Analysis of Attribute Based Encryption Techniques in Cloud Computing Environment

S. Pavan Kalyan[1] Ch. Swathi Sri[2] P. Balaji Reddy[3] Dr Naveen Kumar[4]
[1,2,3]B. E Student [4]Assistant Professor
[1,2,3,4]Department of Computer Science and Engineering
[1,2,3,4]Koneru Lakshmaiah Educational Foundation, Vaddeswaram, AP, India

Abstract— In cloud computing, mobile devices can store personal data from anywhere at any time. The data security and privacy are the major concerns for the cloud. The data transfer should be flexible, scalable, and access control must be maintained in the cloud system. Substantial studies have been conducted to improve the cloud security. There are several existing works for access control, computation overhead and efficiency of the methods. This study is a complete analysis of these methods on various schemes for (ABE) attribute encryption technique. These methods are studied and analyzed for their limitations that consist of Attribute Based Encryption (ABE), Key Policy Attribute Based Encryption (KP-ABE), Cipher text Policy Attribute based encryption (CP-ABE), Cipher text Policy Attribute-Set based Encryption (CP-ASBE), Multiple authority Attribute based encryption (MA-ABE), Batch Attribute Based Encryption (BABE), Hybrid identity-based encryption (HIBE), Hierarchical Attribute Based Encryption (HABE), Hierarchical Attribute Set Based Encryption (HASBE). To achieve scalability, and access control in cloud computing HASBE was implemented. By applying a delegation algorithm to ASBE, the HASBE model integrates a hierarchical structure to device users. HASBE allows compound attributes and also achieves effective user revocation due to multiple attribute values. So, HASBE is the most efficient algorithm among the compared algorithms.

Keywords: Scalability, Flexibility, Access Control and Trusted Authority

I. INTRODUCTION

At present various cloud mobile applications are rapidly used. In these applications data owners can upload their data like documents, videos, photos and other files to cloud. The owners can share the data with another user. Cloud service provider can provide security as there is a valuable and sensitive data in the cloud. The access control mechanism provided by cloud service provider (CSP) is not convenient because the mechanism doesn't meet the requirements of data owners. First, when owner upload their data on cloud, they leave their data in a place. Secondly, authorities have to send a key to each data the key to the groups to share the data. For protecting data in cloud, the data must be encrypted user. To simplify this process data owner can divide data users into different groups and send before uploading to the cloud by using some cryptographic algorithms. As of now, HASBE is the most efficient algorithm which is working efficiently on cloud [7]. The article is discussing the Attribute-Based Encryption (ABE) schemes [1] and how it has been modified for further enhancement into Key Policy Attribute based encryption (KP-ABE), Cipher-text Policy Attribute Encryption (CP-ABE) and more it was proposed as CP-ASBE and further MABE, BABE, HIBE, HASBE.

Flexibility, scalability and access control increases from ABE to HASBE accordingly. In Case of ABE, access control is less and this is increased in KPABE. KPABE is not suitable for all applications so CPABE came into picture. CP-ABE has limitations in specifying user attribute policies and managing user attributes. CP-ASBE overcomes this issue but it constitutes of many steps in encrypting and decrypting the data which is time-taking process. HABE solves this problem. Since the same domain authority can administer the same attribute which becomes a disadvantage to HABE. This problem is solved in HASBE. The main criteria of HASBE were Data confidentiality (protecting the data from unauthorized users), grained access control (Providing access permission to different users), scalability(system performance increases when number of authorized users increase) and flexibility(ability to run an application on any platform and ability to use the application easily and to fix problems by adding or removing some resources, if needed) which are achieved in HASBE algorithm.

II. LITERATURE SURVEY

To store the data in the cloud we need security and privacy. For secure storing and sharing of the data the user can store the data in the form of encryption. Encryption was help to avoid the unauthorized access of data from the cloud [12]. To give the security, privacy and confidentiality for the data stored in the cloud different methods are discussed.

