ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

Attribute Based Encryption for Data Sharing in Cloud

Yesha N B, Dr Ashwini Kodipalli

B.E. Student, Dept. of ISE, New Horizon College of Engineering, Bangalore, Karnataka, India.

Assistant Professor, Dept. of ISE, New Horizon College of Engineering, Bangalore, Karnataka, India.

ABSTRACT: Cloud computing is a model that enables to get access to sharable network resources over the internet on demand. It allows the organizations to deploy and run their applications on the cloud servers over the internet. This has led to major concern over security issues in case of storing sensitive information on the cloud. To ensure the privacy and confidentiality of data there should some be access control policies.Access Control in cloud ensures the security in cloud computing by allowing the authorized users to access and unable access to those who are unauthorized. To ensure this property a cryptographic method called Attribute Based Encryption (ABE) is used. ABE is used in determining the access control and hiding the data from the cloud server. ABE is a scheme that gives access to the users based certain credentials they possess in accessing the data. In this paper Types of ABE techniques that can be used to secure your data and control access to users and how it can be used in data sharing in cloud.

KEYWORDS: Cloud computing, Attribute Based encryption (ABE), KP-ABE, CP-ABE, Data sharing, Data security.

I. INTRODUCTION

Cloud computing is one of the current IT trends that today's organizations and businesses deploy in their business. Cloud computing is a model that offers wide range of services like Platform as a service(PaaS), Infrastructure as a Service(IaaS), Software as a Service(SaaS) to their customers on demand. Large organizations are deploying cloud computing in their business and the organizations that provide cloud services are also increasing day by day. This considerable momentum hasled to major concern over security and privacy. Often the data stored on the cloud servers contain sensitive information like financial data of banks, medical records of a patient and social network[1]. Cloud computing enables customers to store these large sets of sensitive data through various cryptographic methods that ensures security[2]. There are many cryptographic methods that are developed overtime like Public-key Encryption(PKE), Identity Based Encryption(IBE), Homomorphic encryption and Attribute Based Encryption(ABE) of which ABE is the best cryptographic methods that offers high level of security.

The science of cryptography has two types of cryptosystems. The classical cryptosystem and the public-key cryptosystem. The main problem in classical cryptosystem is difficulty in key management and key distribution[2]. In public-key encryption there are two different keys for encryption and decryption which leads to computational problems. These are the major driving forces for developing Attribute Based Encryption.

Let us look at an example of an organization'sdatabase where many people have access to the data stored in database. The System administrator is to oversee and manage the database access. The database administrator can give access to any document based on certain credentials or the position/role of a person. The administrator can set the access control policies for different kinds of users who will be able to see only the files and documents that are relevant to them. In distributed setting all the data may be stored in the server, the server allows to access only those files for which they own the authorization based on the access control policy provided by the database administrator[3]. For e.g.: in a banking database not all the staff members of the bank will be authorized to access the accounting information related to the account holder of that bank. Whenever the database server is compromised then all the data in encrypted form

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

can be accessed by those who are not authorized to do so. In other words they are able to get access to those files that were restricted to them.
Attribute based encryption technique was introduced to provide the mechanism to ensure that even if the storage is compromised, loss of data will be minimal[3]. This paper discusses about the Attribute based encryption technique and its types.

II. RELATED WORK

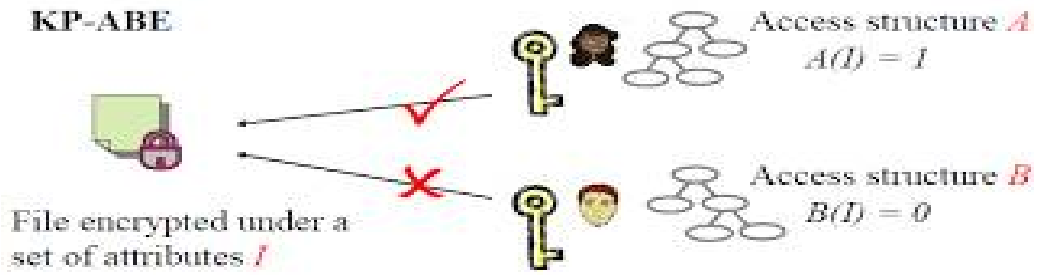
Attributed Based Encryption(ABE):ABE is one of the cryptographic primitives that is mainly used for access control in cloud.The basic Attribute based encryption scheme was proposed by Sahai and Waters in [11]. In ABE the ciphertext is induced with some set of attributes derived from the data and the secrete key given to the user to access the ciphertext is derived from these set of attributes[1]. Only if the set of attributes of the user key matches with that of the attributes induced in the ciphertext, the user will be able to decrypt the ciphertext. What ABE does is that it binds the access control policy to the data and the user instead of having the server mediating the files in the database[3].

