A Review of Attribute based Encryption Technique for Security in Cloud Computing

Etti Mathur
M.Tech Scholar,
Department of CSE,
Maharishi Arvind College of
Engineering and Research Center,
Jaipur

Manish Sharma
Head of Department,
Department of Computer Science,
Maharishi Arvind College of
Engineering & Research Center,
Jaipur

ABSTRACT
Cloud Computing is a talented model which based on cloud services and cloud providers. Cloud computing allows user to slightly store their data in server side. Cloud computing provides services which provides services on demand and anywhere. In data storage data security and privacy are the critical issues which provide data confidentiality and access control. Attribute based encryption is a prominent technique to which provides security and privacy in cloud computing environment. Data is encrypted and managed by data owner which eliminates data replication in cloud environment. In ABE there are many properties for encryption data which generates public key and used to control access to the user. In this survey we used access structures which are monotonic and non-monotonic etc.ABE techniques are analyzed for the cloud computing environment. In this paper we review the various scheme for encryption and finally we made a comparison by taking some criteria in the respect of cloud computing.

Keywords
Cloud Computing, Attribute based encryption, Security, Key policy, cipher text policy, hierarchical-ASBE.

1. INTRODUCTION
Cloud computing is a combination of grid computing and distributing computing. Cloud computing provides many services related to IT sector and business area. Cloud computing depend upon the sharing of resources and other personal services which connected through a network. Basically cloud computing is "ON-DEMAND" computing which provided any services at any time. In the storage service application, the cloud can let the user, data owner, stores and shares these data with other users for the cloud environment [6].

Cloud computing provides major issues i.e. integrity, authorization, performance, accessibility, confidentially and Cloud computing is a part of "VIRTUALIZATION", which provides safeguard on data. There are many deployment models and cloud services which is provided by the cloud provider. In cloud environment data must be secured and confidential, so for that we can use Attribute Based Encryption (ABE) [5].

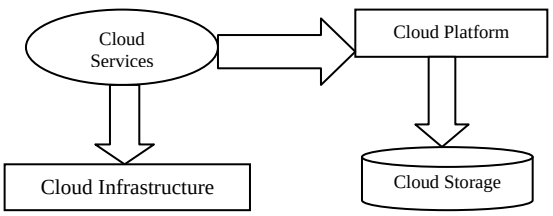

Fig.1 Model Diagram of Cloud Computing

Data storage provider provides services which based on on-demand. Providers are giving the resources for organizations anywhere. The data vendor needs to make a flexible and scalable access control and rules are authenticate and right to use, so that only the authorized person can access the cloud data. The main phases are to provide flexibility, scalability and fine grained access control [3].The infrastructure of cloud computing consists of data centers and data centers are controlled and managed by the data providers. One of the major advantages of the cloud is its probable for real time performance data and on demand transparency [4].

In ABE scheme both the user secret key and the cipher text are correlated with a set of attributes. The subsisting ABE schemes are of two types that is Key-Policy ABE (KP-ABE) scheme and Cipher text Policy ABE (CP-ABE) scheme [3]. In this concept, data or message is encrypted by the user's using the attributes and to assured the access structure which o those users can only decrypt the message. Cloud is a part of Virtualization. The confidentiality, accessibility, security, privacy, performance, integrity are the major concerns for cloud. Encryption is the way to secure the data in the untrusted cloud server. In ABE schemes access structure can be divided into parts i.e. monotonic and non-monotonic.

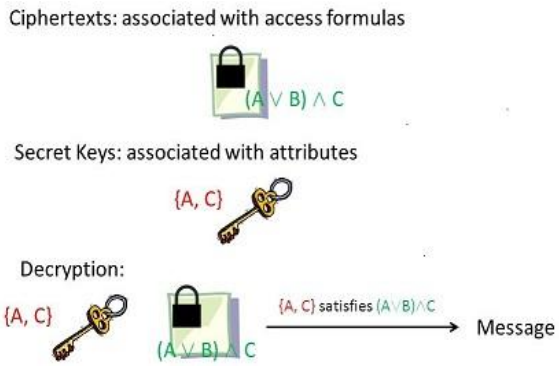

Fig.2 Model for Security using Encryption

2. LITERATURE REVIEW
A. Attribute- based Encryption Scheme
In the encryption process all the sensitive data are encrypted and to avoid the unauthorized user access of the cloud for cloud environment. A user decryption key is relevant with a monotonic access structure. Data security, data confidentiality and access control are provided by the different schemes. Security of cloud data supplies in the encryption scheme. Attribute based encryption is the one of the encryption scheme which depends on authorized person, sender and receiver. There are authority, sender and receiver in this scheme, and authority's role is to generate keys for data owners and users to encrypt or decrypt data [6]. According to attributes the authority generates keys and approved by authority. A data receiver to decrypt encrypted data with private key sent from the authority [3].During Public Key

Cryptography does access control to the user in ABE. The user secret key and the cipher text both are combined with a set of attributes. In ABE scheme every authorized user's public key to encrypt data and private key to decrypts data [1].