A. Attribute Based Encryption (ABE):

In ABE key authority came into picture. Generating the keys for the encrypting and decrypting a message is a major role for key authority. KA generates the keys based on user's attributes. If the user wants to add some attributes or remove the some attributes then KA collect the new attributes and generate new public and private key based on new attributes [12].

B. Key Policy Attribute Based Encryption (KP-ABE):

It is used for one-to-many communication. In the KP-ABE the encrypted data are connected with set of attributes and secret key. The data sharing is the main application of KP-ABE in the un-trusted cloud storage [13]. In this scheme data is firstly encrypted using the symmetric data encryption key then again re-encrypting that data using public key consequent to set of attributes [13].

C. Cipher Policy Attribute Based Encryption (CP-ABE):

CP-ABE depended by cipher text and users which are interconnected with attributes and policy. The data is encrypting using access policy and same message decrypting using attributes [2].

D. Cipher text Policy Attribute-Set Encryption (CP-ASBE):

This study of [3] introduces the concept of Cipher text Policy Attribute-Set Encryption (CP-ASBE). The CP-ASBE organize the user attributes into a recursive set-based structure and allows user to impose dynamic constraints.

E. Multi-Authority Attribute Based Encryption (MABE): The study of [4] introduce the Multi-authority attribute-based encryption. In this framework it uses multiple parties to distribute attributes for users. A Multi Authority ABE framework is compared with K attribute authorities and only one central authority. In setup the security parameter will take as input, it outputs a public key PK and secret key pair for each attribute authorities and system public key and master secret key is used by central authority.

F. Batch Attribute Based Encryption (BABE):

The data owner can share data in batches of the users of different organizations. The setup in BABE takes security parameter and attribute universe U as input and it returns public key PK and master keys MK. The public key PK parameters and a message M which contains different messages and a series of attribute sets return cipher text in the encryption. The key generation takes access structure A and master key as input and it generates the secret key SK.

G. Hierarchical Identity-Base Encryption (HIBE):

The study in [5] tells about hierarchical identity-based encryption (HIBE) is extended from IBE. Here, the private key is delivered by a solo private key generator (PKG) with the public keys as their primitive ID (PID), so-called as 1-HIBE in an overall identity-based encryption scheme and its limitation is heavy key managing. A Hierarchical Identity Based Encryption scheme has Setup, Encryption, Key Generation, Decryption, and Delegate.

H. Hierarchical Attribute-Base Encryption (HABE):

The study in [6] introduces the concept of Hierarchical Attribute-Base Encryption (HABE). In cloud storage service, to provide fine-grained access control Hierarchical Attribute-Base Encryption is introduced.

E. Hierarchical Attribute Set Based Encryption (HASBE):

The study in [7] introduces the concept of Hierarchical Attribute Set Based Encryption (HASBE). In HASBE, the system consists of five modules: cloud service provider, data owner, data consumer, domain authority, trusted authority will arrange in hierarchical manner.

III. ABE BASED ALGORITHMS

A. Attribute Based Encryption (ABE):

The study in [1] is proposed very first, the concept of Attribute based encryption. The ABS (Attribute Based Encryption) main aim is to provide security and access control for Attribute Based Encryption. In these Attribute can be defined as the object that should be managed. Access control means a system that grants or revokes the right to access data like file which give permission to read, write, edit or delete. It is actualized for one to many encryptions that permits users to encrypt and decrypt data based on user attributes. In the algorithm the secret key (SK) of a user and cipher text (CT) are dependent upon the attributes. In the ABE, owner wants to encrypt the file for all users who have a specific set of attributes. In ABE, the decryption is possible only if contains set of attributes of the user key will matches the attributes of the cipher text. User can decrypt a cipher text if there is only match between decryption key and cipher text. The ABE Algorithm consists of following four steps:

1) Step 1: Setup
2) Step 2: Encryption
3) Step 3: Key generation
4) Step 4: Decryption

