A Survey and Comparison of Different Attribute Based Encryption and Access Control Technique and Their Issues in Cloud Computing Security

Omkar Dicholkar[1], Prof. Varsha Bhosale [2]

[1]*M.Tech Scholar. Vidyalankar Instotute of Technology*

[2] *Vice Principal and Associate Professor of Vidyalankar Institute of Technology, Mumbai*

ABSTRACT - Cloud computing is an emerging computing paradigm, enabling users to remotely store their data in a server and provide services on-demand. But the data security and privacy are the critical issues in the cloud computing. So it becomes very necessary to secure the data as well as privacy of users. A secure user enforced data access control mechanism must be provided for the cloud users for having the liberty to outsource sensitive data from the cloud storage. It is imperative to adopt an efficient encryption system with a fine-grained access control to encrypt outsourced data. In such scenario the Attribute based encryption is a prominent technique which provides security and privacy in cloud computing environment. Attribute is a way of public key encryption in which the secret key of the user and the cipher text are dependent. The decryption of a cipher text is only the set of attributes of the user key matching the attributes of the cipher text. There are so many encryption schemes that provide security and access control in cloud security. In this paper, we are going to explore various schemes for encryption that consist of Attribute based encryption (ABE) and its types KP-ABE, CP-ABE. Further discussion consists of improvement in CP-ABE to CP-ASBE and to HASBE. A comparison table has been included for comparative study of these techniques.

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

I. INTRODUCTION

Evolution of computer can considered as mainframes to personal computers, personal computers to mobile computing and mobile computing to cloud computing. Mainframes were one computer for many users, personal computers were single computer for single users, mobile computing is many users to one computer but cloud computing refers to many computers to one user.The Cloud computing is model on which organization and individuals can work with the application from anywhere in the world on demand and Internet is the basic requirement of Cloud Computing. So we can say cloud computing as an internet based computing model. It will provide pay-per-use services as per user demand and increased scalability while providing services at different abstraction levels, namely Software-as-a-Service (SaaS), Platform-as-a-Service (PaaS), and Infrastructure-as-a-Service (IaaS).

Cloud resources are shared among multiple users and organizations as it supports multitenancy. So there is need to defend the security of the user data from unauthorized access.

Access Control models will ensure that only users with access privileges can access the data file. Access control is a simple policy that allows, denies or restricts access to a system [1]. Data access control is an effective way to ensure the data security in the cloud. However, the cloud storage service separates the roles of the data owner from the data service provider, and the data owner does not interact with the user directly for providing data access service.

II. LITERATUREREVIEW

A. *Attribute- based EncryptionScheme*

Recently, attribute based encryption (ABE) has been attracted much more attention because it uses most prominent technique to provide the security and access control in cloud computing environment. An attribute based encryption was introduced by Sahai and waters in 2005. The attribute based encryption enforces the data access control through the public key cryptography with one to many encryption in which cipher-texts are not encrypted to one particular user, it may be for more than one numbers of the users.

In ABE scheme, attributes are playing the very important role as attributes are used as an access policy to control the users' access. In ABE scheme both the user secret key and the cipher-text are associated with a set of attributes. In the Attribute based encryption, all the sensitive and confidential data are encrypted while uploading them onto the cloud to avoid the unauthorized user access in the cloud and provides the security, privacy and access control.In A user can decrypt the ciphertext only if the set of attributes of the user's secret key matches the attributes of the ciphertext. ABE schemes usually consist of four fundamentals of the algorithms which are the Setup, Encryption, Decryption, Key generation.

1. Setup: (K, U) -> (PP, MSK): It takes a security parameter K as input and returns a public key (PP) and system master secret key (MSK). The PP is used by message senders for encryption and MSK is used to generate user secret key.
2. Key Generation: (K,PP,MSK,S)->SK: It takes the public parameter PP, master secret key MSK , set of attributes S as inputs and outputs the decryption key SK that enables the user to decrypt a message which is encrypted under the access tree structure T if and only if it matches T.
3. Encryption: (K, PP, M, T) -> CT: It is performed by a sender to encrypt a message M, with help of the public parameter PP, a set of attributes S, an access structure T and produces the output of ciphertext CT.
4. Decryption: (K, PP, SK, CT) -> M: It takes the ciphertext CT and secret key SK as input for an

attribute set and returns the original message M if and only if satisfies the access structure associated with the ciphertext CT.