B. Key Policy Attribute-Based Encryption

Encrypted , that is who encrypts the data, is companion with the set of attributes to the data or message by encrypting it with a public key. Users are assigned with an access tree structure over the data attributes. Key Policy Attributes scheme designed for one to many communications. In this, the data is defined as a public key, each of which is associated with the characteristics. Key-policy attribute-based encryption (KP-ABE) is imperative class of ABE, where cipher texts are identified with sets of attributes and using the private key to decrypt the structures that enable a user to control the cipher texts are associated with access structure.Each file or message, a symmetric data encryption key (DEK), which re-ABE in KP corresponding to a set of attributes that is encrypted with a public key[1].It allows a data owner to reduce most of the computational upstairs to the servers.ABE scheme, attribute policies are associated with keys and data is associated with attributes. The keys have the same policy that has properties that can decrypt the data are added to the data associated with to be satisfied. Each file or message is encrypted with a symmetric data encryption key (DEK), which is again encrypted by a public key[3].Finally, KB-ABE encrypted data which satisfies the access control structure of an user private key and then user can also get the messages[6].

C. Expressive Key Policy Attribute Based Encryption

Access tree structure is used to decrypt the cipher text with the Key holder. Expressive key-based encryption policy (KP-ABE) based on non-monotonic access structures. Access non-monotonic tree structures in those key-based encryption policy properties negated attributes with continuous cipher-text and can include size [3].Primitive characteristics and enables senders private key to encrypt the message with a set of tree structure which is associated with the use of the key holder to decrypt the cipher text specifies allowed [1].

D. Cipher text Policy Attribute Based Encryption

In CP-ABE plan, policies are associated with the data attributes and key. These policies are able to decrypt content data with the key holder. CP- ABE, each user is associated with a set of attributes. The secret key is generated on the basis of its features [3].In Cipher text-based encryption policy identity-based encryption feature can be seen as a generalization. Identity-based encryption associated with public key and a private key which can be used to create private key restricts.CP- Abe, a cipher text access structure tree is associated with a monotonic and decryption of a user is associated with a set of key features [1]. Basically cloud environment can support access control and secrecy. In addition, a set of attributes in the user's private key is a combination of the scheme, so a user only use this set of properties to meet the encrypted data access structure[2].

E. Cipher text Policy Attribute-Set Based Encryption

A system is defined to recognize complex access control on encrypted data through Cipher text Attribute Set Based Encryption (CP-ASBE). The technique makes sure that encrypted data are kept confidential even if the provider is not credible .In CP-ASBE holds multiple value assignments for an attribute which encrypted by a single key [4].

F. Identity Based Encryption and Hierarchical Identity Based Encryption

The identity-based encryption scheme, such as data and decryption key is encrypted using an arbitrary string. A leading authority arbitrarily by the decryption key is mapped to the encryption key. Hierarchical identity-based encryption (HIBE) to a single IBE is categorically [3].

G. Hierarchical Attribute Based Encryption

The plan assets used HIBE hierarchical scheme to generate keys for key generation. Cloud computing system has five types of parties i.e. a cloud service provider, data owners, data consumers, domain number and a trusted authority [2]. In cloud environment the cloud management and data storage service provides by the providers. Data encrypt your data files and data owners to share with the consumer to store them in the cloud offers.

H. Hierarchical Attribute Set- Based Encryption

The HASBE scheme extends the ASBE scheme to handle the hierarchical structure of system as shown in figure-1.

HASBE planning algorithm using a delegation consists of the hierarchical structure of system users. HASBE compound flexible feature set due to a combination of features as well as many of the characteristics values assigned achieve efficient trusted user support repeal.