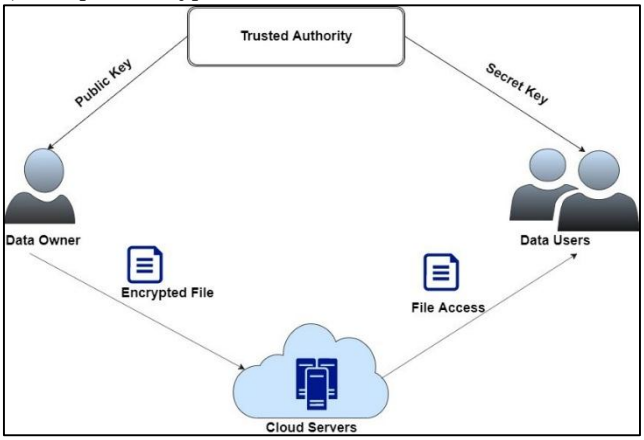

Fig. 1: ABE Architecture

In the above figure 1 it consists of three entities in ABE. The user and the data owner and a trusted authority (third party). The trusted authority generates the keys for the encryption and decryption of data owners and users. With the help of pre-defined set of attributes, public and master keys are generated. When a user with new attributes is added, then those attributes are added to the set and new public and master keys are generated.

1) Limitation of ABE

1) The Problem with attribute-based encryption scheme is that data owner needs to use every user's public key encrypt data.
2) If there are more users to access a single data file uploaded by a data owner in the cloud, the data owner needs to know the public keys of each and every user which is not an efficient process in the cloud. This is one of the important limitations that becomes problem to the data owner to keep track each and every one user public key. This process raises the ambiguity in giving access to users, loosing access control over users by data owner. So, it is concluded that Access Control is weak in ABE.

B. Key Policy Attribute Based Encryption (KP-ABE):

The study in [1] proposed a KP-ABE scheme. It is modified version of standard [1] ABE in which attribute policies are associated with keys and the data is associated with attributes. The KP-ABE provides a public key encryption technique that's designed for one-to-many communications. Key Policy Attribute Based Encryption main aim is to provide more general access control. The setup step in KP-ABE takes security parameter as input and returns the public key pk and master key mk. The public key is used by senders for encryption. The master key will generate user secret key and it is known to authority. The set of attributes and public key pk takes as input in the encryption and returns the cipher text. In the key generation master secret key MK and access structure T will come under input and enable the user to decrypt a message under the set of attributes. Re-encryption

technique is used in KP-ABE. The KP-ABE Algorithm consists of following four steps:

1) Step 1: Setup (security parameter k and returns public key PK and master security key MK)
2) Step 2: Encryption (message M, public key PK, set of attributes and returns cipher text E)
3) Step 3: Key Generation (access structure T, master security key MK and returns secret key SK)
4) Step 4: Decryption (cipher text E and returns message M)

The figure 2 there are four steps in KPABE: In the first step, the security parameters are taken as input and a public key and a master key are generated as output. Public key is used by owners for encryption and master key is used for users. In the second step, the algorithm takes the data, the public key and an arrangement of attributes as input and gives cipher text as output. In the key generation step, the algorithm accepts a structure of access and the master key as input and gives a secret key as output for the users.

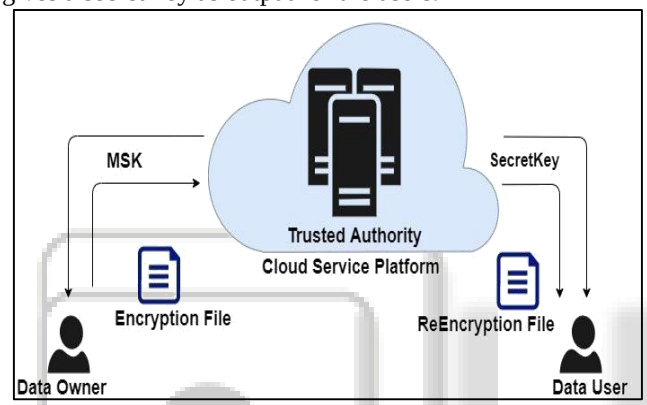

Fig. 2: KP-ABE Architecture

1) Limitation of KP-ABE

It is providing access control but has no longer with flexibility and scalability. This algorithm fails to run in different devices and has no ability to handle growing and decreasing resources in cloud. So, this algorithm fails to provide flexibility and scalability.

