Deployment Model which can be categorized into Public, Private, Community and Hybrid Cloud. Private Cloud infrastructure is provisioned for a single organization for their exclusive use. Public Cloud infrastructure is provisioned for the general public for open use [1]. Hybrid Cloud infrastructure is a combination of two or more cloud infrastructures such as private cloud or public cloud. Community Cloud infrastructure is provisioned for a specific community of users who share the data for their exclusive use.

There is a need to securely share, manage, store and analyze the data in the cloud server. It is important to maintain the clouds to be secure. The main security challenge is that the data owner may not have control to place the data in a specified location in the cloud environment [2]. There are many security issues in cloud computing, including networks, resource scheduling, databases, virtualization, load balancing etc. Data security entailed encryption of the data and guarantee that appropriate policies are inflicted for data sharing. The following are the key security challenges.

- Data Location
- Investigation
- Data Segregation
- Recovery
- Regulatory Compliance

II. LITERATURE SURVEY

A. *Attribute Based Encryption*

Attribute Based Encryption scheme was introduced by Sahai and Waters in the year 2005 and the main objective is to provide data security and data access control. In this ABE scheme, there are three types of entities, namely Authority, Data Owner (Sender) and Data User (Receiver) [5]. The role of the Authority is to generate keys for data owners and data users to encrypt or decrypt the data. The Authority generates keys based on the user attributes. In which the secret key of the user and the cipher text are depend on the attributes. The role of the Data Owners is to encrypt the data with a public key and a set of descriptive attributes.

The Data User's role is to decrypt the encrypted data based on the attributes and with the private key. The decryption is possible only if the set of attributes of the user key matches the attributes of the cipher text. In decryption, the attributes in the data user's private key will check by matching with the attributes in the encrypted data. The number of matching should reach at least a threshold value 'd'. If it reaches the threshold value 'd' then the data users private key will be permitted to decrypt the data [4]. Consider an example, for a set of descriptive attributes in the encrypted data are {Food, Trainer, Dog} and the threshold value is '2'. If the data user needs to decrypt the encrypted data, the number of attributes

Manuscript received Sep, 2014.

R.Nallakumar, Teaching Fellow*, Department of Computer Science , Anna University/ Anna University Regional Centre, Coimbatore/ India,*

S.Ayyasamy PG Scholar*, Department of Computer Science, Anna University Regional Centre, Coimbatore/ India.*

M.Nithya PG Scholar*, Department of Computer Science, Anna University/ Anna University Regional Centre, Coimbatore/ India.*

in private key should be at least two or more than two attributes in the encrypted data. So that the data user has a private key with {Food, Dog} attributes to decrypt and obtain the original data. ABE scheme has significant advantages which it achieves flexible one to many encryption and it is very useful for addressing the security problems and to address the fine grained data sharing and access control of that data.

B. Key Policy Attribute Based Encryption

Key Policy Attribute Based Encryption scheme was proposed by V. Goyal, O. Pandey, A. Sahai and B. Waters. It was introduced to overcome the limitations of ABE scheme. In this method, it uses a set of attributes to describe the encrypted data and it builds the access policies in the user's private key. If the attributes of the encrypted data can satisfy the access structure in user's private key 'D' , then the user can obtain the message content through any decryption algorithm. KP-ABE scheme is designed for one to many communications.

The KP-ABE is useful for providing fine-grained access control to the data item because it will specify that which part of the data item can be accessed by which user and what are the operations they can execute over the data item. This scheme has some of the following disadvantages here with the data owner is also a trusted authority (TA), If we will apply this scheme to a PHR system with the multiple data owner and users, it would be inefficient because each user would receive many keys from multiple owners, even if the key contain the same set of attributes.

C. Cipher text Policy Attribute Based Encryption

Cipher text Policy Attribute Based Encryption scheme was introduced by Sahai et al. It is the modified form of Attribute based Encryption (ABE) scheme. The access control method of CP-ABE scheme is similar to the KP-ABE scheme. In KP-ABE scheme, the access policy can be defined in the user's private key, whereas In CP-ABE, the access policy is defined in the encrypted data (cipher text) and the set of attributes are associated with the user's private key and the access policy is built in the cipher text [5]. If the set of attributes in the user's private key satisfies the access structure of the encrypted data, then the user can decrypt the encrypted data.

The advantages of this CP-ABE scheme are, The third party server won't have access on the plain data. Decryption is possible only when the secret key is matched up with the access policies defined in the attributes and every user is required proper authorization to access the data. Even though this scheme have the above advantages this scheme have some of the following challenges that are Difficulty in user revocation, whenever the owner wants to change the access rights of the user, it is not possible to do efficiently. Decryption keys only support user attributes that are organized logically as a single set, so users can only user all possible combinations of attributes in a single set issued in their keys to satisfy the policies.

