International Journal of Advanced Pervasive and Ubiquitous Computing
Volume 11 • Issue 3 • July-September 2019

A Comprehensive Review of Access Control Mechanism Based on Attribute Based Encryption Scheme for Cloud Computing

Lokesh B. Bhajantri, Basaveshwar Engineering College, Bagalkot, India
Tabassum N. Mujawar, Ramrao Adik Institute of Technology, Navi Mumbai, India

ABSTRACT

Cloud computing is the most prevailing paradigm, which provides computing resources and services over the Internet. Due to immense development in services provided by cloud computing, the trend to share large-scale and confidential data on cloud has been increased. Though cloud computing provides many benefits, ensuring security of the data stored in cloud is the biggest challenge. The security concern about the data becomes main barrier for adoption of cloud. One of the important security aspects is fine grained access control mechanism. The most widely used and efficient access control scheme for cloud computing is Attribute Based Encryption (ABE). The Attribute Based Encryption (ABE) scheme provides a new technique for embedding access policies cryptographically into encryption process. The article presents an overview of various existing attribute-based encryption schemes and traditional access control models. Also, the comparison of existing ABE schemes for cloud computing, on basis of various criteria is presented in the article.

KEYWORDS

Access Control, Attribute-Based Encryption, Cloud Computing, Outsourcing

INTRODUCTION

In today's era, cloud computing has become an attracting technology, which has brought extreme changes to IT industry. Cloud Computing enables network access to various computing resources such as servers, storage, networks, applications and services. It is basically a paradigm that provides access to shared pool of resources online on demand (Armbrust et al., 2010). It is computing over internet. The users can store any amount of data on cloud and then can access it at any time, from anywhere. The most fascinating benefit of cloud computing is that it provides cost saving as the users will pay only for their usage. Cloud computing is also termed as distributed computing over a network. The term cloud can be defined as collection of servers delivering computing resources as a service on demand. Generally, the cloud comprises various interfaces, networks, hardware, storage devices etc. (Majumder et al., 2014).

DOI: 10.4018/IJAPUC.2019070103

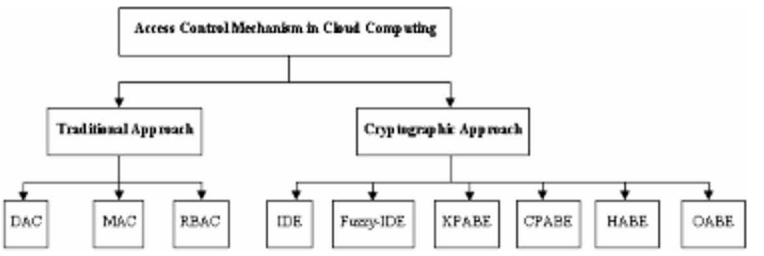
Security is the biggest barrier for adoption of cloud computing. The data is present in shared environment, where other users can also access it. The users do not have complete control over the transit of data stored in cloud as both users and data are present in different domain. Hence the privacy concern arises for user's data and many users cannot completely trust the cloud environment. (KPMG, 2010; Hashizume et al., 2013, Tabassum et al., 2017). The security challenges can be faced at different levels such as architectural level, communication level and contractual and legal level (Ali et al., 2015). After adoption of cloud computing the organization cannot apply traditional security mechanism such as authentication, authorization in similar way as they exist. The reason is that the security requirements of organization with cloud environment are very much different than the traditional organization (Li and Ping, 2009).

Generally, in cloud environment users share their sensitive data with other users. In order to access the data, user must possess necessary permissions or credentials. Access control is a mechanism, which decides who can use a specific system, resource or application. It defines a way to allow, deny or restrict user access to system or its resources (Khan, 2012). Access control mechanism ensures that data must be accessed by authorized users only. In cloud environment, the owner of data and the data are present in different administrative domains. Thus, it is extremely important to ensure authorized access to data and manage user's identity. Due to the distributive and dynamic nature of cloud computing access control becomes very complex task. In traditional method the data is stored on some third-party server and access control mechanism is employed statically. However, this method does not guarantee the confidentiality of data because the server storing the data can be untrusted entity. Therefore, providing better access control mechanism is a very important component of cloud security (Majumder et al., 2014). The main goal of access control is to restrict user to access what he/she should be able to do and prevent unauthorized access. The access control is defined as a mechanism to determine correct access to data by legitimate user depending on access privileges and permissions that are already defined in security policies (Younis et al., 2014). The major endeavor of this paper is to present brief overview of access control mechanisms used for cloud computing. Here, the classification of access control models applied for cloud computing that includes some traditional models and various Attribute Based Encryption schemes is elaborated.

The classification of access control models for cloud computing includes two categories as traditional models and the models based on cryptographic approaches. The taxonomy of access control models applied for cloud computing is depicted in Figure 1. The Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role based Access Control (RBAC) model come under traditional access control models.

This classification is based on the way in which access for any object is granted to any user. The traditional models lack in meeting all security requirements of cloud computing. Hence a new paradigm of integration of cryptographic techniques into access control model is introduced. On basis of this approach, the different access control techniques presented in literature includes Identity Based Encryption (IBE), fuzzy- Identity Based Encryption (fuzzy-IBE), Key Policy-Attribute Based

Figure 1. Taxonomy of access control models



Encryption (KP-ABE), Ciphertext Policy-Attribute Based Encryption (CP-ABE), Hierarchical Attribute Based Encryption (HABE) and Outsourcing based Attribute Based Encryption (OABE).

The following sections describe an overview of traditional access control models, the different cryptographic access control techniques, the comparison of all schemes and finally concluding remarks of the paper.

TRADITIONAL APPROACH FOR ACCESS CONTROL

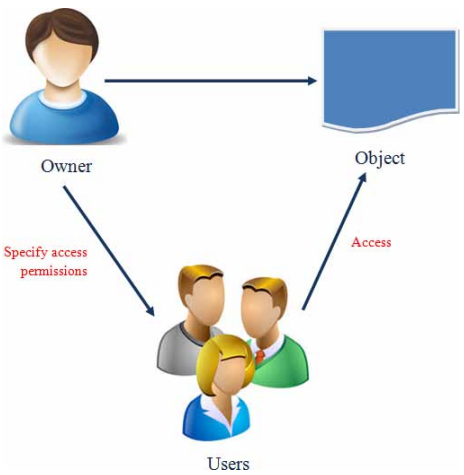
The different traditional Access Control Models presented in literature are Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role based Access Control (RBAC) model (Ausanka, 2004). All these models are elaborated in following subsections.

Discretionary Access Control (DAC) Model

In Discretionary Access Control (DAC), the owner of data or object decides the access permissions for other users. This model allows owner of object to restrict access to their objects based on user's identity or membership in a particular group. This model is also called as owner-controlled model. Figure 2 provides overview of DAC model.

The fine-grained access control for data is provided by this model. In this model separate access rules are defined for individual user or group of users. In order to specify such access rules an access control list (ACL) is maintained. The ACL contains tabular representation of mapping between subjects and individual access rules over objects. The system performs right lookup in the ACL, on each object accesses and decides access rights of any user over the objects (Majumder et al., 2014). The main advantage of DAC model includes its flexibility. The DAC model has lots of disadvantages when adopted for cloud computing. In DAC there is no mechanism provided for management of improper access rights. Suppose any user has only read access to a file. Such user can copy the contents of file to another file and then can use it in any way or pass it to another user. Thus, DAC model does not have any control over copies of data created by user. The major drawback of DAC model is that there is no control over usage of object and information flow. Also, the DAC model cannot deal with Trojan horses, where access permissions are inherited. It is also possible that the user can pass its access rights to another user, which can violate the security of an object (Younis et al., 2014). Another disadvantage associated with DAC is that it is not scalable. The system, where large number of subjects and objects are present such as cloud computing, the management and

Figure 2. Discretionary access control (DAC) model



updation of access rules becomes very complex. Therefore, the DAC model is not suitable for such systems (Majumder et al., 2014).