C. Cipher Text Policy Attribute Based Encryption (CP-ABE):

The work done in [2] introduces the concept of CP-ABE. Cipher text Policy Attribute Based Encryption objective is to provide secure access control. It works in the reverse way of KP-ABE. In CP-ABE scheme attribute policies are associated with data and keys are associated with data. CP-ABE schemes can fall into different types of access structures. They are including AND gate access structure [8] and threshold access structure [9][10] for short ciphertexts. In CP-ABE users can obtain the credentials from a system manager at beginning of the setup phase. The access ability in CPABE is valid even may break the rules from the private information. CP-ABE will depend upon the policy and attributes associated with cipher text and user decryption keys. In setup security parameter as taken as input and it will return the public key and master secret key MK. PK public key is used for encryption of message. The CP-ABE in decryption it takes cipher text as input and returns the message If it satisfies the access structure associated with the cipher text. In CP-ABE the secret key will be generated based upon the attributes. The encrypted data will be very confidential and it provide secure access to the user. Compare to KP-ABE the computation overhead is very less in CP-ABE.

The CP-ABE algorithm consists of following four steps:

1) Step 1: Setup (security parameter k and returns public key PK and master security key MK)
2) Step 2: Encryption (message M, public key PK, access structure T and returns cipher text E)
3) Step 3: Key Generation (set of attributes, master security key MK and returns secret key SK)
4) Step 4: Decryption (cipher text E, secret key SK and returns message M)

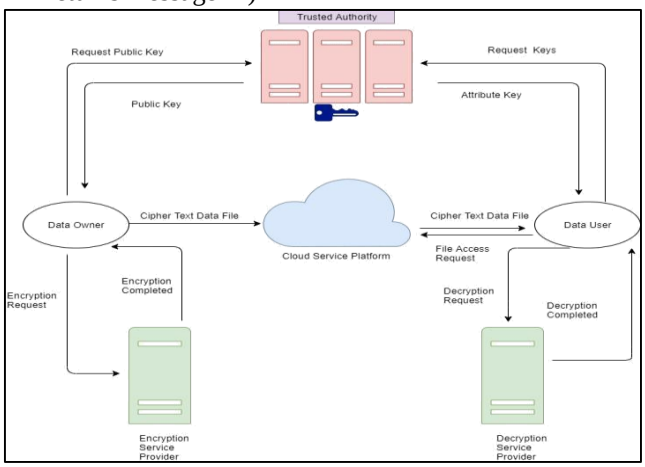

Fig. 3: CP-ABE Architecture

In the above figure 3 there are three steps in CP-ABE which are Encryption, Key generation and decryption. Before these it gives out a public key and a master key as the output. Encryption: To encrypt the data the algorithm accepts the public key, data and access structure as input. Key Generation: It accepts the universal key and set of attributes from data owner and gives out secret key. Decryption: It accepts the public key cipher text and the secret key from the user data will be decrypted only if the set of attributes in secret key corresponds to the structure of access.

1) Limitations CP-ABE

1) Cipher text Policy Attribute Based Encryption is not fulfilling the enterprise requirements means business logic of access control which require considerable flexibility and efficiency.
2) Since users in the cloud share a share common attribute space, it becomes a complicated task to remove a user or to deny user's access to a particular data.

D. Cipher text Policy Attribute-Set Encryption (CP-ASBE):

This study of [3] introduces the concept of Cipher text Policy Attribute-Set Encryption (CP-ASBE). The CP-ASBE organize the user attributes into a recursive set-based structure and allows user to impose dynamic constraints. CP-ASBE consists of recursive set of attributes. Consider the attributes for student will derived from the courses they have taken. Each student has a set of attributes (Course, Year, Grade) for every course he/she has taken. To have a policy consider an example of student. "The students who took a course that should be satisfies 300<=course<400 and Year>=2009 and Grade>3". Enforcing such policy in CP-ABE is very difficult, student could have taken multiple courses and will obtain different grades. The encryption will

ensure the student cannot select and combine attributes from different sets. In CP-ABE, the decryption of keys can support user attributes that organizes as a single set, so users can only use possible combinations of attribute in a single set issue in their keys to satisfy policy. The CP-ASBE overcome the above problem.