Advantage:

1. It provides more flexibility than ABE schemes and similar to fine-grained access control.
2. Less communication overhead than other non-ABE schemes.
3. First scheme which has collusion-resistance mechanism.
4. Monotonic attributes are used for controlling user access.

Disadvantage:

1. Not suitable for the real environment.
2. In encryption of data required all authorized user's public key.
3. If the Key generator fails system fails.
4. Its threshold semantics lacks expressibility.

The existing ABE schemes are of two types. They are Key-Policy ABE (KP-ABE) scheme and Ciphertext-Policy ABE (CP-ABE) scheme. That can be discussed further.

B. Key Policy Attribute-BasedEncryption

V. Goyal, O. Pandey, A. Sahai, and B. Waters [2] proposed a key-policy attribute-based encryption (KP-ABE) scheme which is the modified and improved version of ABE model to enable more general access control.

In the KP-ABE scheme, the attribute policies are associated with keys and data is associated with attributes. The encrypter can encrypt the data, only if it is associated with the set of attributes. In KP-ABE, the secret key of the user is defined to reflect the access tree structure. Hence, so the user can decrypt the encrypted data, only if the attributes of encrypted data is satisfy the access tree structure.

KP-ABE is suitable for structured organizations with rule about who may read particular documents.KP-ABE prevents any unauthorized users from accessing of data, even if the data were stores data in an untrusted server.

KP-ABE scheme consists of the following four algorithms:

1. Setup: This algorithm takes as input a security parameter and returns the public key PK and a system master secret key MK. PK is used by message senders for encryption. MK is used to generate user secret keys and is known only to the authority.
2. Encryption: This algorithm takes a message M, the public key PK, and a set of attributes as input. It outputs the ciphertext E.
3. Key Generation: This algorithm takes as input an access structure T and the master secret key MK. It outputs a secret key SK that enables the user to decrypt a message encrypted under a set of attributes if and only if matches T.
4. Decryption: It takes as input the user's secret key SK for access structure T and the ciphertext E, which was encrypted under the attribute set . This algorithm outputs the message M if and only if the attribute set satisfies the user's access structure.

Advantage

1. It's a fine-grained access control.
2. More control over users provide key revocation.
3. It is used for one-to-many communications.
4. Based on Linear Secret Sharing Schemes (LSSS) and monotone access formula.

Disadvantage

1. Trust issue on the key issuer is a measure problem in KP-ABE.
2. Not suitable in a federated model because of trust issue.
3. No control on who can decrypt data.

C. Expressive Key Policy Attribute BasedEncryption

The KP-ABE enables senders to encrypt messages with a set of attributes and private keys which are associated with access tree structure that specifies which all the ciphertext's the key holders are allowed to decrypt [5].

Expressive key-policy attribute-based encryption (KP- ABE) schemes is proposed for non-monotonic access structures which are the access tree structures that contain the negated attributes and with constant size of the cipher-text.

1. Setup (d): In the basic construction, a parameter d specifies how many attributes every ciphertext has.
2. Encryption (M, γ,PK): To encrypt a message M ε GT under a set of d attributes γ C Zp, choose a random value s ε Zp and output the ciphertext E.
3. Key Generation (˜A, MK, PK): This algorithm outputs a key D that enables the user to decrypt an encrypted message only if the attributes of that ciphertext satisfy the access structure A
4. Decrypt (C, D): Input the encrypted data CT and private key D, if the access structure is satisfied it generate the original message M

Advantage

1. The owner of data can add excluded attributes in encrypted data.
2. It's non-monotonic access structure with negated attributes.

Disadvantage

1. In this encrypted data contain many not related attributes (useless attributes) but is exists in the encrypted data.

More computational overhead in encryption of data. This expressive key-policy attribute-based encryption (KP-ABE) schemes allowing for non-monotonic access structures that may contain negated attributes and fixed constant size ciphertext [5].

D. Cipher text Policy Attribute BasedEncryption

CP-ABE scheme is the Another form of ABE scheme. In CP-ABE [7] each user is associated with the set of attributes and private key of the user is generated based on these attributes.