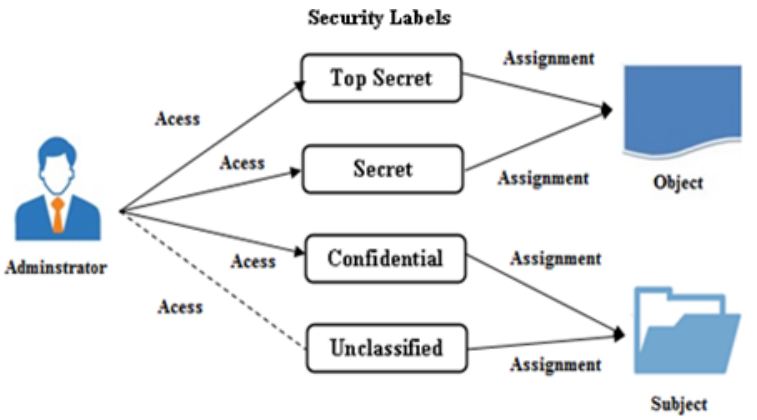
Mandatory Access Control (MAC) Model

In MAC model, the central authority of the system decides access permissions. The user does not play any role for deciding the access permissions. Thus, in this model the central administrator controls all the access permissions, which user cannot modify. The policy defined by administrator will determine who can have access to which data or object. It is mainly based on security levels that help to identify access right of subject over the objects. Each object and subject are assigned a security level. The security levels are organized in hierarchical manner. The security levels classification consists of labels such as secret, top-secret, unclassified and confidential. The basic idea of MAC model is depicted in Figure 3.

The security labels are attached with the subjects and objects throughout the system. The objects are classified according to these security labels that are assigned based on the sensitivity of information contained in it and subjects are classified on basis of trustworthiness or rules for subject. There are two security models associated with MAC: Bell and LaPadula Model (Bell and LaPadula, 1973) and BiBa Model (Biba, 1977). The Bell and LaPadula model mainly focuses on confidentiality of information. It follows two basic principles i.e. "no-read-up" and "no-write-down." The no-read-up rule says that the user at lower level cannot read anything from object at higher level. The no-write-down rule says that the user at higher level can only write to object at same level but not at lower level. On other hand the Biba model focuses on integrity of information and states two principles as "read-up" and "write down". Here the user at lower level is allowed to read information from higher level and user at higher level can write to lower level (Millen, 2011).

These two models guarantee secure data flow and integrity of objects; still they do not provide complete secrecy of information. The MAC model is simple and provides higher security as only central administrator can decide and modify all access permissions. However, the central administrator can become single point failure in MAC. The user has to take permission from system administrator for each activity, so it is quite difficult to implement (Majumder et al., 2014). The MAC model overcomes the disadvantage of DAC, but it lacks in flexibility. The security labels are not flexible enough and cannot be used to execute task (Younis et al., 2014). Also, it does not ensure fine-grained access control, dynamic separation of duty, least privilege and validation of trusted components (Majumder et al., 2014).

Figure 3. Mandatory access control (MAC) model



Role-Based Access Control (RBAC) Model

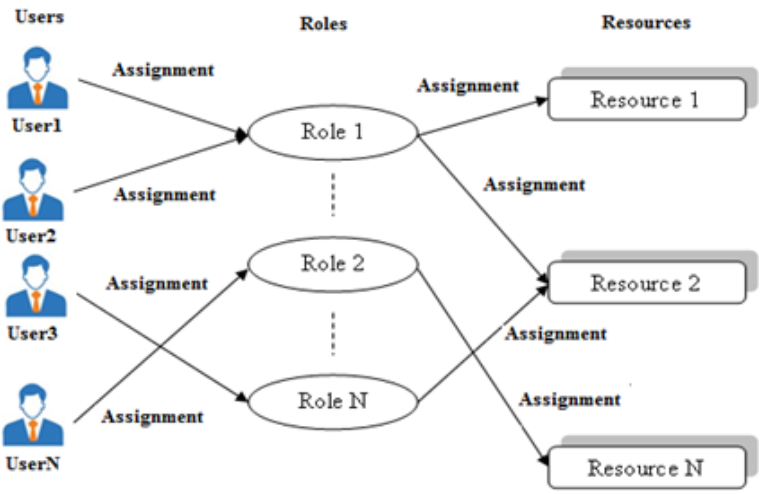
The benefits and limitations of DAC and MAC models are discussed in previous sections. Neither DAC nor MAC model provides an appropriate balance between security and productivity (Hazen, 2003). The National Institute of Standard and Technology (NIST) have started a project to present better administrator model. The solution is proposed in terms of Role based Access Control (RBAC) model by Ferraiolo and Kuhn (1992). Here the access decision is on basis of user's role in the system. The access permissions are granted to a role not to particular user. The users are mapped to roles. The system administrator decides the access permission for a particular role. The access for an object is granted to user only if the user is allowed to perform that role. The concept of RBAC is shown in Figure 4.

The users cannot transfer access permissions assigned to a particular role to which they are mapped to other users. The principle behind RBAC is "a subject's responsibility is more important than whom the subject is mapped" (Laurie, 2009).

The evolution of RBAC model consists of four different models. The $RABC_0$ is the simplest model based on principles of least privileges and separation of duties (Hazen, 2003). In this model access permissions are assigned to the roles directly and it does not use concept of role hierarchy. The next model proposed is $RBAC_1$ that integrates use of hierarchies into $RABC_0$. The distribution of responsibilities at different levels within an organization is considered while assigning the access permissions (Hazen, 2003). The next model $RBAC_2$ is based on the concept of constraints (Hazen, 2003). Here access permissions are granted if certain criteria are met. It does not have the role hierarchies. The $RBAC_3$ is the most detailed model designed by NIST that contains both constraints and hierarchies. Thus, the RBAC model integrates the support for principle of separation of duties, least-privilege, and central administration of role memberships and access controls (Ausanka, 2004). The RBAC model is mostly suitable for enclosed network such as some small organization or enterprise. It fails to meet security requirements of large multi-domain environment such as cloud computing.

Thus, it can be observed that the traditional models cannot be applied directly to the multi-domain environment such as cloud computing the way they exist. Hence there was requirement of secure, efficient access control mechanism that provide fine grained access control for cloud computing. The access control methods based on cryptographic approach are presented in literature to satisfy this demand. The next section discusses different variations of such access control methods.

Figure 4. Role-based access control (RBAC) model



CRYPTOGRAPHIC-APPROACH-BASED ACCESS CONTROL

The major drawback of traditional Public Key Infrastructure (PKI) is the need for exchange of keys while communicating. The third-party key generation center is responsible for issuing and exchange of keys. This process generates extra overhead on system. It is not completely secure as the key generation center can be compromised. It provides the coarse-grained access control. This idea of identity-based encryption (IBE) replaces the traditional PKI system and provides fine grained access control.

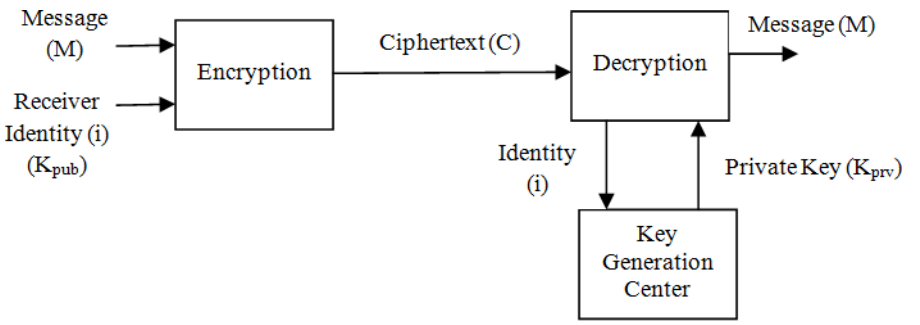
Identity-Based Encryption (IBE)

Identity based Encryption (IBE) scheme is proposed by Shamir (1985). The overall scheme is based on public key cryptography with some differences. The IBE is a cryptographic approach that enables users to communicate without any third-party existence and without any key exchange process. In this scheme the public key is the combination of user's attributes that uniquely identifies the user, e.g. name, address, network address, mobile number, employee id, department, etc. The private key is computed by some Key Generation Center (KGC). This key is available in a smart card and issued to user whenever user joins the network. In this scheme the role of third party i.e. KGC is limited for issuing smart card to all users of network, which contains secret key of the user. The smart card contains various programs for encryption/decryption and programs for signature verification/ generation. If a user "A" wants to send message to other user "B", he can sign the message with the secret key contained in his card and then encrypt it with the receiver's attributes i.e. public key. The user "B" can decrypt the received ciphertext by his secret key embedded in his card and verifies signature using the sender's attributes i.e. public key of user "A."