The CP-ASBE algorithm consists of following four steps:

1) Step 1: Setup (depth parameter d and returns public key PK and master security key MK)
2) Step 2: Key Generation (master security key MK, identity of user u and returns secret key SK)
3) Step 3: Encryption (message M, public key PK, access structure T and returns ciphertext E)
4) Step 4: Decryption (cipher text E, secret key SK and returns message M)

1) Limitations of CP-ASBE

As this algorithm includes in lot of steps in encrypting, decrypting and getting public and private keys from trusted authority which consumes a lot of time, efficiency and Computation overhead cannot be fulfilled.

E. Multi-Authority Attribute Based Encryption (MABE):

The study of [4] introduce the Multi-authority attribute-based encryption. In this framework it uses multiple parties to distribute attributes for users. A Multi Authority ABE framework is compared with K attribute authorities and only one central authority. It allows any number of independent authorities to monitor attributes and distribute private keys and Tolerate any number of corrupted authorities. In setup the security parameter will take as input, it outputs a public key PK and secret key pair for each attribute authorities and system public key and master secret key is used by central authority. Authority secret key and authority value, set of attributes will be taken as input for attribute key generation and it outputs a secret key for the user. Master secret key takes as input for the central key generation and produces secret key of each user. Each authority will take set of attributes for input in encryption and it outputs ciphertext. In decryption it takes ciphertext as input and it generates outsource data files. The complexity in the multi-authority scheme required that each authority's attribute set should be disjoint. The Multi-Authority Attribute Based Encryption consists of following five steps:

1) Step 1: Setup (security parameter and returns public key and master secret key)
2) Step 2: Attribute Key Gen (authority secret key SK, authority value and returns secret key)
3) Step 3: Central Key Gen (master secret key, users set and returns secret key)
4) Step 4: Encryption (attributes for each authority, public key PK and returns cipher text)
5) Step 5: Decryption (cipher text, attribute set and M)

F. Batch Attribute Based Encryption (BABE):

ABE is a one type of public key encryption suitable for cloud storage. Each user holding a secret key, one can decrypt a ciphertext only if the associated attributes match the predetermined access policy, which allows one to access control on outsourced files. The issue in existing ABE schemes is that they are designed for the users of a single organization. When owner wants to share the data with the users of different organizations, the owner needs to encrypt the data to the users of one organization and it repeats this process for another organization. In this batch attribute-based encryption (BABE) approached to address this problem in a secure way. The data owner can share data in batches of the users of different organizations. The setup in BABE takes security parameter and attribute universe U as input and it returns public key PK and master keys MK. The public key PK parameters and a message M which contains different messages and a series of attribute sets return cipher text in the encryption. The key generation takes access structure A and master key as input and it generates the secret key SK. The Decryption in BABE is takes input as secret key, cipher text, access structure and it returns message. The BABE Algorithm consists of four steps:

1) Step 1: Setup (security parameter K, attribute universe U and returns public key PK and Master security key MK)
2) Step 2: Encryption (message M, public key PK, set of attributes and returns ciphertext CT with the attributes sets)
3) Step 3: Key Generation (access structure A, master security key MK and returns secret key SK)
4) Step 4: Decryption (secret key SK, cipher text CT, access structure A as input and returns message M)