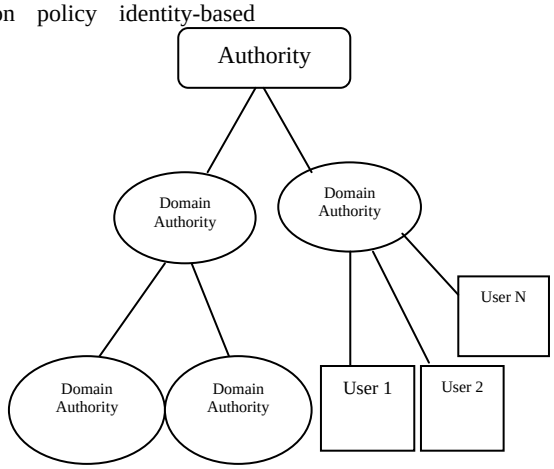

Fig.3: Hierarchical Structure

3. COMPARISON ANALYSIS

After the review of various attribute based techniques, we showed a comparison in the below table on the basis of different parameters. This table is clearly indicate the behavior of different techniques on different parameters and provide a review that which technique is more efficient.

Techniques/ Parameters	ABE	KP-ABE	EKP-ABE	CP-ABE	CP-ASBE	HIBE	HABE	HASBE
Access Control	Low	Low.High if there is reencryption techniqe	Better Access control than that of KP-ABE	Average Realization of complex Access Control	Better Access Control than that of CP-ABE	Lower than CP-ASBE	Good Access control	Better Access control
Efficiency	Average	Average, High for Broadcast type system	Higher than KP-ABE, allows constant cipher text only	Average Not efficient for modern enterprise environments	Better than CP-ABE as there is Less collusion attacks	Better, Lower as compared to ABE schemes	Flexible and scalable	Most efficient and flexible
Computation Overhead	High	Most of computational overheads	Reduces computational overheads	Average computational overheads	Lower than CP-ABE computational overheads	Most computational overheads	Some of overhead	Less overhead than others
Collusion Resistant	Average	Good	Good	Good	Good	Good	Good	High
Scalability	Good	Poor	Poor	Poor	Good	Good	Good	Good
Reliability	Good	Poor	Poor	Poor	Good	Good	Good	Good
Access Structure	Monotonic	Monotonic	Non-Monotonic	Monotonic	Monolithic	Hierarchical	Hierarchical	Hierarchical

4. CONCLUSION AND FUTURE SCOPE

In this paper we have overviewed different attributes based encryption (ABE) schemes that can be used in cloud systems for providing effective security. Many encryption schemes like KP-ABE, EKP-ABE, CP-ABE, H-ABE, HI-ABE are discussed by taking various parameters and finally we conclude that all the algorithms are strong and efficient on different domain. In Attribute based encryption attributes are associated with two things which is "secret key" and "cipher text". Both are important concepts in the term of providing the security in cloud using encryption. On the basis of comparison table, conclude that HBASE are the most scalable, efficient and secure algorithm than any other scheme to provide security in cloud computing.

As a future work, we now focus on in-depth analysis to make a secure algorithm which is much effective and efficient in terms of securing the cloud data with compare to other algorithms.

5. REFERENCES

[1] Dr. Ananthi Sheshasaayee, and K. Geetha B. Waters, "An Efficient Presentation of Attribute Based Encryption Design in Cloud Data", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 5, Issue 2, February 2015.

[2] Minu George, Dr. C.Suresh Gnanadhas, Saranya.K, "A Survey on Attribute Based Encryption Scheme in Cloud Computing", International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 11, November 2013.

[3] 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- volume4 ,Issue3- 2013.

[4] Surya Prabha.U.S, Marikkannu.P, Arul Vineeth.A.D , "Cipher text Policy Attribute Set Based Encryption with One-Fold Data Access in Cloud," International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970) Volume-4 Number-1 Issue-14 March-2014

[5] Saravana Kumar Na,Rajya Lakshmi G.Vb ,Balamurugan Ba , "Enhanced Attribute Based Encryption for Cloud Computing," International Conference on Information and Communication Technologies (ICICT 2014)

[6] M. D. Dikaiakos, D. Katsaros, P. Mehra, G. Pallis, and Athena Vakali, Cloud computing: Distributed internet computing for it and scienti¯c research," *IEEE Internet Computing*, vol. 13, pp. 10 {13, 2009.

[7] Jin Sun, Yupu Hu, Leyou Zhang," A Key-policy Attribute-Based Broadcast Encryption," The International Arab Journal of Information Technology, vol.10, No.5, September 2013.