The KGC must follow some verification process before issuing smart card to any user so that any forgeries or any misrepresentation can be avoided. This process may involve verification of documents related to identity of the user. After doing thorough verification of all necessary documents, the KGC r will issue smart card to user. The overall process of identity-based scheme is depicted in Figure 5. The user's identity (U_i) is used as public key (K_{pub}) and it is used for encryption of message. The secret key (K_{prv}) is generated using some random seed k and a function $f(i,k)$, where i is identity of user. It can be observed from the Figure 5 that any channel for exchange of keys is not required. Every user carries his key in form of smart card.

The IBE scheme overcomes the limitations of traditional PKI system. One of the important features of IBE is that without using PKI it is possible to encrypt the message. Here identities are termed as string of characters. One major flaw associated with the identity-based encryption scheme presented in (Shamir, 1985), is that there is no error-tolerance. Therefore, user's biometrics such as iris scan, fingerprint etc. cannot be used as identities for encryption because biometric measurements are noisy. In order to support error tolerance and biometric identities a Fuzzy Identity Based Encryption scheme is introduced.

Figure 5. Identity-based encryption (IBE)



Fuzzy-Identity-Based Encryption (Fuzzy-IBE)

Fuzzy Identity Based Encryption (Fuzzy-IBE) (Sahai and Waters, 2005) is a variation of IBE with identities as a collection of descriptive attributes. The Fuzzy-IBE scheme supports user's biometric as identities because it has error tolerance property. Thus, user's biometric is used as identity to encrypt a message and it is possible to decrypt the message by same biometric measurement with little difference. In IBE scheme the third party i.e. Key Generation Center (KGC) issues secret key to each user. In order to obtain the key the user has to follow some verification process. The KGC authenticates the user to ensure that the user is one who he/she is claiming. This process may involve verification of some documents or credentials. But this is not clear or robust process as documents are subject to forgery. However, if biometric is used as an identity then there are very less chances of any fraud. Also, the verification process followed by KGC will be more accurate as no one can steal biometric identity of other people. Another benefit of biometric identity is that user can always carry his key along with him wherever he goes.

The fuzzy-IBE scheme gives rise to an application called as Attribute Based Encryption (ABE). The concept of Attribute Based Encryption (ABE) has introduced first time in 2005 (Sahai and Waters, 2005). Attribute Based Encryption (ABE) provides a new paradigm in which access policies are cryptographically embedded in the encryption algorithm. This scheme provides a new way of providing encrypted access control. In the ABE system, the data is not encrypted for a particular user. The ciphertext and private keys both are associated with set of attributes or some access policy over attributes. The user can decrypt the ciphertext only if the associated attributes satisfy the associated access policy. The efficient and collusion resistant Attribute based Encryption scheme is proposed in (Sahai and Waters, 2005). This scheme is also referred as threshold Attribute based Encryption (th- ABE) scheme. For this scheme attributes are selected from a single set and system wide unique threshold value is used. In ABE scheme user can encrypt a message for group of users having same attributes. For example, consider that faculty wants to send some message to all students registered for course "Database" and department "Computer". The faculty can encrypt the message to identity as {"Database", "Computer"}. Any student who has identity, which contains all these attributes, can decrypt the message. Thus, in this scheme identities are considered as set of descriptive attributes that user possesses. The private key comprises set of private key components of each attribute.

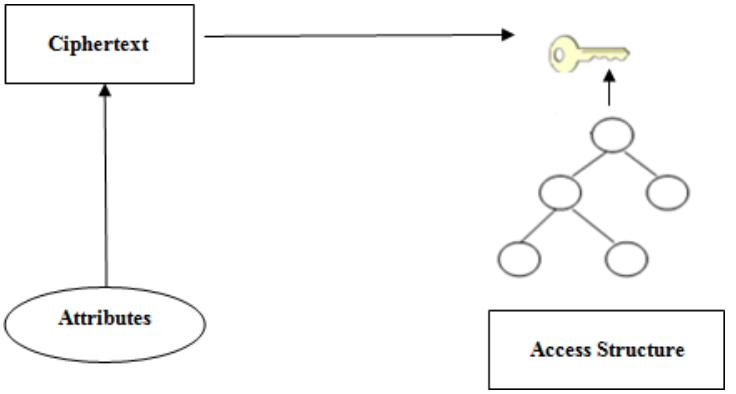
The fuzzy-ABE scheme adds error tolerance to the Identity based Encryption system and also supports biometric identities. But the scheme is not much expressive to be applied for general systems. The decryption process is very expensive as it requires *(d-1)* pairing operations where *d* is threshold value. Nail et al. (2005) have presented a new threshold Attribute based Encryption scheme. The main objective of this scheme is to define more flexible and computationally efficient Threshold-Attribute based Encryption (new th-ABE) scheme. The scheme is also resistant to collusion attack. The new th-ABE scheme allows user to select attributes from multiple sets and also allow different threshold values associated with the sets. The decryption process requires only two pairing operations that are very less as compared to scheme presented in (Sahai and Waters, 2005). Hence the new th-ABE scheme is computationally efficient. The scheme can be applied to any practical biometric based cryptographic access control.

The Attribute based Encryption (ABE) scheme presented by Sahai and Waters (2005) is not expressive enough to apply to large systems. Further in literature two major flavors of ABE system are presented such as Key-Policy based ABE (KP-ABE) and Ciphertext Policy based ABE (CP-ABE). The following subsections describe these schemes in depth.

Key-Policy-Attribute-Based Encryption (KP-ABE)

The Key Policy based ABE (KP-ABE) scheme is first time presented by Goyal et al. (2006). In this scheme the set of descriptive attributes are related with the ciphertext and access structure is related with private key. The access structure specifies which type of ciphertext the key can decrypt (Goyal et al., 2006). A tree-based access structure is used where attributes are present at leaves. The intermediate

Figure 6. KP-ABE scheme



nodes consist of AND or OR gates. A user can decrypt the ciphertext if the access structure associated with key is satisfied by the attributes associated with ciphertext. Figure 6 shows the KP-ABE scheme.

The private key consists of set of elements and every element corresponds to an associated attribute. The elements from single set can be used to satisfy the access policy in order to avoid the collusion attack.

Access Structure

Consider T is tree that represents an access policy. In this tree each intermediate node is threshold gate. The children nodes and a threshold value are associated with this node. Consider any node n_l of tree which has *m* children. The threshold value is denoted by K_{nl}. Then the following is true for the threshold value:

$$0 < K_{n1} \leq m$$

If it is OR gate then the threshold value will be K_{nl} =1. And if it is AND gate then the threshold value will be K_{nl}=2. The leaf nodes describe the attributes and their threshold value will be K_{nl} =1. The function *parent* (n_l) is used to denote the parent of node n_l. The function *atr*(n_l) is associated only with leaf node to denote its attribute. The nodes are numbered in the access tree. The function *index*(n_l) is used to find the number assigned to the node.

Satisfying the Access Tree

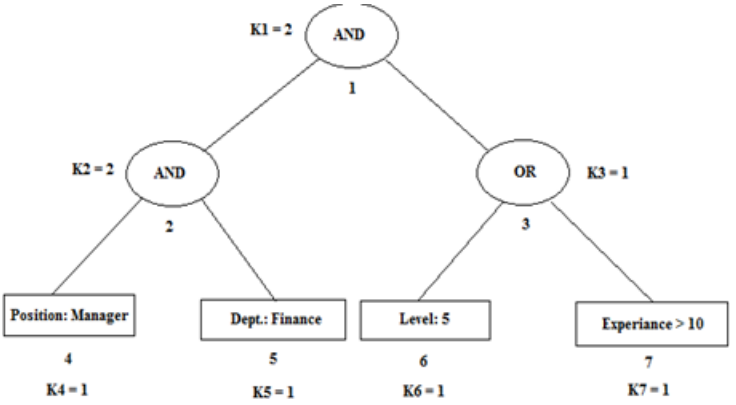
Consider that T_R is an access tree with root node as R. Let *S* be the set of attributes. The set *S* satisfies the access structure given by T_R if and only if T_R (S) = 1.

T_{n1} (S) for every node *n1* is computed recursively in following way.

If n1 is a leaf node then T_{n1} (S)=1 if atr(n1) ϵ S. If n1 is a non leaf node then compute T_x (S) for all children x of n1. T_x (S) =1 if at least K_x children return 1. Let us consider the example depicted in Figure 7. The example consists of set of attributes S as: S={Position: Manager, Department: Finance, level:5}.