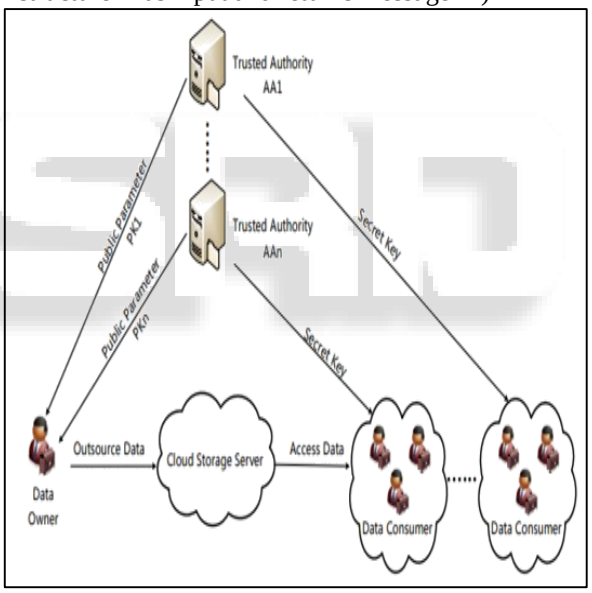

Fig. 4: BABE Architecture

In the above figure 4 it consists of four types of parties: the data owner, the cloud server, the data users and the authority. The data owner would like to share data with the data users managed by different authorities. Each authority will generate a secret key for the data user according to the user's attributes. The data owner can encrypt the data for the users of different organizations, i.e., the users are managed by different authorities. Then, the data owner can upload the encrypted data to the cloud storage server. When a data user requests for the cloud server, the server responds with the corresponding ciphertext. The user can decrypt if the attributes labelled with the ciphertext meets the access policy associated with the secret key of the user data.

G. Hierarchical Identity-Base Encryption (HIBE):

The study in [5] tells about hierarchical identity-based encryption (HIBE) is extended from IBE. Here, the private

key is delivered by a solo private key generator (PKG) with the public keys as their primitive ID (PID), so-called as 1-HIBE in an overall identity-based encryption scheme and its limitation is heavy key managing. Therefore, to overcome this, a 2-HIBE scheme is introduced that consists of domain PKG and a root PKG. The consumers and these are connected with a random string of PID. A Hierarchical Identity Based Encryption scheme has Setup, Encryption, Key Generation, Delegate and decryption. In Setup it takes a security parameter λ as input and outputs the public parameters PK and a master secret key MSK. And in the Ken Generation it takes the master secret key and an identity vector I as input and outputs a private key. In the Delegate it takes a secret key for the identity vector I of depth d and an identity I as input and outputs a secret key. And in the decryption step it takes the public parameters PK, a ciphertext CT, and a secret key SK as input and outputs the message M, if the ciphertext was an encryption to an identity vector I and the secret key is for the same identity vectors. A Hierarchical IBE system (HIBE) will provides additional functionality by forming levels of an organizational hierarchy. A user at level k will delegate secret keys to descendant identities at lower levels, however it cannot decrypt messages supposed for a recipient that is not among its descendants. For example, a user with the identity "University of Texas: computer science department" can delegate a key for the identity "University of Texas: computer science department: grad student", but however it cannot delegate keys for the identities that don't begin with "University of Texas computer science department".

The HIBE Algorithm consists of following five steps:

1) Step 1: Setup (security parameters and returns public key PK and master secret key MSK)
2) Step 2: Key Generation(master secret key and identity vector and generates private key)
3) Step 3: Delegate (Generate secret key and identity vector)
4) Step 4: Encryption (message M, public key PK and returns ciphertext E)
5) Step 5: Decryption (ciphertext E, secret key SK and returns message M)

H. Hierarchical Attribute-Base Encryption (HABE):

The study in [6] introduces the concept of Hierarchical Attribute-Base Encryption (HABE). In cloud storage service, to provide fine-grained access control Hierarchical Attribute-Base Encryption is introduced text. The HABE model consists of a root master corresponding to the trusted third party, multiple domain masters in which top level domain masters correspond to multiple users of enterprises and numerous users corresponding to all employees of an organization. This scheme used the hierarchical generation property when keys are used to be created in HIBE scheme. It uses a file, a DNF access control rule, and public keys to all attribute's inputs for encryption and cipher text. The setup consists of a trusted authority which provides secret keys to the users. HABE is the combination of HIBE and CPABE.HABE provides fine-grained access control to the users. The HABE model consists of a root master corresponding to the trusted third party, multiple domain masters in which top level domain masters correspond to multiple users of enterprises and numerous users corresponding to all employees of an organization. This scheme used the hierarchical generation property when keys are used to be created in HIBE scheme. The root master takes as input a sufficiently large security parameter and outputs system parameters and root master key. The HABE can satisfy the property of secured access control and scalability. The root master takes as input a sufficiently large security parameter and outputs system parameters and root master key. Otherwise it outputs null. The algorithm uses a file, a DNF access control rule, and public keys to all attribute's inputs for encryption and cipher text. This algorithm can satisfy the property of secured access control and scalability. The HABE Algorithm consists of following five steps:

1) Step 1: Setup (Root Master RM and returns system parameter and return root master key MK0)
2) Step 2: Create DM (RM or DM generates master keys)
3) Step 3: Create User (Generates user identity secret key and user attribute secret key)
4) Step 4: Encryption (message M, public key PK and returns ciphertext E)
5) Step 5: Decryption (ciphertext E, secret key SK and returns message M)

I. Hierarchical Attribute Set Based Encryption (HASBE):

The study in [7] introduces the concept of Hierarchical Attribute Set Based Encryption (HASBE). In HASBE, the system consists of five modules: cloud service provider, data owner, data consumer, domain authority, trusted authority will arrange in hierarchical manner. The cloud service provider manages to provide data storage service. The data files are encrypted by the data owners. Data owner can store encrypted files in the cloud to share with data consumers. Later data consumer can download the encrypted files and decrypt them. The trusted authority will distribute the keys to domain authority. Domain authority distribute the keys to the data owner and data consumer. Domain authority is responsible for sending keys to owner and users. The data is encrypted by taking public key and owner can upload the data in cloud. Using the secret key by checking the correspondence between the attributes of secret key and access structure, the data is decrypted. The HASBE Algorithm consists of following four steps:

1) Step 1: System Setup (d as depth parameter and returns public key PK and master key MK)
2) Step 2: Key Gen (master secret key MK, key structure A and return master secret key SK)
3) Step 3: Encryption (public key PK, message M, access tree T and returns cipher
4) Step 4: Decryption (ciphertext, secret key SK and returns message M

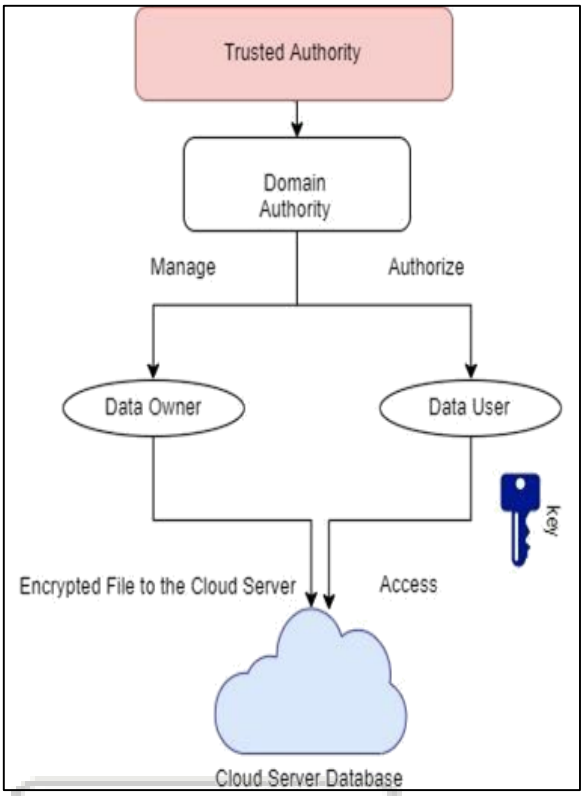

Fig. 5: BABE Architecture

In the figure 5 there are five steps in HASBE a certain trusted authority is set for the attributes and it gives public key and master key to domain authority. Domain authority is responsible for sending keys to owner and users. The data is encrypted by taking public key and owner can upload the data in cloud. Using the secret key by checking the correspondence between the attributes of secret key and access structure, the data is decrypted.

IV. A Complete Analysis of ABE Based Algorithms

The below table gives the comparison of attribute-based encryption techniques.