The CP-ABE encrypts an access policy that specifies which the private keys will be able to decrypt the ciphertext. When encrypting a message M, the encryptor specifies an access structure which is presented in terms of set of selected attributes for M. so that the message is the encrypted based on the access structure in the such way that those attributes satisfy this access structure can decrypt the message. CP-ABE scheme consists of following four algorithms:

1. Setup: This algorithm takes as input a security parameter κ and returns the public key PK as well as a system master secret key MK. PK is used by message senders for encryption. MK is used to generate user secret keys and is known only to the authority.
2. Encrypt: This algorithm takes as input the public parameter PK, a message M, and an access structure T. It outputs the ciphertext CT.
3. Key-Gen: This algorithm takes as input a set of attributes associated with the user and the master secret key MK. It outputs a secret key SK that enables the user to decrypt a message encrypted under an access tree structure T if and only if matches T.
4. Decrypt: This algorithm takes as input the ciphertext CT and a secret key SK for an attributes set . It returns the message M if and only if satisfies the access structure associated with the ciphertext CT

Advantage

1. This scheme overcomes a disadvantage of KP-ABE.
2. A reverse version of the KP-ABE.
3. Used store data on the un-trusted.
4. It's suitable for some the real environment applications.
5. It has more complex access control model access control model, based on RBAC schemes.
6. It has control over who can decrypt data method.

Disadvantage

1. The combination of attributes can bypass the access policy.
2. The CA has all the authorities which can be misused.
3. Not satisfying the enterprise prerequisites.
4. Lack of adaptability and proficiency.
5. User who wants to decrypt data can rearrange attributes to satisfy access policy.

E. Cipher text Policy Attribute-Set BasedEncryption

The Ciphertext policy attribute set based encryption (CP-ASBE) is introduced by Bobba, Waters et al [6]. The CP-ASBE consists of recursive set of attributes. The Ciphertext Policy Attribute Set Based Encryption (CP-ASBE) is a modified form of CP-ABE. It organizes user attributes into a recursive set based structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. The desirable feature and the recursive key structure is implemented by four algorithms - Setup, KeyGen, Encrypt, and Decrypt.

1. Setup: Here is the depth of key structure. Take as input a depth parameter 'd'. It outputs a public key PK and master secret key MK.
2. Key-gen: Takes as input the master secret key MK, the identity of user u, and a key structure A . It outputs a secret key SK for user u.
3. Encrypt: Takes as input the public key PK, a message M, and an access tree T . It outputs a ciphertext CT.
4. Decrypt: Take as input a ciphertext CT and a secret key SK for user u. It outputs a message m . If the key structure A associated with the secret key SK, satisfies the access tree T, associated with the ciphertext CT, then m is the original correct message M.

Advantage

1. User's access structure based a monolithic set of user attributes for the
2. private key.
3. It's support enterprise need of a set of related attributes with various differential values for each attribute.
4. No attribute collision.
5. The owner of data can add excluded attributes in encrypted data.
6. It's non-monotonic access structure.

Disadvantage

1. Making composite attributes for a user's key is a
2. practical difficulty.
3. Avoiding collision of attributes is very difficult in this scheme.
4. In this encrypted data contain many not related attributes (useless attributes) but is exists in the encrypted data.
5. More computational overhead, in encryption of data.

F. Hierarchical Identity Based Encryption

Traditionally public key cryptography is used to maintain confidentiality and Authentication. But it is Difficult to associate user with its genuine public key. So Public Key Infrastructure (PKI) has been used which consist of certificate authority (CA) that provides assurance about originality of Public key through digitally signed certificates. But PKI Comes with overhead of generation of certificate request message, certificate verification.

But the identity based encryption (IBE) doesn't require the certificates unlike PKI. The concept of identity based encryption(IBE) was first introduced by Shamir in 1984.Three main components involved in IBE are Sender which encrypts the message with public key of the receiver, Receiver which Decrypts the message with its private key with help of master private key and Key Generator which maintains the pair of master public/Private keys. But main drawback of the IBE is that it gives the separate public key to each user, so each time encryption is done with specific public key of that identity.