D. Attribute Based Encryption scheme with Non-Monotonic Access Structure

ABE with non-monotonic access structure was proposed by Ostrovsky et al in the year 2007. In this scheme, the access formula for the access structure in private key can represent any type through attributes such as negative attributes. It is different from the previous attribute based encryption schemes such as KP-ABE. In KP-ABE scheme, the access structure in the user's private key has a monotonic access method. There are no negative attributes associated with it.

The access structure of this scheme will have the negative attributes associated with this scheme. It has the Boolean formula such as AND, OR and a threshold gate in the access structure of the previous schemes. In addition to that this scheme is having a Boolean formula NOT in the access structure of this scheme [5]. This is a first scheme that proposes a negative constraint to describe the attributes and it is more flexible to use access policies for a data owner. This scheme is undesirable for the below reasons. There are many negative attributes in the cipher text, but they don't relate to the cipher text. It means that each attribute adds a negative word to describe it, but these are useless for decrypting the cipher text. It can cause the encrypted data overhead and making the huge overhead. Monotonic Access Structure uses 'AND gate', 'OR gate' or 'k out of N' threshold gates. Non Monotonic Access Structure uses additional 'NOT gate'. The Fig. 1 illustrates the example for monotonic access structure and the Fig. 2 illustrates the example for non-monotonic access structure.

E. Hierarchical Attribute Based Encryption Scheme

Hierarchical Attribute Based Encryption Scheme was proposed by Wang et al in the year 2011. This scheme is a combination of Hierarchical IBE (HIBE) and CP-ABE schemes. This scheme uses the property of a hierarchical generation of keys in HIBE scheme to generate the keys and it uses Disjunctive Normal Form (DNF) to express the access control policy. This scheme consists of the five roles. Cloud storage service, data owner, root authority, domain authority, and data users.

The cloud storage service's role is that it lets a data owner to store the data and share the data with the users. The data owner is to encrypt the data and sharing of those data with the users. The root authority is used to generate the system parameters and domain keys to distribute them. The domain authority is managing the next level domain authority and all users in its domain to delegate keys for them. It can distribute secret keys to the users. The users can use their secret keys to decrypt the data to obtain the original message.

This scheme has many advantages with it can satisfy the property of fine-grained access control to the cloud by combining HIBE and CP-ABE schemes. It can share the data for users in the cloud in an enterprise environment and it can be applied to achieve the proxy re-encryption. And this scheme has some of the disadvantages with it is unsuitable to implement because all the attributes in one conjunctive clause in this scheme may be administrated by the same domain authority and the same attribute may be administrated by multiple domain authorities.Table1 represents the comparisons of the above mentioned ABE schemes.