Each node has assigned a unique number as shown in access tree. The respective threshold values of each node are also given in the access tree. Consider the access policy as: ((manager AND Finance) OR level 5). In order to satisfy this policy, we call the function T_x (S) for every node *x* recursively in following way:

Figure 7. Example of access structure



T_4 (S) =1 because node 4 is a leaf node and atr(4)= "manager" ϵ S

In similar way, T_5 (S) =1 because node 5 is a leaf node and atr(5)= "finance" ϵ S. Now consider node 2, the threshold value of node 2 is 2 as it is AND gate. T_2 (S) will return 1 only if at least its 2 children return 1. As node 4 and 5 both return 1, T_2 (S) =1. In same way we can compute: T_6 (S)=1 because node 6 is a leaf node and atr(6)= "5" ϵ S. T_7 (S)=0 because node 7 is a leaf node and atr(7)= ">10" does not belongs to set S. Now for node 3, its threshold value is 1 as it is an OR gate. T_3 (S) will return 1 only if at least one of its children returns 1. As node 6 returns 1, T_3 (S) = 1. Finally, T_1 (S)=1 as it is AND gate and both of its children return 1. In this way the access tree is processed in order to satisfy the given policy.

Variations of KP-ABE Schemes

There exist several other variations of KP-ABE scheme in literature. One of the schemes is proposed by Ostrovsky et al. (2007) that is based on non-monotone access structure. The threshold ABE (th-ABE) scheme presented in (Sahai and Waters, 2005) is less expressive as it only supports threshold policies. The more expressive ABE system is presented by Goyal et al. in (Goyal et al., 2006), which uses monotone access formula with AND, OR and threshold gates. Although the system presented in (Goyal et al., 2006) is more expressive, one limitation associated with the scheme is the negative constraints in access formula are not supported. In order to address this limitation Ostrovsky et al. (2007) presents a new ABE scheme with non-monotone access structure including AND, OR, NOT and threshold gates. This system uses concept of broadcast revocation (Naor and Pinkas, 2000) to support non-monotone access structure and negative constraints. The system also preserves collusion resistance property of ABE scheme.

The scheme presented by Ostrovsky et al. (2007) is more expressive but incurs overhead for encryption and decryption. Also, the size of ciphertext and private key is doubled (Pang et al., 2014). The issue is addressed by Lewoko et al. (2010) and produced an efficient non-monotonic KP-ABE scheme with small key size. This scheme is based on the user revocation system. The other variation presented in (Attrapadung et.al. 2011) is non-monotonic access structure based KP-ABE scheme. This scheme is selectively secure and is based on the Identity based Broadcast Encryption system (IBBE) (Boneh and Hamburg, 2008). This scheme supports constant ciphertext size with expressive access structure. Also the Identity based Revocation (Lewoko et al., 2010) has been revised to support O(1) of ciphertext size, which in turn produces more efficient KP-ABE system with monotonic access structure and short ciphertext size.

In the KP-ABE scheme the access structure is embedded in user's private key and set of attributes are related with the ciphertext. Therefore, the user's private key can decide which data can be decrypted by it. However, there is no control over which user can decrypt a particular ciphertext. This fact is serious disadvantage of the KP-ABE scheme. In order to tackle this issue a Ciphertext Policy Attribute based Encryption scheme is proposed by Bethencourt et al. (2007).

Ciphertext-Policy-Based ABE (CP-ABE)

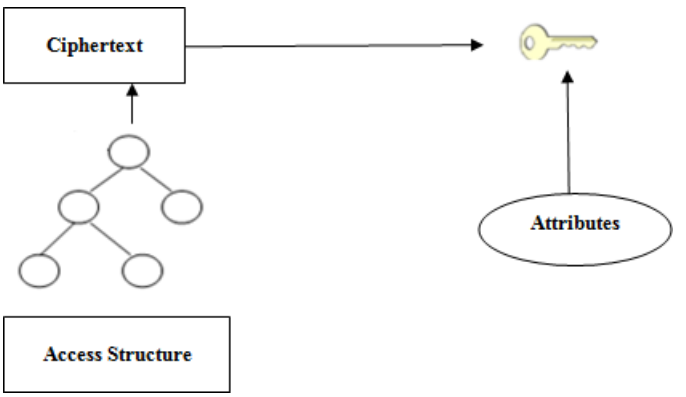
Bethencourt et al. (2007) have proposed the first implementation of Ciphertext Policy based ABE scheme. In this CP-ABE scheme, the access policy is embedded in cipher-text and set of attributes are bounded with the keys. The user can decrypt the ciphertext only if attributes associated with the private key satisfy the access policy associated with the ciphertext. The access structure is specified using monotonic access tree. The intermediate nodes of such trees are threshold gates. The attributes are presented at leaves. The nodes can be presented using "AND" and "OR" gates. The construction of AND and OR gates is based on *n-of-n* threshold gates and 1-of-n threshold gates respectively. The access structure and the process of satisfying access structure are similar to KP-ABE scheme. The Figure 8 presents the basic CP-ABE scheme.

Variations of CP-ABE Scheme

The scheme presented by Bethencourt et al. (2007) is one of the most efficient CP-ABE systems presented in literature. But the scheme also has some limitation. In the current CP-ABE scheme users can use attributes organized in a single set. All possible combinations of attributes from the single set are used to satisfy the access policies. Due to this feature it is not possible to specify policies using compound attributes. The compound attributes are those attributes which are built from other singleton attributes. Also the current CP-ABE scheme allows numerical value assignment for attributes but only single value can be assigned. But in real life scenarios it is necessary to assign multiple values to user attributes. For example, student enrolling for multiple courses, customer holding multiple bank accounts etc. The multiple values assignment adds flexibility in the specification of access policy.

The Attribute Set Based Encryption (ASBE) (Bobba et al., 2009) scheme is designed to overcome above mentioned limitations of existing CP-ABE scheme. The ASBE is the extension of CP-ABE scheme. In this scheme the attributes are organized into a recursive set structure. While designing access policy attributes from same set can be combined easily. Also, this scheme allows combining attributes from different sets with the use of translating nodes. At the same time the access policies are framed in such a way that the decryption key can use attributes belonging to same set. This scheme supports the compound attributes in the specification of policies. It also allows multiple values

Figure 8. CP-ABE scheme



assignment for an attribute. Therefore, it is possible to assign multiple values to same attributes in different sets. At the time of decryption, the user is restricted to combine attributes from same set to prevent the collusion attack. In the basic CP-ABE system the key revocation was not efficient (Bobba et al., 2009). The system in (Bethencourt et al., 2007) uses the concept of expiration date for keys, which has some limitations. Whenever the validity of the key is expired the entire key needs to be regenerated and redistribute. This process put overhead on the overall system. The CP-ASBE (Bobba et al., 2009) scheme solves this problem by following a new approach, where the new value of expiration time is added to the existing key. So, there is no need to regenerate the entire key and redistribute it into the system. Thus, the CP-ASBE scheme presented in (Bobba et al., 2009) supports compound attributes, numerical attributes with multiple values, efficient key revocation mechanism and collusion resistance.

The CP-ABE schemes discussed above are based on secret sharing construction. Cheung and Newport in (Cheung and Newport, 2007) have presented CP-ABE scheme based on chosen plaintext secure construction under the Decisional Bilinear Diffie-Hellman (DBDH) assumption (Boneh et al., 2006). The scheme involves access structure based on AND gates on positive and negative attributes. The authors in (Cheung and Newport, 2007) have also presented a scheme that is chosen ciphertext (CCA) secure. For that purpose, the Canetti-Halevi-Katz (Canetti et al., 2004) technique is applied and concept of one-time signature is used. The scheme organizes the attributes in logical hierarchies. Due to the hierarchy the efficiency of encryption and decryption process is improved. Thus, the size of ciphertext, the number of exponentiations in encryption and the number of pairing operations in decryption are reduced. The drawback of scheme in (Cheung and Newport, 2007) is that it is limited to AND gate and allows fixed number of system attributes. Hence the scheme becomes less expressive. Goyal et al. (2008) have presented an approach to transform KP-ABE system to CP-ABE system. The authors have applied the concept of universal access tree and accommodate the general access formula of size *n*. The scheme represents first feasible expressive CP-ABE system. At the same time the ciphertext size, private size, and encryption and decryption complexity has increased by $n^{3.42}$ factor. In order to overcome these limitations, Waters have proposed a CP-ABE system with general access structure (Waters, 2011). The scheme reduces the ciphertext size and encryption overhead. If n is the size of access formula, then the encryption time scale with O(n) where and decryption time scales with the number of nodes. Dazza et al. (2008) has presented a scheme with extended access structure that uses a set of dummy players along with the existing set of real players. The scheme is applicable for CP-ABE system. The CP-ABE construction following this approach has general access structure and uses dummy attributes. The advantage of such approach is that it reduces the ciphertext size.