The advantage of using HIBE [10] over IBE is that keys can be generated for vector of identities. So Message can be reached to more than one identity, only one Encryption key is required in this case as well as only one time Encryption is needed. So there is saving of encryption time as well as time to compute keys. HIBE provides more functionalities than IBE by using more than one private key generator. Hierarchical Identity Based Encryption (HIBE) is the hierarchical form of identity based encryption [3]. The HABE scheme is defined by following algorithm: The desirable feature and the recursive key structure is implemented by four algorithms, Setup, KeyGen, Encrypt, and Decrypt.

1. Setup: Here is the depth of key structure. Take as input Security Parameter 'λ'. It outputs a public key PK and master secret key MK.
2. Key-gen: Takes as input the master secret key MK and an identity vector 'I'. It outputs a a private key SK.
3. Delegate: It takes an input a secret key for the identity vector _I of depth d and an identity I and outputs a secret key for the depth d+1 identity vector _I : I formed by concatenating I onto the end of _I
4. Encrypt: Takes as input public parameters PK, a message M, and an identity vector _I and outputs a ciphertext CT.
5. Decrypt: Take as input a public parameters PK, ciphertext CT and a secret key SK. It outputs a message m.

one level HIBE (1-HIBE) scheme, there is only one private key generator (PKG) that distributes private keys to each users, having public keys are their primitive ID (PID) arbitrary strings.A two-level HIBE (2-HIBE) scheme consists of a root PKG, domain PKGs and users, all of which are associated with PID's. A user's public key consists of their PID and their domain's PID (in combine, called an address) .

Advantage

1. Combining the features of ABE and Hierarchical Identity-Based Encryption (HIBE).
2. Support Multiple Authorities.
3. It is more scalable and provides fine-grained access.
4. Generation of keys uses a hierarchical structure.

Disadvantage

1. All attributes in one conjunctive clause which makes difficult to implement.
2. Difficult to manage Multiple Authorities in the system.
3. The computational overhead increase with an increase in authorities.
4.

G. Hierarchical Attribute BasedEncryption

The cloud computing system consists of five types of parties: a cloud service provider, data owners, data consumers, a number of

domain authorities, and a trusted authority. The cloud service provider manages a cloud and provides data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. Each data owner/consumer is administrated by a domain authority. A domain authority is managed by its parent domain authority or the trusted authority. This is the concept of Hierarchical attribute based encryption (HABE) in the cloud security.

This scheme Hierarchical attribute-based encryption (HABE) is derived by Wang et al [10].The HABE model consists of a Root Master (RM) that corresponds to the Third Trusted Party (TTP), Multiple Domain Masters (DMs) in which the top-level DMs correspond to multiple enterprise users, and numerous users that correspond to all personnel in an enterprise. In HABE model, the Root Master(RM)'s role closely follows the root private key generator (PKG) which is as similar to the HIBE system, is responsible for the generation and distribution of system parameters and domain keys and the Domain Master(DM), is responsible for delegating keys to DMs at the next level and distributing keys to users. Since in the HABE scheme, the attributes which are in one conjunctive clause that are administered by the same domain authority according to the specified policies. The HABE scheme is defined by following algorithm:

1. Setup (K) -> (params, MK0): The RM takes a sufficiently large security parameter K as input, and outputs system parameters params and root master key MK0.
2. CreateDM (params,MKi, PKi+1) -> (MKi+1): Whether the RM or the DM generates master keys for the DMs directly under it using params and its master key.
3. CreateUser (params,MKi, PKu, PKa) -> (SKi,u, SKi,u,a): The DM first checks whether U is eligible for a, which is administered by itself. If so, it generates a user identity secret key and a user attribute secret key for U, using params and its master key; otherwise, it outputs "NULL".
4. Encrypt (params, f, A, {PKa|a E A}) -> (CT): A user takes a file f, a DNF access control policy A, and public keys of all attributes in A, as inputs, and outputs a ciphertext CT.
5. Decrypt (params, CT, SKi, u, {SKi,u,a|aECCj} -> (f):A user, whose attributes satisfy the j-th conjunctive clause CCj, takes params, the ciphertext, the user identity secret key, and the user attribute secret keys on all attributes in CCj, as inputs, to recover the plaintext

Advantage

5. This is designed for an enterprise environment.
6. Combining the features of ABE and Hierarchical Identity-Based Encryption (HIBE).
7. Support Multiple Authorities.
8. It is more scalable and provides fine-grained access.
9. Generation of keys uses a hierarchical structure.
10. Short start-up time.
11. Require less expensive to maintenance, operations and provide disaster recovery.
12. Used for proxy re-encryption.