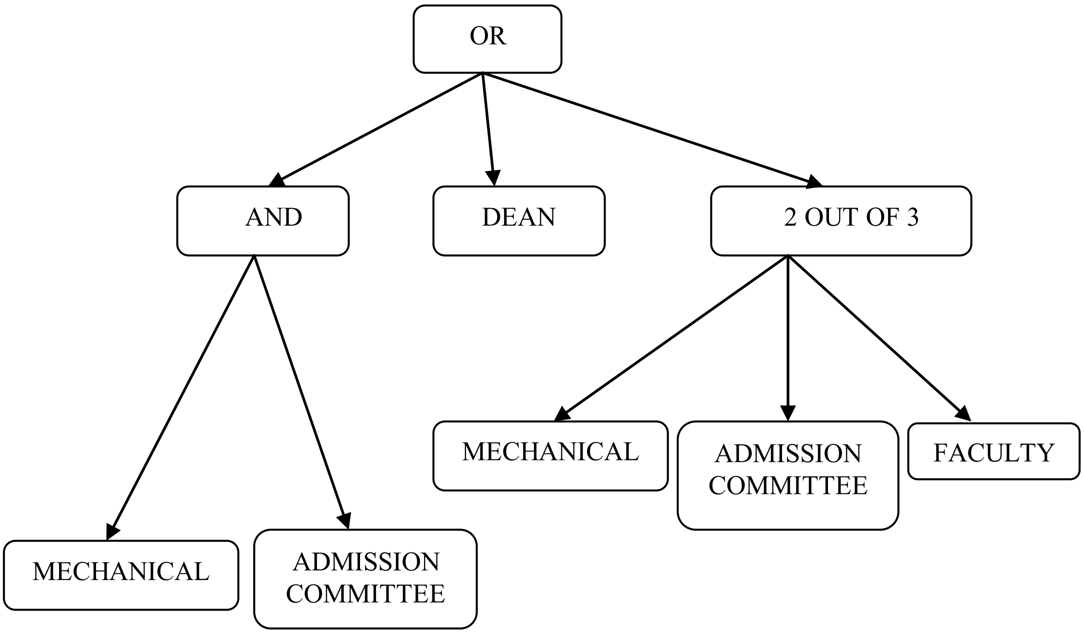

Fig.1 Example for monotonic access structure

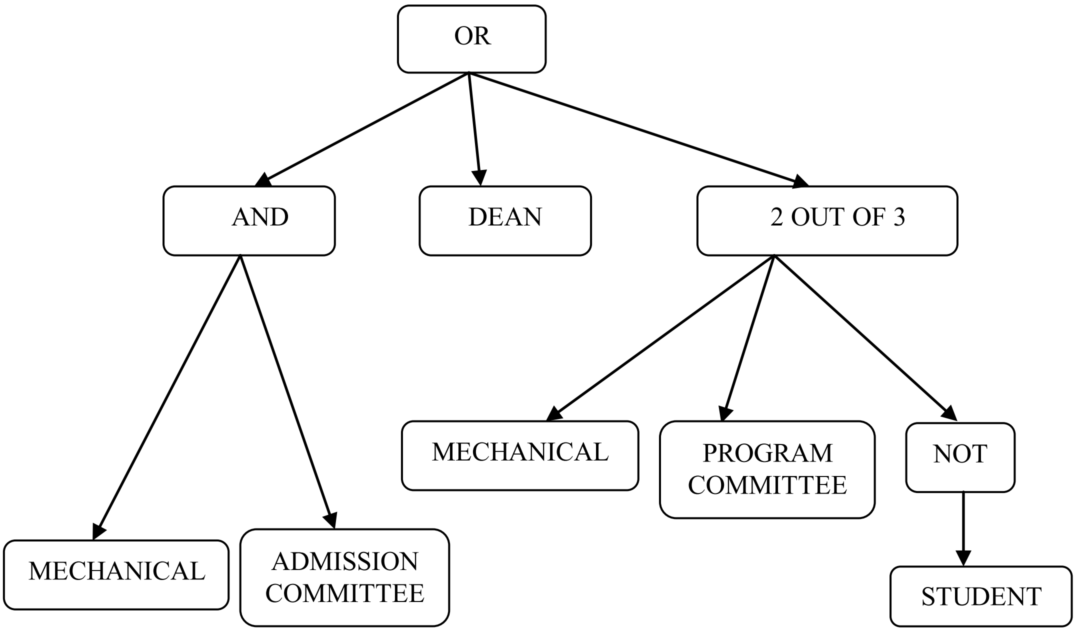

Fig.2 Example for non-monotonic access structure

COMPARISON OF VARIOUS ABE SCHEMES

Techniques/Parameter	**ABE**	**KP-ABE**	**CP- ABE**	**ABE with Non Monotonic access structure**	**HABE**
Fine grained access control	Low	Average	High	High	Good
Scalability	High	Low	Low	Low	High
Efficiency	Low	Average	High	Medium	Low
Data confidentiality	High	High	High	High	High
User accountability	Low	Low	High	Low	High
User revocation	Low	High	High	High	High
Collusion resistant	Average	High	High	High	High
Computational overhead	High	High	Average	Medium	Medium

TABLE 1 Comparison of various ABE schemes

III. Conclusion

In this paper, different Attribute based encryption schemes are analyzed. Attribute Based Encryption (ABE), Key-Police ABE, Cipher text-Policy ABE, ABE with Non-monotonic Access Structure, Hierarchical ABE, and Identity Based Encryption. Among these analyzes, this survey paper will help to determine the differences in various encryption techniques and to make future improvements among those techniques.

.

REFERENCES

[1] An Introduction To Securing a Cloud Environment (http://www.sans.org/reading-room/whitepapers/cloud/introduction-securing-cloud-environment-34052)

[2] Kevin Hamlen, Murat Kantarcioglu, Latifur Khan and Bhavani Thuraisingham "Security Issues for Cloud Computing "

[3] V. Goyal, O. Pandey, A. Sahai and B. Waters "Attribute-based encryption for fine-grained access control of encrypted data,".

[4] Minu George, Dr.C.Suresh Gnanadhas, Saranya.k "A Survey on Attribute Based Encryption Scheme in Cloud Computing"

[5] Cheng-Chi Lee, Pei-Shan Chung, and Min-Shiang Hwang "A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments"

Mr.R.Nallakumar received his B.E degree in Computer Science Engineering from S.S.M College of Engineering, Erode in 2009 and received his M.E degree in Computer Science and Engineering from Nandha Engineering College, Erode in 2011 and received his M.B.A degree in Anna University, Chennai. He is pursuing PhD in Anna University, Chennai. At present he is a Teaching Fellow in Anna University Regional Centre, Coimbatore. His area of interest is cloud computing.

Mr.S.Ayyasamy received his B.E degree in Computer Science Engineering from Erode Sengunthar Engineering College, Erode in 2008 and received his M.B.A degree in Information System Management from Bharathiyar University, Coimbatore in 2013. He is pursuing M.E Computer Science and Engineering from Anna University Regional Centre, Coimbatore. His area of interest is cloud computing, Network and Information Security, Database.

Ms.M.Nithya received her B.E degree in Computer Science Engineering from Sri Krishna College of Engineering and Technology, Coimbatore in 2013. She is pursuing M.E degree in Computer Science and Engineering from Anna University Regional Centre, Coimbatore. Her area of interest is cloud computing, Networks, Database.