Which include ABE, KP-ABE, CP-ABE, CP-ASBE, MABE, BABE, HIBE, HABE and HASBE.

S.NO	ABE Techniques	Access Control	Efficiency	Computational Overhead
1.	ABE	Medium	Average	More
2.	KP-ABE	Medium	Average	More
3.	CP-ABE	Average	Average	Average
4.	CP-ASBE	Better compare to CP-ABE	Better than CPABE as there is less collision attacks	Better than CP-ABE
5.	MABE	Better	Better and Scalable	Average
6.	BABE	Better	Better	More
7.	HIBE	Lower than CPASBE	Better than CPASBE	More
8.	HABE	Better	Flexible and Scalable	Some Overhead will takes place
9.	HASBE	Good	More efficient and Flexible	Less Overhead Than all ABE Techniques

V. Conclusion

In this paper we have seen different attribute-based encryption algorithms that are used for flexible, scalable and access control in cloud computing. A collection of attributes is associated with both the secret key and cipher-text in the ABE scheme. ABE is also developed into KPABE, which provides control of access. In KPABE, keys are associated with attribute policies and the attributes are associated with data. Data can be decrypted by keys associated with the policies that is satisfied by attributes. Moreover, we have explored CP-ABE and CPASBE. The CP-ABE scheme differs from KP-ABE in such a way that ciphertext is combined with an access tree structure and array of attributes is inserted in each user's secret key. Attribute policies are linked to data and attributes are linked to keys and only those keys that the associated attributes meet the data policy can decrypt the data. HASBE incorporates HIBE and ASBE features. The HASBE scheme easily implements a device client hierarchy structure. This uses an algorithm for delegation to CP-ASBE. Out of those schemes, the HASBE scheme can provide more scalability, flexible and fine access control than any other schemes in cloud computing.

References

[1] Li Jiguo, key-policy attribute-based encryption against continual auxiliary input leakage. Information Sciences 470 (2019)
[2] Jiang, Y Susilo, W. Mu, Y. and Guo, Ciphertext-policy attribute-based encryption against the key-delegation abuse in the cloud computing. Future Generation Computer Systems(2018)
[3] Kumar, G. Sravan, and A. Sri Krishna. The Privacy Sustaining Constant Length CiphertextPolicy Attribute-Based Broadcast Encryption. Soft Computing and Signal Processing. Springer (2019).
[4] Sandor, VoundiKoe .The Efficient decentralized multi-authority attribute based encryption for mobile cloud data storage. Journal of Network and Computer Applications 291 (2018)
[5] Zhong, Hong, Yan Xu, and Jie Cui. Multi-authority attribute-based encryption access control scheme with hidden policy for cloud storage."Soft Computing 22, no. 1 (2018)
[6] Huang, Yixian Yang, and Mansuo Shen. The Secure and efficient data collaboration with hierarchical attribute-based encryption in cloud computing. Future Generation Computer Systems 72 (2017)

[7] Ahuja R, Mohanty SK. A scalable and flexible attribute-set-based access control with both sharing and full-fledged delegation of access privileges in cloud computing. Computers & Electrical Engineering. 2017.
[8] L. Cheung and C. C. Newport. The provably and secure ciphertext policy in ABE. in Proc of ACM Conference on Computer and Communications Security'06. ACM, 2017, pp. 456– 465.
[9] J. Herranz, and C. Rafols, Constant size ciphertext in threshold attribute-based encryption in cloud. Public Key Cryptography'10, ser. LNCS, vol. 6056, 2010, pp. 19–34.
[10] C. Chen, J. Chen, Z. Zhang, D. Feng, S. Ling, and H. Wang, Fully secure attribute-based scheme systems with short ciphertext and threshold access structures in Proc. CTRSA'13, vol. 9779, 2013.
[11] Zhiguo Wand Robert H. Deng: 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 2012
[12] S.Yu, Ch. Wang, K. Reny, and W. Louis :The attribute based data sharing with attribute revocation, in ASIACCS'10, 2010
[13] Chang-ji Wang, Jian Fa Luo: The key-policy Attribute-based Encryption scheme with Constant size Ciphertext(2012)