The CP-ABE scheme with constant size ciphertext and constant number of pairing operations is proposed by Emura et al. (2009). In most of the existing CP-ABE schemes the size of ciphertext depends on the number of attributes in access structure. The authors in (Emura et al., 2009) have proposed first time a CP-ABE scheme with constant ciphertext size that uses a conversion method presented in (Cheung and Newport, 2007). The access structure of this scheme supports AND gate and multi-valued attributes. The scheme is also secure against chosen plaintext attack and chosen ciphertext attack (Emura et al., 2009). Though the scheme presented by Emura et al. (2009) achieves short ciphertext, the scheme only supports (s,s)-threshold decryption policies with *s* number of attributes. This fact limits the expressibility of the scheme. A more expressive CP-ABE scheme with constant ciphertext size is proposed by Javier Herranz et al. (Herranz et al., 2010). The construction of the system is based on the dynamic threshold encryption scheme presented in (Delerablee and Pointcheval, 2008) that produces constant size ciphertext. But the scheme in (Delerablee and Pointcheval, 2008) does support the collusion resistance property. Therefore Herranz et al. (2010) have modified the scheme and constructed a CP-ABE scheme with collusion resistance property and constant size ciphertext. The scheme uses threshold policies. The set of attributes and threshold value are selected at encryption time by sender. The users holding at-least threshold of the all attributes can only decrypt the ciphertext.

There are some ABE systems presented in literature that yield constant ciphertext size, but they support estricted access structure. The ABE system presented by Attrapadung et.al in (Attrapadung et al., 2011) supports constant ciphertext size with expressive access structure. The authors in (Attrapadung et al., 2011) devised CP-ABE scheme with threshold access policy supporting O(1) ciphertext size. The second scheme presented in (Attrapadung et al., 2011) is monotonic access structure based KP-ABE scheme. Another effort to produce ABE system with short ciphertext is presented in (Zhou and Huang, 2010). In this paper a constant size CP-ABE scheme (CCP-ABE) is proposed with AND gate access policy and constant size ciphertext. On basis of the CCP-ABE scheme the more expressive and efficient Attribute based Broadcast Encryption (ABBE) system is presented in (Zhou and Huang, 2010).

Many of the existing ABE schemes suffer from efficiency drawback such as large ciphertext size and computation overhead that limits its applicability in real world. A CP-ABE scheme with constant ciphertext size and computation cost is presented by Zhang et al. (Zhang et al., 2014). The scheme supports AND-gate access policies along with multiple attribute values and wildcards. Most of the CP-ABE schemes designed with the aim of producing constant length ciphertext are based on selectively secure mechanism. Indeed, a fully secure CP-ABE scheme with constant ciphertext size is proposed by Doshi and Jinwala (2014). Many of the CP-ABE schemes focus on the short ciphertext or full security proofs. The exception is the scheme presented by Guo et al. (2014), which addresses the issue of decryption key size. Generally, the length of the key is dependent on the number of attributes. Therefore CP-ABE schemes are not efficiently applied for lightweight devices with storage constraints. Guo et al. (2014) have proposed a provably secure CP-ABE scheme with short decryption keys applicable for lightweight devices. The CP-ABE schemes available in literature either support constant ciphertext size or constant decryption key size. If both are provided, then the scheme is not expressive enough. Thus, the open research issue is to have an expressive CP-ABE scheme with both constant ciphertext size and constant decryption key size. In order to satisfy this demand, Odelu et al. (2016) have proposed provably secure, an expressive CP-ABE scheme with constant ciphertext size and constant decryption key size.

The data stored on cloud must be accessible to user at any time and from anywhere. Therefore, encryption scheme must provide high performance. In order to improve the flexibility and scalability the delegation mechanism in key generation is required (Wang et al., 2010). The existing CP-ABE scheme generates heavy computation for user revocation process; hence some efficient and scalable revocation scheme is required. The solution is provided in terms of the Hierarchical Attribute Based Encryption (HABE) scheme proposed by Wang et al. (2010).

Hierarchical-Attribute-Based Encryption (HABE)

The Hierarchical Attribute Based Encryption (HABE) (Wang et al., 2010) scheme is extension of CP-ABE scheme (Bethencourt et al., 2007) with hierarchical structure. The objective of this scheme is to provide fine grained access control mechanism to share data with flexibility, efficiency and high performance. The HABE scheme is actually a combination of Hierarchical Identity based Encryption (HIBE) (Gentry and Silverberg, 2002) and Ciphertext Attribute Based Encryption (CP-ABE) (Bethencourt et al., 2007). The scheme has the hierarchical model, where users are organized into some hierarchical structure.

The HABE system uses Proxy re-encryption and lazy re-encryption scheme for revocation. This scheme associates version number with each attribute a. This version number is incremented each time the user associated with a is revoked. Thus, the HABE scheme provides fine-grained access control mechanism, with features like; high performance, scalable, collusion resistant and full delegation (Wang et al., 2010).

Hierarchical-Attribute-Set-Based Encryption (HASBE)

The HABE scheme presented in (Wang et al., 2010) provides fine grained access control mechanism. The scheme is scalable and also collusion resistant. The HABE scheme uses disjunctive normal form policy and all attributes in one conjunctive clause are administered by same domain masters (Wan et al., 2012). Hence it is possible that the multiple domain masters administer the same attribute. Therefore, it is very difficult to implement practically. The HABE scheme is extension of CP-ABE scheme, so it has similar drawbacks as of CP-ABE scheme. The scheme does not support compound attributes and multiple value assignments. Wan et.al has presented the Hierarchical Attribute Set Based Encryption (HASBE) scheme in (Wan et al., 2012), which is extension of CP- ASBE scheme with hierarchical user structure. The major objective is to provide high performance, flexible, scalable and fine-grained access control. Thus, the HASBE scheme extends ASBE scheme by inclusion of hierarchical structure of users. The HASBE scheme realizes various features such as fine-grained access control, scalable, flexible, efficient user revocation and expressive.

Outsourcing-Based ABE Scheme

The most important drawback of ABE schemes presented in previous sections is that the decryption process is very expensive due to the pairing operations required to decrypt the ciphertext. As the complexity of access structure increases the number of pairing operations required for decryption also increases (Green et al., 2011). One of the efficiency drawbacks of ABE schemes is size of ciphertext and time required for decryption grows linearly with the complexity of access structure (Green et al., 2011). The question is whether cloud services can be used to outsource decryption process in ABE system. The simple approach is to hand over secret key to cloud service then that could decrypt the ABE ciphertext for the user. However, in this case the outsourcing service must be trustworthy because once it gets the secret key, the service can decrypt any message intended for that user (Green et al., 2011). Another solution is to use Gentry's fully Homo-morphic encryption (Gentry, 2009) system for outsourcing the decryption in ABE system. Similar approach is implemented in (Gennaro et al., 2010; Chung et al., 2010). Here outsourcing of general computation can be done and the privacy of input is preserved. Therefore, the message and the key remain secret. The limitation of this system is the large computation overhead that is impractical.

The technique based on outsourcing of pairing operations is proposed in (Benoit et al., 2010). Here user can securely outsource the pairing operations to the third-party server. This scheme lacks in minimizing the computation overhead of the user as every pairing operation trigger four pairing operations for server. Thus, the overhead increases in a factor of at least four as compared to original decryption algorithm (Benoit et al., 2010). The other issue is the bandwidth requirements of user also get increased. In order to tackle all these limitations, the system for outsourcing decryption of ABE ciphertext is proposed by Green et al. (2011). In this scheme the ciphertext is stored in the cloud. A cloud uses a single transformation Key (TK) to translate the ABE ciphertext into Elgmal style (El Gamal, 1984) small ciphertext. During the transformation the cloud cannot read anything from the ciphertext. Thus, the scheme reduces overhead of decryption for users.