Disadvantage

5. All attributes in one conjunctive clause which makes difficult to implement.
6. Difficult to manage Multiple Authorities in the system.
7. The computational overhead increase with an increase in authorities.
8. The CA have to manage all the keys in the system which make the user privacy and confidentiality issue.
9. The trust issue is a major problem in the system because CA has the ability to decrypt all ciphertext.

This scheme is a combination of HIBE and CP-ABE. It uses the property of hierarchical generation of keys in HIBE scheme to generate keys. This scheme can satisfy the property of fine grained access control, scalability and full delegation. It achieves fine grained access control in cloud storage services. 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- BasedEncryption

However, HABE uses all attributes in one conjunctive clause those are administrated by the same domain master. Thus the same attribute may be administrated by multiple domain masters according to specific policies, which is most complicated to implement in practice. This scheme has issues with multiple values assignments. HASBE scheme is proposed and implemented by Zhiguo Wan et al [11]. The HASBE scheme is an enhancement of ASBE scheme for handling the users with different privilege levels as shown in Figure

Above system model consists of a root authority, also known as trusted authority (TA), and child authorities which are called as domain authorities (DA), and users like data owners (DO) and data consumers (DC). The cloud computing system consists of five types of parties: a cloud service, provider, data owners, data consumers, a number of domain authorities, and a trusted authority. The trusted authority is root or we can call higher authority. The cloud service provider manages a cloud and provides data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. Each data owner/consumer is administrated by a domain authority. A domain authority is managed by the trusted authority. The trusted authority is responsible for managing top-level domain authorities. It is root level authority. The major functionality of existing HASBE can be explained in: System Setup, Trusted Authority, Domain Authority, File Creation, File Access, and File Deletion

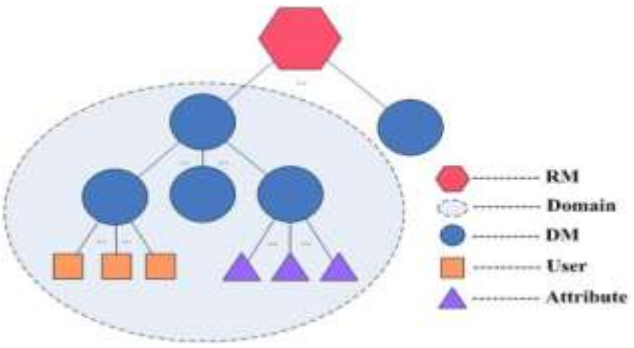

Fig.3: Hierarchical Structure

1. System Setup: In system set up, the trusted authority will select attributes and some random numbers to generate Public Key (PK0), Secret Key and Master Key (MK0). Because of several exponentiation

operations computation complexity of System Setup is O (1).

2. Trusted Authority Grant: Trusted Authority will provide unique ID and a recursive attribute set A= {A0, A1, A2, .Am} to the domain authority. Trusted authority upon receiving join request from domain
3. User Grant: New user either DO/DC will be created by DA here. Domain authority will first verify whether the requested user is valid or not in the basis of its attributes. If user is valid DA will create DO and DC.
4. New File Creation: Here we can assume that cloud service provider may not be trust worthy. He can easily read, alter or delete files uploaded by the data owner. So the data owner has to encrypt his document before uploading it. Using symmetric key each data file is encrypted using the symmetric key and later by using HASBE authority will initially verify whether the requested one is valid authority or not. If it is authorized, the trusted authority will call "create DA", which in turn will generate the master key required for new ly joined DA.
5. User Grant: New user either DO/DC will be created by DA here. Domain authority will first verify whether the requested user is valid or not in the basis of its attributes. If user is valid DA will create DO and DC.
6. New File Creation: Here we can assume that cloud service provider may not be trust worthy. He can easily read, alter or delete files uploaded by the data owner. So the data owner has to encrypt his document before uploading it. Using symmetric key each data file is encrypted using the symmetric key and later by using HASBE.
7. File Access: File Access operation is performed by Data Consumer. To access the file consumer have to decrypt the file for that DEKs is used with the Decrypt algorithm. The coast of decryption depends on the length of the keys used for decryption.
8. File Deletion: This operation is performed by data owner only. The Cloud will check, if the requested user is owner of the file or not, if yes than the cloud will delete the data file.