Access Control Policy: refers to the policy that defines the kind of users who are authorized to access the data and forbidding other users who does not have proper authorization[1]. Consider an example of digitized health records stored in the cloud. The users store health records in the cloud. These records contain the fields like: name, gender, address of a patient, medical history, and hospitals visited for treatment, family history of the disease, health insurance policies etc. All this information is very sensitive and different parts of data can be accessed by different hospital personnel. For instance, management staff in the hospital should not know the medical history of the patient and only the nurses and doctors should know the details of the patient's disease, inheritance of the disease, the medicines given to the patient etc. Different fields in the records can be accessed by only certain group of people who are authorized to do so and should not be accessible by other user groups[1].

Here the different fields in the records represent the attributes and predicating itself represents the access policy as access-tree. The access of the above taken instance is quite simple but in real world the access trees are much more complex involving large number of attributes to work on.

Attribute based encryption can be classified into two types mainly Key-Policy Attribute Based Encryption(KP-ABE) and Ciphertext policy Attribute Based Encryption(CP-ABE). The difference between the two lies in whether the attributes are embedded in the ciphertext or the access policy is embedded in the ciphertext[2].

*A) Key-Policy Attribute Based Encryption(KP-ABE):*In KP-ABE, the data is encrypted by using a set of attributes and the access structure is given to the receiver as a part of the secrete key. The Key generation System(KGS) is responsible for generating the master key and issuing the secret keys to the users after authenticating the set of attributes they possess[6]. The data owner has some set of attributes and the receiver is given the secrete key with the access structure representing the attributes they have[1]. By using the attributes of sender public key is generated. This public key is used by the sender to encrypt the data and send it to the cloud. The decryption of the ciphertext is possible only if the set of attributes the user has matches with that of the attributes of the ciphertext[3]. Therefore in KP-ABE the secrete key is associated with the access policy and the ciphertext is associated with attributes[3].



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

The above figure demonstrates the KP-ABE technique, Bob is the sender, who encrypts the message using a set of attributes. It defines the access tree which is a policy that Bob wants to enforce. Alice and Tim are the users trying to decrypt the message, the access structure Tim has does not conform to the Bobs enforcement of Access policy, therefore he will not be able to decrypt the message.(B(I)=0). Whereas Alice access structure matches with the attributes of Bob(A(I)=1) allowing him to decrypt the message using the secret key[12].

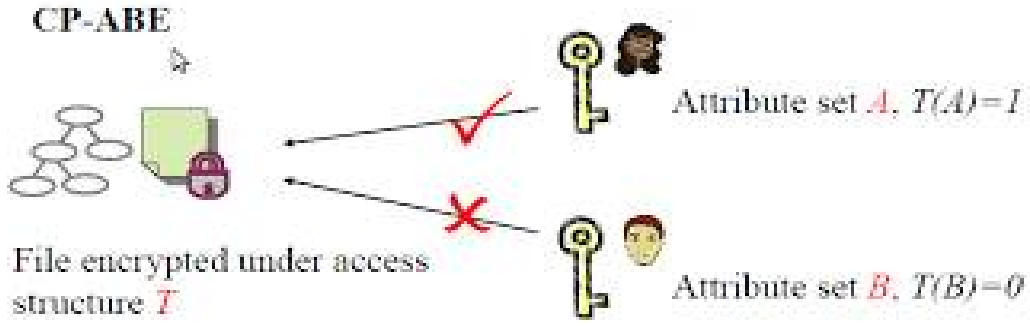
Implementation of KP-ABE:

Key-Policy Attribute Based Encryption has four phases:
Setup: The KP-ABE is a public protocol and has the same algorithm as public-key encryption. So, the public key algorithm setup(*m*) takes in the security parameters as input and output the public parameters(*PK*) and the master key*(MK).* The security parameters are chosen by key distribution center. The threshold t is decided where t represents the least number of attributes that must match the sender's ciphertext in order to decrypt it.

