Extensive Survey on Usage of Attribute Based Encryption in Cloud

Balamurugan B
School of Information Technology and Engineering, VIT University, Vellore, India
Email: balamuruganb@vit.ac.in

Venkata Krishna P
School of Computing Science and Engineering, VIT University, Vellore, India
Email: pvenkatakrishna@vit.ac.in

Abstract—**Cloud computing has risen in the last decade to be the most aspired technology by the IT Industry. Cloud computing initially started as a technology for data outsourcing, later developed in to a newer computing platform for all IT related activities .The advent of cloud computing to deploy mission critical application has raised the value of cloud. On the contrary, cloud security is encountering infinite treats and vulnerabilities from several fronts. Security features like access control, digital signature, encryption and decryption are forced inside cloud environment to secure the cloud data. The paper surveys extensively all the varieties of the Attribute Based Encryption (ABE) access control techniques available to be used for cloud environments. Observations are made about the use of ABE and the ways access privileges are provided. The different ABE techniques are compared analyzed and recommendation for it to be used in deploying different cloud applications are mentioned.**

Index Terms—**Attribute Based Encryption, Access control, Cloud security**

I. Introduction

In the last decade if we quantify the value of investments made by software industries, several billions were done on Cloud. It will be more than any investment made for any other technology. More and more software, manufacturing and other sectors that produce quick revenue are moving towards cloud for their storage, computing and services. The main impact of cloud is its capability to reduce the infrastructure and maintenance cost needed to start computing. Cloud has also become a non-rigid option for companies to store and maintain data securely without overheads. Let us take an example of a scenario, to emphasize the very need of cloud computing. Taking the case of startups. Startup software companies are a trend in developing countries, where a pool of talented human resources comes together to create a software. After the development and testing process is over, the application should be made available to the public to be consumed. It needs a lot of budget in terms of infrastructure like servers, hardware, software's and tools. On the other hand, the cloud provides all these needs by means of different models like platform as a service (PaaS), Infrastructure as a service (IaaS) and software as a service (SaaS) catering all the computing needs.

On one hand cloud services and utilization grows exponentially and on the other hand, critics and security analysts are complaining about the non-competitive security aspects of the cloud. This trade-off can be removed by rolling out newer, efficient and effective cloud security up gradations like good access control techniques, strong digital signature, and competent encryption/decryption algorithms.

In cloud the access control technique sets the control and limitations to the actions done by several users over the data on the cloud. It processes the capability to allow or deny access to a resource on the cloud based on certain constraints and protocols followed extensively for all the users. The access control algorithm sets the abstraction level to the data for the cloud users thereby achieving confidentiality, integrity, availability and scalability.

Cloud application deployment depends on several factors like load balancing, bandwidth, data size and security. Access into the cloud environment is determined by the access control techniques provided by the cloud service provider. A weak access control technique will lead to several attacks like insider attacks, collusion attack, and denial of service attacks. It is necessary for a cloud environment to have an access control policy to give fine grained and scheduled access to users. There are several access control policies available for cloud computing ranging from Discretionary access control (DAC), Mandatory Access control (MAC), Role based access control (RBAC) and Attribute based encryption access control (ABAC). Each of these access control has been designed for policy neutral, administrative convenient access design .The imperative properties of DAC and MAC are combined together to get RBAC. While DAC is user discretionary, MAC is based on lattices .Certain limitations of RBAC had led to the development of ABE based access control schemes [28]. The primary being the role explosion that happens in

doi:10.4304/jetwi.6.3.263-272

large enterprises which needs finite access control, secondly the difficulties in role designing accordance to the top-down or bottom approach of the role hierarchy. At times, in RBAC assigning users/permissions to role becomes difficult due to the adjustments to be done based on local and global situational factors. All these limitations has forced some of the applications in need of fine grained access control to go for ABE based access control techniques.

In cloud computing, Public Key Infrastructure (PKI) is used to achieve trust .Most of the access control algorithms are based on PKI. In generic public key infrastructure, the encryption and decryption process starts with sender requesting public key from key distribution center (KDC).Then PKI signs the public key and sends to the requester. The sender uses the public key to encrypt the message for the receiver. Receiver uses the private key to decrypt the message encrypted by the sender. This has certain limitations like ,to communicate with the receiver ,the sender has to communicate with the PKI.To overcome this limitation, cloud based Identity Based Encryption(IBE) uses one's publicly known identity like email id, social security number(SSN),Date of Birth(DOB) as his/her public key and private key is generated from his/her known identity. The cloud based IBE has four phases: setup, keygen, encryption and decryption. The setup generates the master key for the receiver. The receiver then shows and proves his/her identity like SSN, email to the private key generator (PKG).Given the identity keygen algorithm generates the private key for the receiver. In encryption phase the sender knows the identity of the receiver (email) and uses it to encrypt the message. The receiver uses his/her private key which had been generated by the PKG to decrypt the message. The primary advantage of using cloud IBE is the user need not to communicate for the public key with the KDC as the sender already knows the receiver identity.

The attribute based encryption (ABE) overcomes the limitation of the cloud based IBE. In ABE the key policy is being associated with the identity of the user. The ABE has four phases which includes set up algorithm, key generator, Encryption and Decryption. The phases are explained in detail in section II. Attribute Based Encryption.

This paper analyses the different ABE techniques for its strengths and weaknesses.

II. Attribute Based Encryption Scheme

In the year 2005, Sahai and Water proposed fuzzy Identity-based Encryption based on Adi Shamir's Identity based encryption [27].The scheme used biometric as an identity for encryption and decryption process, having an edge over traditional Identity Based Encryption (IDE). Figure 1 shows a generic ABE based access control scheme. The ABE scheme has entities authority, sender and receiver. The authority's functionality is to generate keys according to the attributes for the purpose of encryption and decryption. Keys are generated by means of attributes. If the data is encrypted using two attributes, then the threshold is set as two and needs at least two matching attributes from the file user to decrypt the data and consume it. The prominent features of attribute based encryption are its capacity to address complex access control policies and its ability to cater supplementary number of users in large scale without the knowledge of the capacity of users before settings up the system.