Advantage

1. Improved version of H-ABE.
2. Provide combine features of HIBE and ASBE.
3. Hierarchical access structure.
4. Users attributes have recursive set.
5. User's attributes can have set of values.
6. All users in this scheme manage by the Domain Authority (DM).

Disadvantage

1. Uses very complex access structure.
2. Verification query for the access policy takes more execution time.
3. Decrease system performance.

Multi- Authority Attribute- Based Encryption (MA-ABE)

All the existing access control mechanisms are based on the ABE encryption techniques and work with only single attribute authority in a system.

The Attribute Authorities (AA) manages all the attributes with both secret keys and public keys in the system. Most of the time, single attribute authority fails to manage all the user's attributes and system overhead increases with a number of users.

However, in the real world situations, it requires more than one attribute authority to manage users in the system where users have registered to the multiple attribute authorities with attributes. All authorities should provide control and share mechanism for user's encrypted data.

To overcome this limitation of the present ABE, Yang et al [17] extends single authority system to a multi-authority based scheme called Multi Authority-based Attribute-Based Encryption (MA-ABE).

The author proposed this scheme for the cloud-based storage which supports multi authorities in the system to provide access control mechanism for efficient encryption and decryption of data.

It has the central authority who is responsible for managing all the registered attribute authorities in the system.

All attribute authorities have to register with the central authority which provides the unique identity to each attribute authorities.

The encryption process uses symmetric encryption techniques for encrypting the data based on the owner's policy where data is divided into different into segments based on the specified policy and each segment encrypted separately.

Attribute Key Generation: A random algorithmic program is pass associate attribute authority. The key secret is to require as associate input for security authority and also the authority's price dk, a user's GID, and a collection of attributes within the authority's domain and output secret key for the user.

Central Key Generation: A central authority is used be pass a random algorithmic program. It takes the master as associate input and a user's GID and outputs secret key for user

Encryption: This system is passing a sender. Take a collection of attributes as associate input for every authority, and also the system public key. The outputs area unit within the variety of cipher text.

Decryption: This mechanism is done by a receiver. Takes input as a cipher text that was encrypted underneath a collection of decoding keys for attribute set. By mistreatment this ABE and MA-ABE it'll increase the system measurability; there are a unit some Restriction in building PHR system. The ABE doesn't handle it with efficiency. In this state of affairs one might regard with the assistance of attributes primarily based broadcast cryptography

Advantage

1. Support multiple authority systems with Collusion resistance.
2. More efficient and scalable.
3. All attribute authorities independently, manages all register users attribute.
4. All attribute authorities work independently which improves the robustness.
5. Attribute authorities need to communicate with each other for encryption and decryption of data.
6. Failure of one or more authorities is not let down the whole system.
7. It is more expressive, efficient and secure than the single-authority system.

Disadvantage

1. Difficult to manage Multiple Authorities in the system.
2. As an increase in the authority involved in the data encryption and decryption time increases.
3. More Communication overhead.

in this scheme is a lower level authority is absent from the work then its stops all the process for authorities attached to the authority.

Parameter / Technique	Fined grained access control	Access structure	Efficiency	Computational overload	Collusion Resistant	Scalability
ABE	Low	Monolithic	Average	High	Average	Good
KP-ABE	Low, high if there is re-encryption technique	Monolithic	Average, high for broadcast type system	Most of the computational overload	Good	Poor
EKP-ABE	Better-Access control than thatof KP-ABE	Non- Monotonic	Higher than KP-ABE, allows constant cipher-text only	Reduces computational overheads	Good	Poor
CP-ABE	Average realization of the complex access control	Monolithic	Average not efficient for modern enterprise environments	Flexible	Scalable	Poor
CP-ASBE	Better-Access Control thanthat of CP-ABE	Monolithic	Better than CP-ABE as there is Less collusion Attacks	Lower than CP-ABE computational overheads	Good	Good
HIBE	Lower than CP-ABE	Hierarchical	Better, Lower as compare to the ABE	Most computational overload	Good	Good
HABE	Good Access control	Hierarchical	Flexible	Some of the overload	Good	Good
HASBE	Better Access control	Hierarchical	Most efficient and flexible	Less overheadthan others	High	High
MA-ABE	Better Access control	Hierarchical	Most efficient and flexible	Less overheadthan others	High	High