The major change the system has done in the key generation algorithm. The new key generation algorithm generates one Elgmal type (El Gamal, 1984) short secret key (SK) and one transformation Key (TK). The transformation key is shared with the server, which will do the decryption for ABE ciphertext. The server then transforms the received ABE ciphertext (CT), which satisfies user's attributes into simple and short Elgamal ciphertext (CT') using the transformation key (TK). The server transmits the CT to user. Now, user requires only one simple exponentiation operation to decrypt the received CT' using SK. The computation overhead for server is less than the original decryption algorithm. The scheme is also secure against malicious server. The CP-ABE scheme with modified key generation algorithm is implemented in this paper. The respective changes are also done in the part of libfence library (Green et al.). The monotone access structure is used by the system.

The KP-ABE scheme is also implemented in same way; just the role of access structure and set of attributes is reversed. The similar five algorithms are used to implement the scheme. The system has following advantages: The time required for decryption of ABE ciphertext with 100 attributes with original decryption algorithm took 30 seconds on a mobile device. Whereas the outsourcing based ABE (Green et al., 2011) system requires 60 milliseconds on a same device. In this system the complex pairing operations are pushed to server. Therefore, the size of code remaining on client's machine is very small. Henceaq the size of trusted codebase is decreased.

Variations of OABE Scheme

The aim of the scheme presented in (Green et al., 2011) is to outsource the decryption of the ABE ciphertext. The authors in (Zhou and Huang, 2011) have proposed the privacy preserving CP-ABE scheme for outsourcing the encryption and decryption to the third-party servers. The enhancement to the scheme presented in (Zhou and Huang, 2011) is proposed by Li et al. (2012). The work in Li et al. (2012) presents a novel approach for outsourcing encryption of ABE system. Here the two-leveled Map-reduce paradigm (Dean and Ghemawat, 2008) is used to construct a partial ciphertext. The encryption algorithm at user's node generates partially encrypted ciphertext (CT_u) and set of encryption keys for outsourcing. Then the delegated encryption algorithm at Map-reduce node will take these outsourcing encryption keys and attribute set or access structure and generates partially encrypted ciphertext (CT_{MR}) (Li et al., 2012). In order to improve the work (Zhou and Huang, 2011), the scheme (Li et al., 2012) uses trivial policy. The generic tree-based access policy can be utilized by the scheme.

Along with expensive decryption, another challenge for ABE system is the complex key issuing process. The generation of use's secret keys also requires large amount of modular exponentiation in ABE system (Li et al., 2013). In order to address this challenge, Li et al. (2013) have proposed a scheme for outsourcing key issuing and decryption simultaneously, in ABE system. The scheme uses two cloud service providers (CSP), as key generation cloud service provider (KG-CSP) and decryption cloud service provider (D-CSP). So, the two CSPs will perform the expensive tasks of key issuing and decryption respectively. Thus, the scheme reduces overhead from both user's side and attribute authority side. The outsourcing scheme discussed above guarantees the security of ciphertext i.e. the server cannot read anything from ciphertext while transformation process. But theses scheme does not provide any mechanism to verify correctness of transformation done by the server (Lai et al. 2013). It is possible that, to save computation cost the server may return previously transformed ciphertext to the user. Another possibility is, due to some malicious attack the server may perform incorrect transformation. Lai et al. (2013) presents ABE with verifiable outsourced decryption for ABE system without random oracle. The scheme is enhancement of the work presented by Green et al. (2011), by inclusion of verifiability concept. The original ciphertext is included into the input of function, $Decrypt_{out}$ presented in Green et al. (2011). Therefore, it is possible to utilize some part of original ciphertext to verify correctness of the transformation done by server. The scheme appends redundancy with ciphertext to verify the correctness.

The scheme in Lai et al. (2013) provides mechanism for outsourced decryption, whereas the concept of outsourced key-issuing is not considered. The ABE scheme with outsourced decryption and outsourced key issuing along with chekability concept is presented by Li et al. (2014). Similar to the scheme presented in Li et al. (2013), this scheme also uses Key Generation Service Provider (KGSP) and Decryption Service Provider (DSP). The generation of partial private keys for user's policy is delegated to KGSP. By using the concept of blinding key, the DSP performs the decryption of ciphertext and output partial ciphertext. The concept of ringer (Golle and Mironov, 2001) and appending redundancy is used for checking the correctness of computation done by KGSP and DSP (Li et al., 2014). The techniques presented by Lai et al. (2013), Li et al. (2012, 2013, 2014) present outsourced decryption, encryption and key issuing mechanism for ABE system based on tree access

structure. They do not support linear secret sharing scheme (LSSS) (Zhang et al, 2016). Also, these schemes are not suitable for small devices, as additional communication cost is introduced.

Thus, there is need of such an OABE scheme that is secure, provides outsourced encryption, decryption, key issuing simultaneously and also efficient in terms of bandwidth utilization. Zhang et al. (2016) presents a secure fully Outsourced ABE (FOABE) scheme, to solve above mentioned challenge. The scheme provides outsourced encryption, decryption and key issuing simultaneously. Also, the scheme improves communication cost. The system in Zhang et al. (2016) uses concept of two service providers namely Key Generation Service Provider (KGSP) and Encryption Service Provider (ESP). The KGSP generates intermediate secrete keys and the ESP performs the computation of partial encryption. The KGSP and users can communicate offline hence the communication cost is minimized (Zhang et al., 2016). The blinding key concept is used to perform secure outsourced decryption.

COMPARISON OF THE SCHEMES

In this section we present the comparison of the schemes based on different criteria. The comparison of different variations of KP-ABE scheme is presented in Table 1. The schemes are compared with respect to their access structure, access policy, security model, assumption, expressiveness, size of key and ciphertext.

In the similar way the comparative analysis of different CP-ABE schemes is presented in Table 2.

Finally the different OABE schemes are compared with respect to multiple parameters as shown in Table 3.

CONCLUSION

The main objective of access control mechanism is to ensure that the data is accessed by authorized users only. Firstly the paper discusses the traditional access control models that include DAC, MAC and RBAC. These models cannot be applied to cloud computing in the form they exist presently. Hence the concept of Attribute based Encryption is introduced to provide access control in cloud computing in more efficient way. The Attribute based Encryption (ABE) system provides a new notion of encrypted access control mechanism for cloud computing. The base of ABE systems is the

Table 1. Comparative analysis of variations of KP-ABE scheme

Criteria\Scheme	Sahai and Waters (2005)	Goyal et al. (2006)	Ostrovsky et al. (2007)	Lewoko et al. (2010)	Attrapadung et al., 2011)
Access Structure	Monotonic	Monotonic	Non-Monotonic	Non- Monotonic	Non- Monotonic /Monotonic
Access Policy	Threshold	Threshold, AND, OR	Threshold, AND, OR, NOT	LSSS	LSSS
Expressiveness	Less	More	More	More	More
Key length growth	Linear	Linear	Linear	Constant	Linear
Ciphertext size growth	Linear	Linear	Linear	Linear	Constant
Security Model	SS	SS	SS	SS	SS
Algorithm/ Assumption	DBDH	DBDH	DBDH	DBDH	DBDH

Table 2. Comparative analysis of variations of CP-ABE scheme

Criteria\ Scheme	Access Policy	Access Structure	Key Length Growth	Ciphertext Size Growth	Algorithm/ Assumption	Security Model	Remark
Bethencourt et al., 2007	AND, OR, Threshold	Tree	Linear	Linear	DBDH	Adaptive	Large computation overhead due to pairing operations
Cheung and Newport, 2007	AND, NOT	AND gate between two-value attributes	Linear	Reduced CT size	DBDH	SS/ CPA secure	Reducing Ciphertext size and encryption/ decryption time
Emura et al., 2009	(s-s) Threshold	AND gate among multi-valued attributes	Linear	Constant	DBDH	SS	Less expressive
Herranz et al. 2010	Threshold	General	Linear	Constant	aMSE-DDH	SS	Reasonably expressive decryption policy with constant ciphertext size.
Zhou and Huang, 2010	AND	General	Linear	Constant	BDHE	SS	Constant ciphertext size and more efficient ABE broadcast encryption scheme.
Waters, 20011	(s-s) Threshold	LSSS	Linear	Constant	PBDHE	SS	Reduces the ciphertext size and encryption overhead
Attrapadung et.al. 2011)	Threshold	Monotonic access structure	Linear	Constant	DBDH	SS	constant ciphertext size and more expressive
Zhang et al., 2014	AND	AND gate among multi-valued attributes & wildcard	Linear	Constant	*n*- BDHE	SS	constant ciphertext size and computation cost
Doshi and Jinwala (2014).	AND	AND gate among multi-valued attributes	Linear	Constant	DBDH	FS	Fully secure and constant ciphertext size
Guo et al., 2014	AND	General	Constant	Linear	DBDH	SS	Short decryption keys applicable for lightweight devices. also more expressive
Odelu et al. (2016)	AND	General	Constant	Constant	aMSE- DDH	SS	Supports both constant size ciphertext and constant size secret keys

DBDH: Decisional Bilinear Diffe-Hellman; aMSE- DDH: augmented multi-sequence of exponents decisional Diffe- Hellman; PBDHE: Parallel Bilinear Diffe-Hellman Exponent, *n*-BDHE: *n*-Bilinear Diffe-Hellman Exponent; BDHE: Bilinear Diffe-Hellman Exponent assumption; LSSS: Linear Secret Sharing Scheme.