Key Generation: Let *Ss* and*Sr* be the set of attributes of sender and receiver respectively. The key generation algorithm Keygen*(MK,PK,Sr)* takes in the master key value*(MK),* public parameters*(PK)* and the attribute set of the receiver(A) as the input and outputs the receiver's secret key which confirms the users possession of the attribute set (A) and no other external attributes.

Encryption: The sender*(Us)* uses the encryption algorithm Encr*(PK,M,Ss)* which takes public parameters*(PK),*Message(M), the attribute set of the sender Ss as input andoutputs the Ciphertext*(CT).* In other words we can say that the attributes *Ss* are embedded into the ciphertext such that only the users having the access structure that represent the set of attributes given by the sender Us will be able to decrypt and receive the message. *Decryption:*the decryption algorithm Decr*(PK,CT, SK)* takes as input the Ciphertext*(CT),* public parameters*(PK)* and secret key(SK) and outputs the decrypted message only if the access structure representing the attribute set in the secrete key matches with that of the attribute set of the sender.

B) Ciphertext Policy Attribute Based Encryption(CP-ABE): In CP-ABE, the data is encrypted under access structure which is constructed using the policy[5]. The Key Generation System(KGS) just issues the private keys for the users according to the attributes they have. If the users satisfy the access structure they data owner defined then they will be able to decrypt it. is given to the receiver as a part of the secrete key[12]. Therefore in CP-ABE the access policy is associated with set of attributes and the access structure is associated with the Ciphertext[4].



The above figure demonstrates the CP-ABE technique, Bob is the sender, who encrypts the message using the access structure which is constructed using the access policy. It defines the access tree which is a policy that Bob wants to enforce. Alice and Tim are the users trying to decrypt the message, the attributes Tim conform to the Bobs enforcement of Access structure, therefore he will be able to decrypt the message.(T(A)=1). Whereas Alice attributes does not conform toaccess structure of Bob(T(B)=0) not allowing him to decrypt the message using the secret key[12].

Implementation of CP-ABE :

*Setup:*The public key algorithm Setup(*m*) takes in security parameters as input and gives the outputs a set of public parameters *(PK)* and the master key values *(MK).* The security parameters are chosen by key distribution center. The

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

threshold t is decided where t represents the least number of attributes that must match the sender's ciphertext in order to decrypt it.

Key Generation: Let*Ss* and *Sr* be the set of attributes of sender and receiver respectively. The key generation algorithm Keygen*(MK, PK, Sr)* takes in the master key value*(MK),* public parameters*(PK)* and the attribute set of the receiver(A) as the input and outputs the receiver's secret key which confirms the users possession of the attribute set (*A*) and no other external attributes

Encryption: the sender x uses algorithm Encr*(M, T, PK)* which takes in the message to be encrypted *(M),* the access structure T and the public parameters*(PK)* and outputs the ciphertext *CT.*The ciphertext CT embeds the access structure and if the attributes that the user has conform to the access structure then they will be able to decrypt and receive the message.

*Decryption:*The decryption algorithm Decr*(CT, SK, PK)* takes as input the ciphertext *CT*, the public parameters *PK*, the secrete key and it outputs the encrypted message *(M)* if and only if the attributes embedded in *SK* satisfy the access structure T which was used while encrypting the ciphertext *CT.*

Problem with Existing CP-ABE system

Problem statement: The data stored in the cloud may get into the hands of unauthorized users and malicious attacks by hackers[9]. At this point your sensitive data is at risk. The data owner encrypts the data and saves it in the cloud. The cloud server sometimes replaces the delegated ciphertext and may result in malicious intent. The eligible users may sometimes be responded that they are ineligible for decrypting the data[8]. There is also much complexity involved in access policy. The existing system also leads to key escrow problems[10]. The technical problem is largely structural since only the intended recipient and at least one third partiescan get access to the protected information. The third party will be permitted access only under controlled conditions which is very difficult to achieve[10].