III. CONCLUSION

In recent years, attribute based encryption is a relatively attractive research topic and has many attracting properties. 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.

Firstly we expound the emergence and development of ABE schemes and then the two of ABE schemes: KP-ABE and CP-ABE. In ABE scheme, there are both the 'secret key' and 'cipher- text' are associated with a set of attributes. ABE is further modified into KP-ABE that provides fine grained access control.

In KP-ABE, attribute policies are associated with keys and data is associated with the attributes. Keys associated with the policy that is satisfied by the attributes can decrypt the data.

Moreover, we have explored CP-ABE and CP-ASBE. The CP-ABE scheme differs from KP-ABE in such a way that in CP-ABE, ciphertext is associated with an 'access tree structure' and each user 'secret key' is embedded with a 'set of attributes'. The concept of expressive key-policy attribute-based encryption (KP-ABE) scheme is allowing the non-monotonic access structures that may contain negated attributes and fixed constant size ciphertext. The idea of hierarchical IBE (HIBE) in 2002, a user in the higher hierarchical position of the system could create private keys for lower position users. HIBE provides more functionalities than IBE by using more than one private key generator. Hierarchical Identity Based Encryption (HIBE) is the hierarchical form of identity based encryption (IBE).

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. This scheme is a combination of HIBE and CP-ABE. It uses the property of hierarchical generation of keys in HIBE scheme to generate keys. This scheme can satisfy the property of fine grained access control, scalability and full delegation. It achieves fine grained access control in cloud storage services.

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 algorithm

Reference

[1] A.Sahai and B. Waters. "Fuzzy Identity-Based Encryption." In Proc. of EUROCRYPT'05, Aarhus,Denmark, 2005, , pp. 457473

[2] V. Goyal, O. Pandey, A. Sahai, and B.Waters"Attribute-based encryption for fine-grained access control of encrypted data," in Proceedings of the 13th ACM conference on Computer and communications security, pp. 89{98, 2006}

[3] Changji Wang, Yang liu"A secure and Efficient Key-Policy attribute based Encryption Scheme",International Conference on information science and Engineering.2009

[4] 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

[5] N. Attrapadung, B. Libert, and E. de Panafieu, ―Expressive key policy attribute-based encryption with constant-size ciphertexts,‖ in Public Key Cryptography—PKC 2011, vol. 6571, pp. 90– 108, Springer, 2011.

[6] Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran, "AttributeSets: A Practically Motivated Enhancement to Attribute-Based Encryption".

[7] Bettencourt, A. Sahai, andB.Waters"Ciphertext-policy attribute based encryption "in Proceedings of IEEE Symposium on Security and Privacy, pp. 321V334, 2007

[8] R. Ostrovsky, A. Sahai, and B.Waters, ―Attribute-based encryption with non-monotonic access structures,‖ in Proceedings of the 14th ACM Conference on Computer and Communications Security (CCS '07), pp. 195–203, November 2007.

[9] Horwitz and B. Lynn, "Toward hierarchical identity-based encryption," in Advances in CryptologyEUROCRYPT 2002. Springer, 2002, pp. 466–481

[10] G. Wang, Q. Liu, and J.Wu,"Hierachical attribute-based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM conference on Computer and communications security

[11] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access control in Cloud Computing", IEEE Transactions on Information Forensics And Security, Vol.7 ,No. 2 , April 20

[12] Kan Yang, Xiaohua Jia, Expressive, Efficient, and Revocable Data Access Control for Multi-Authority cloud Storage" IEEE Transactions on Parallel and Distributed Systems,Vol,25,No 7, July 2014