Identity based Encryption (IBE) system. The different ABE schemes such as Fuzzy- ABE, CP-ABE, KP-ABE, HABE and OABE are reviewed in this paper. In these schemes the access is granted to user only if his/her attributes satisfy the access structure. The schemes mainly differ in the access structure and access policy. The important property of all these schemes is that they are collusion resistant, so that two users cannot combine their attributes to decrypt the ciphertext. On basis of the comparison presented in this paper following points are observed.

Table 3. Comparison of OABE schemes

Criteria\Scheme	Outsourced Operation	CPABE/ KPABE	Access Structure	Verifiability	Constant Ciphertext	Remark
Green et al., 2011	Decryption	CPABE, KPABE	Tree	No	No	Only decryption is outsourced
Zhou & Hang, 2011	Encryption & Decryption	CPABE	Tree	No	NO	Provides outsourced encryption also but still generates overhead.
Li et al., 2012	Encryption	CPABE, KPABE	Tree	No	No	Extension of Zhou & Hang, 2011based on map reduce model
Li et al. 2013	key issuing & Decryption	CPABE, KPABE	Tree	No	No	Reduces overhead from both user's side and attribute authority side.
Lai et al., 2013	Decryption	CPABE	Tree	Yes	No	Produces redundancy
Li et al., 2014	key issuing & Decryption	CPABE, KPABE	Tree	Yes	No	Provides check ability mechanism
Zhang et al. 2016	Encryption, Decryption & key issuing	CP-ABE	LSSS	No	No	Reduced communication cost

The basic drawback of KP-ABE scheme is that there is no control over who can decrypt the particular ciphertext. This shortcoming is overcome by the CP-ABE, which associate access structure to the ciphertext and attributes to the key. After in the literature many KP-ABE schemes are presented with non-monotone access structure and constant ciphertext size, to improve the performance. The lots of variations of CP-ABE schemes are available. In order to provide more efficient scheme some CP-ABE systems with fully secure model and constant ciphertext size and key size are developed.

One of the variations of ABE scheme is the HABE scheme where the users are organized into some hierarchical structure. This scheme generated more flexible and scalable ABE systems. Though many expressive and efficient CP-ABE systems are developed, the computation overhead of these schemes is quite large. This issue can be tackled by outsourcing some of the computation to trusted third party servers. There are several OABE systems developed, in which either the encryption or decryption operation is outsourced to the third-party server. Some of systems also outsource the key issuing operation. In order to ensure the correctness of computation done by the third-party server, the verifiability mechanism is introduced.

Thus, many ABE schemes are presented in literature that provides fine grained access control in cloud computing. There are some issues that can be addressed in future, such as fully outsourced ABE system with more functionality like user revocation, user accountability, policy update and constant ciphertext and key size.

REFERENCES

Ali, M., Khan, S. U., & Vasilakos, A. V. (2015). Security in cloud computing: Opportunities and challenges. *Inf. Sci.*, *305*, 357–383. doi:10.1016/j.ins.2015.01.025

Armbrust, J., Fox, A., Grith, R., Joseph, A. D., Katz, R., Konwinski, A., & Stoica, I. et al. (2010). A view of cloud computing. *Communications of the ACM*, *53*(4), 50–58. doi:10.1145/1721654.1721672

Attrapadung, M., Libert, B., & DePanafieu, E. (2011). Expressive Key-Policy Attribute based Encryption with Constant-Size Ciphertexts. In Public Key Cryptography-PKC 2011 (pp. 90–108). Springer.

Ausanka-Crues, R., & Mudd, H. S. (2004). Methods for Access Control: Advances and Limitations. Harvey Mudd College. Retrieved from http://www.cs.hmc.edu/wmike/public_html/courses/security/s06/projects/ryan.pdf

Bell, D., & LaPadula, L. (1973). Secure Computer Systems: Mathematical Foundations. *MITRE*. Retrieved from http://www-personal.umich.edu/~cja/LPS12b/refs/belllapadula1.pdf

Benoit, C., Coron, J., McCullagh, N., Naccache, D., & Scott, M. (2010). Secure delegation of elliptic-curve pairing. In *Proceedings of the International Conference on Smart Card Research and Advanced Applications* (pp. 24–35). Academic Press.

Bethencourt, J., Sahai, A., & Waters, B. (2007). Ciphertext-Policy Attribute based Encryption. In *Proceedings of the IEEE Symposium on Security and Privacy*. Academic Press.

Biba, K. (1977). Integrity Considerations for Secure Computer Systems. Retrieved from http://oai.dtic.mil/oai/oai?verb1/4getRecord&metadataPrefix1/4html&identifier1/4ADA039324

Bobba, R., Khurana, H., & Prabhakaran, M. (2009). Attribute Sets: A Practically Motivated Enhancement to Attribute based Encryption. In *Proceedings ESORICS*, Saint Malo, France. Academic Press. doi:10.1007/978-3-642-04444-1_36

Boneh, C., Shen, E., & Waters, B. (2006). Strongly Unforgeable Signatures based On Computational Diffie-Hellman. In *Proceedings of PKC* (pp. 229–240). Academic Press. doi:10.1007/11745853_15

Boneh, D., & Hamburg, M. (2008). Generalized Identity Based and Broadcast Encryption Schemes. In *ASIACRYPT 2008. 5350* (pp. 455–470). Springer. doi:10.1007/978-3-540-89255-7_28

Canetti, R., Halevi, S., & Katz, J. (2004). Chosen Ciphertext Security from Identity based Encryption. In Advances in Cryptology – Eurocrypt (pp. 207–222). Academic Press. doi:10.1007/978-3-540-24676-3_13

Cheung, J., & Newport, C. (2007). Provably Secure Ciphertext Policy abe. In *Proceedings of the 14th ACM Conference on Computer and Communications Security* (pp. 456–465). ACM.

Chung, K., Yael, K., & Salil, P. V. (2010). Improved Delegation of Computation using Fully Homomorphic Encryption. In *Proceedings of the Annual Cryptology Conference Advances in Cryptology – CRYPTO 2010* (pp. 483–501). Academic Press. doi:10.1007/978-3-642-14623-7_26

Daza, V., Herranz, J., Morillo, P., & Rafols, C. (2008). Extended Access Structures and Their Cryptographic Applications. *Journal of IACR Cryptology ePrint Archive*, 1-25.

Dean, J., & Ghemawat, S. (2008). Mapreduce: Simplified Data Processing on Large Clusters. *ACM Communications*, *51*(1), 107–113. doi:10.1145/1327452.1327492

Delerablee, A., & Pointcheval, D. (2008). Dynamic Threshold Public Key Encryption. In *Proceedings of Crypto'08* (pp. 317–334). Springer-Verlag.

Doshi, N., & Jinwala, D. C. (2014). Fully secure ciphertext policy attribute based encryption with constant length ciphertext and faster decryption. *Security and Communication Networks*, *7*(11), 1988–2002. doi:10.1002/sec.913

El Gamal, T. (1984). A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms. *IEEE Transactions on Information Theory*, *31*(4), 10–18.

Emura, J., Miyaji, A., Nomura, A., Omote, K., & Sosh, M. (2009). A Ciphertext-Policy Attribute based Encryption Scheme with Constant Ciphertext Length. In *Proceedings of ISPEC'09* (pp. 13-23). Springer-Verlag. doi:10.1007/978-3-642-00843-6_2

Ferraiolo, D., & Kuhn, R. (1992). Role based Access Control. In *Proceedings of 15th National Computer Security Conference* (pp. 554-563). Academic Press.

Gennaro, R., Gentry, C., & Parno, B. (2010). Non-interactive Verifiable Computing: Outsourcing computation to Untrusted Workers. In *Proceedings of the Annual Cryptology Conference on Advances in Cryptology – CRYPTO 2010* (pp. 465–482). Springer. doi:10.1007/978-3-642-14623-7_25

Gentry, C. (2009, May). Fully homomorphic encryption using ideal lattices. In Stoc (Vol. 9, No. 2009, pp. 169-178).