*Proposed system:*By introducing the concept of attribute with weight, we can enhance the expression of attributes which provides more flexibility in terms of access policy. An improved two-party key issuing protocol guarantee that the key generation authority as well as the cloud service provider cannot compromise the whole secrete key of the user individually. This was introduced to resolve the problem of key escrow problem. This way the security and privacy is achieved by protecting the data from unauthorized users, the key generation authority, the cloud service provider and from malicious attacks.

Advantages of proposed system:

1. Key-escrow problem can be resolved.
2. Protecting the data from key generation authority and the cloud service provider so that the overhead involved in eligible users decrypting the data is reduced.

III. CONCLUSION

In this paper we presented some of the problems in access control and discussed different techniques of ABE used to solve this problem[1]. Considering the heavy computation overhead while encryption and decryption of the data in the cloud appropriate ABE scheme should be designed which reduces the cost incurred[1]. Various dimensions in ABE is under progress which includes ABE with hidden access policy, comparison based encryption and temporal encryption gives an interesting direction to work[2]. Another type of encryption technique named multi authority ABE ensures more security in cloud where critical data is stored. Encryption and decryption of data in cloud using multi-authority ABE is easier when compared to CP-ABE and KP-ABE. But CP-ABE as well as KP-ABE has their own significance in securing the data. In future scope many enterprises could implement the proposed encryption techniques to secure their data and do computations to scale up their businesses[4].

REFERENCES

1. SushmitaRuj, 'Attribute Based Access Control in Clouds: A Survey', IEEE, 2014.
2. R.Manjusha, R.Ramachandran, 'Comparative Study of Attribute Based Encryption Techniques in Cloud Computing', International Conference on Embedded Systems, 2014.
3. SubhashiniVenugopalan, 'Efficient Multi-level Threshold Attribute Based Encryption', ABE scheme.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 3, March 2017

4. ChaudhariSwapnil H, Mandre B.R, 'Secure Data Retrieval based on Attribute-based Encryption in Cloud', International Journal of Computer Applications(IJCA), Vol. 134, No.13, pp. 31-35, Jan 2013.
5. Mr. Anup R. Nimje, Prof. V. T. Gaikwad, Prof. H. N. Datir, 'Attribute-Based Encryption Techniques in Cloud Computing Security : An Overview' , International Journal of Computer Trends and Technology(IJCTT), Vol. 4, No.3, pp. 419-423, 2013.
6. ParmarVipul Kumar, RajaniKanthAluvalu, 'Key Policy Attribute Based Encryption (KP-ABE): A Review', International Journal of Innovation and Emerging Research in Engineering (IJIERE), Vol. 2, No. 2, pp. 49-52, 2015.
7. Cheng-Chi Lee, Pei-Shan Chung, Min-Shiang Hwang, 'A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments', International Journal of Network Security (IJNS), Vol. 15, No. 4, pp. 231-240, July 2013.
8. Deepika.P.Pachpute, Prof.Vina M. Lomte, 'Cipher Text-Policy Attribute-Based Encryption in Cloud Computing for Data Sharing' International Journal of Innovative Research in Computer and Communication Engineering(IJIRCCE) , Vol. 4, No.12, pp. 21233-21235, December 2016.
9. AbhaPandit,AishwaryaLamture, PoojaSankpal, Shubham Dixit, TabassumMaktum, 'Attribute-Based Encryption with Verifiable Outsourced Decryption' , International Journal of Tecchnical and Research Application(IJTRA),Special Issue 41, pp. 57-61, March 2016.
10. https://en.wikipedia.org/wiki/Key_escrow, 25 June 2016.
11. https://en.wikipedia.org/wiki/Attribute-based_encryption, 20 February 2017.
12. http://mohamednabeel.blogspot.in/2012/03/aattribute-based-encryption-abe-and-its.html, 14 March 2012.