Gentry, C., & Silverberg, A. (2002). Hierarchical ID-Based Cryptography. In *Proceedings of ASIACRYPT* (pp. 548- 566). Academic Press.

Golle, P., & Mironov, I. (2001). Uncheatable Distributed Computations. In *Proceedings of the 2001 Conference on Topics in Cryptology: The Cryptographer's Track at RSA* (pp. 425-440). Academic Press. doi:10.1007/3-540-45353-9_31

Goyal, V., Jain, A., Pandey, O., & Sahai, A. (2008). Bounded ciphertext policy attribute-based encryption. In *Proceedings of the International Colloquium on Automata, Languages, and Programming* (pp. 579-591). Springer.

Goyal, V., Pandey, O., Sahai, A., & Waters, B. (2006). Attribute based Encryption for Fine-Grained Access Control of Encrypted Data. In *Proceedings of ACM Conference on Computer and Communications Security* (pp. 89–98). Academic Press. doi:10.1145/1180405.1180418

Green, M., Akinyele, A., & Rushanan, M. libfenc: The Functional Encryption Library. Retrieved from http://code.google. com/p/libfenc

Green, M., Hohenberger, S., & Waters, B. (2011). Outsourcing the Decryption of abe Ciphertexts. In *Proceedings of SEC'11 the 20th USENIX conference on Security* (pp. 34-34). Academic Press.

Guo, F., Mu, Y., Susilo, W., Wong, D. S., & Varadharajan, V. (2014). CP-ABE with Constant Size Keys for Light Weight Devices. *IEEE Transactions on Information Forensics and Security*, *9*(5), 763–771. doi:10.1109/TIFS.2014.2309858

Hashizume, K., Rosado, D. G., Fernandez-Medina, E., & Fernandez, E. (2013). An Analysis of Security Issues for Cloud Computing. *Journal of Internet Services and Applications, 4(5),* 1-13.

Hazen, A. W. (2003). Role-Based Access Control: The NIST Solution. *SANS Institute*. Retrieved from https://securitycommunity.tcs.com/infosecsoapbox/articles/2016/02/25/security-model-bell-lapadula-model

Herranz, J., Laguillaumie, F., & Rafols, C. (2010). Constant Size Ciphertexts in Threshold Attribute based Encryption. *International Workshop on Public Key Cryptography – PKC 2010* (pp. 19-34). Springer.

Khan, A. R. (2012). Access Control in Cloud Computing Environment. *Journal of Engineering and Applied Sciences*, *7*(5), 613–615.

KPMG. (2010). From hype to future: KPMG's Cloud Computing survey. Retrieved from http://www.techrepublic.com/whitepapers/from-hype-to-futurekpmgs

Lai, J., Robert, H. D., Chaowen, G., & Weng, J. (2013). Attribute-Based Encryption with Verifiable Outsourced Decryption. *IEEE Transactions on Information Forensics and Security*, *8*(8).

Laurie, B. (2009). Access control (v0.1). Retrieved from http://www.links.org/files/capabilities.pdf

Lewko, A., Sahai, A., & Waters, B. (2010). Revocation Systems with Very Small Private Keys. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P).* Academic Press. doi:10.1109/SP.2010.23

Li, J., Chen, X., Li, J., Jia, C., Ma, J., & Lou, W. (2013). *Fine-Grained Access Control System based on Outsourced Attribute-Based Encryption. In Computer Security – ESORICS 2013* (pp. 592–609). Springer.

Li, J., Huang, X., Li, J., Chen, X., & Xiang, Y. (2014). Securely Outsourcing Attribute based Encryption with Checkability. *IEEE Transactions on Parallel and Distributed Systems*, *25*(8), 2201–2210. doi:10.1109/TPDS.2013.271

Li, J., Jia, C., Li, J., & Chen, X. (2012). Outsourcing Encryption of Attribute based Encryption with Mapreduce. In *Proceedings of the International Conference on Information and Communications Security* (pp. 191–201). Springer. doi:10.1007/978-3-642-34129-8_17

Li, W., & Ping, L. (2009). Trust model to enhance Security and interoperability of Cloud environment. In *Proceedings of the 1st International conference on Cloud Computing* (pp. 69-79). Springer. doi:10.1007/978-3-642-10665-1_7

Majumder, A., Namasudra, S., & Nath, S. (2014). Taxonomy and classification of access control models for cloud environments. In *Continued rise of the cloud* (pp. 23–53). London: Springer.

Millen, J. K. (2011). Biba Model. In H. C. A. van Tilborg & S. Jajodia (Eds.), *Encyclopedia of Cryptography and Security*. Boston, MA: Springer.

Mujawar T. N., Sutagundar, A. V., & Ragha, L. L. (2017). Security Aspects in Cloud Computing. *International Journal of Advancing Cloud Database Systems and Capacity Planning with Dynamic*, 320-342.

Nali, D., Adams, C., & Miri, A. (2005). Using Threshold Attribute based Encryption for Practical Biometric based Access Control. *International Journal of Network Security*, *1*(3), 173–182.

Naor, M., & Pinkas, B. (2000). Efficient Trace and Revoke Schemes. In Financial Cryptography, 1–20.

Odelu, V., Das, A. K., Rao, Y., Kumari, S., Khan, M., & Raymond, K. (2017). Pairing based CP-ABE with Constant-Size Ciphertexts and Secret Keys for Cloud Environment. *Journal of Computer Standards & Interfaces*, *54*(1), 3–9. doi:10.1016/j.csi.2016.05.002

Ostrovsky, R., Sahai, A., & Waters, B. (2007). Attribute based Encryption with Non-Monotonic Access Structures. In *Proceedings of the 14th ACM conference on Computer and communications security* (pp. 195-203). Academic Press. doi:10.1145/1315245.1315270

Pang L., Jie Y., & Zhengtao J. (2014). A Survey of Research Progress and Development Tendency of Attribute based Encryption. *The Scientific World Journal*.

Sahai, A., & Waters, B. (2005). Fuzzy Identity based Encryption. In *Proceedings of EUROCRYPT* (pp. 457–473). Academic Press.

Shamir, A. (1985). Identity based Cryptosystems and Signature Schemes. In *Proceedings of CRYPTO 84 on Advances in cryptology* (pp. 47-53). New York: Springer Verlag.

Wan, Z., Liu, J., & Deng, R. H. (2012). HASBE: A Hierarchical Attribute based Solution for Flexible and Scalable Access Control in Cloud Computing. *IEEE Transactions on Information Forensics and Security*, *7*(2), 743–754. doi:10.1109/TIFS.2011.2172209

Wang, F., Liu, Q., & Wu, J. (2010). Hierarchical Attribute based Encryption for Fine-Grained Access Control in Cloud Storage Services. In *Proceedings of ACM Conference Computer and Communications Security (ACM CCS)*, Chicago, IL. Academic Press. doi:10.1145/1866307.1866414

Waters, B. (2011). Ciphertext-policy Attribute based Encryption: An Expressive, Efficient, and Provably Secure Realization. In Proceedings of Public Key Cryptography (pp. 53-70). Academic Press.

Younis A., Younis, K., & Merabti, M. (2014). An Access Control Model for Cloud Computing. *Journal of Information Security and Applications, 19*.

Zhang, R., Hui, M., & Yao, L. (2016). Fine-Grained Access Control System based on Fully Outsourced Attribute based Encryption. *Journal of Systems and Software*, *125*, 344–353. doi:10.1016/j.jss.2016.12.018

Zhang, Y., Zheng, D., Chen, X., Li, J., & Li, H. (2014). Computationally Efficient Ciphertext- Policy Attribute based Encryption with Constant-Size Ciphertexts. In *Provable Security* (pp. 259–273). Springer.

Zhou, Z., & Huang, D. (2010). On Efficient Ciphertext-Policy Attribute based Encryption and Broadcast Encryption. In *Proceedings of the 17th ACM Conference on Computer and Communications Security* (pp. 753–755). ACM. doi:10.1145/1866307.1866420

Zhou, Z., & Huang, D. (2012, October). Efficient and secure data storage operations for mobile cloud computing. In *Proceedings of the 2012 8th international conference on Network and service management (CNSM) and 2012 workshop on systems virtualiztion management (SVM)* (pp. 37-45). IEEE.