Attribute Based Encryption access control (ABAC) has emerged as a prominent access control algorithm for cloud computing in the recent years. The applications of ABE in cloud environment ranges from traditional backup applications, financial applications to critical medical data storages applications.

The ABE schemes have four phases to be executed: Setup, Key Generation, Encrypt and Decrypt.

A. Basis of ABE

G_1 and G_2 be the Bi-linear group both of prime order p Defining the continuous function e by the map (bilinear map),

$e: G_1 \times G_1 \rightarrow G_2$.

g, d are generator of G_1 and processing parameter respectively.

1. Setup (m):

Let $\{r_1, r_2, \ldots, r_n\} \in Z_q$ be the random positive integers.

Let $x \in Z_q$ be the integer.

The

$PK = \{R_1 = g^{r_1}, R_2 = g^{r_2}, \ldots, R_n = g^{r_n}, \mathrm{X} = e(g,g)^x\}$

be the public key and $MK = \{r_1, r_2, \ldots, r_n, x\}$ be the master key.

2. Key generation (AU, PK, MK):

Let u be the data user. Let q be the polynomial of degree m-1, where m is the limit value. Let q(0)=x. Let UPK be the private key of data user u which is given by, $\frac{C1e(g,g)^{px}}{e(\mathrm{C},\mathrm{DK})}$ for each user i.

3. Encrypt (ACT, PK, M):

Let M be the message in G_2 and let p be the random number in Z_q.

Message is encrypted by,

$E = MX^p = e(g,g)^{xp}, E_i = g^{r_i p}$ for each user i.

4. Decrypt (CT, PK, D):

The CT is decrypted with UPK.

Select m such that $i \in AU \cap ACT$ .and

$e(E_i, UPK_i) = e(g,g)^{q(i)p}$ if $|\mathrm{AU} \cap \mathrm{ACT}| \geq \mathrm{m}$.

$X^p = e(g,g)^{xp}$.

Therefore the original message is obtained by $M = EX^{-p}$.

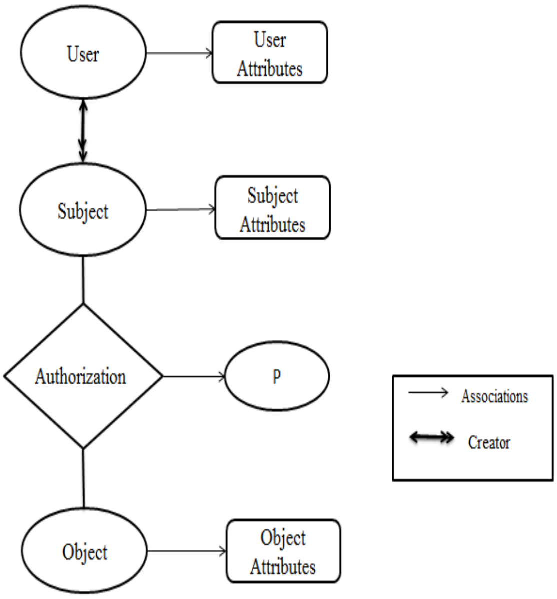

Figure 1 .Overview of ABE based access control model.

III. Related works

A. Derivatives of Attribute Based Encryption

Sahai and Waters [1] proposed the ABE system and it is the first scheme which achieved the One-to-many public-key encryption .In this scheme, the cipher text and the users secret key are related with the set of attributes and these set of attributes act as a access policy. Only when there is a match between the attributes of the decryption key and cipher text, the users will be capable of decrypting the cipher text. The main limitation of the ABE system is the lack of expressibility in threshold semantics and also the number of pairing operations increases with the increase of complexity of access policy. There is also possibility for the malicious users to leak the key to others without knowing the seriousness of traceability. It is not suitable for the applications with different categories of users and it will incur a computation overhead. In the Yu et al proposed[2] concept, the access policies are framed by means of the data attributes and almost all the computational tasks of the user revocation part are delegated to the third party cloud server, without revealing the content. The proposed scheme combines the Attribute Based Encryption scheme with Proxy re encryption and Lazy-re-encryption to achieve the efficiency. The proposed scheme also maintains the accountability to some extent through the advent of AHL and UL. The Attribute History lists (AHL) is mainly managed for tracing the evolution of attribute versions and Proxy re encryption keys (PRE keys) and it also upholds the UserList (UL) for recording and accounting the IDs of all the verified and genuine users in the system. There are two levels of operations such as system level and algorithm level. Here in this scheme, the cloud server will update the required attributes upon receiving the request from the user and waits until it gets the request with the generated update keys. The problems encountered in this scheme are that there is a deficiency of flexibility in managing attribute and it also deficit of scalability in handling the multi-level authorities.

In the Sascha Muller, Stefan Katzenbeisser, and Claudia Eckert proposed [3], there will be arbitrary number of attribute authorities for generating, managing and issuing the secret and public attribute keys for each attribute distinct to the CP-ABE scheme. For encrypting the message, the user has to first calculate the access policy in the Boolean formula on few attributes and finally use public keys associated with the attributes to encrypt. To decrypt, the user has to have minimum number of attributes. It also includes separate algorithms for creating user, attribute authority, requesting secret key and requesting public key and this avoids the collusion attack. There comes the complexity while calculating the access policy.

In Junbeom Hur and Dong Kun Noh proposed [4] scheme, they have used a dual encryption technique and selective group key distribution for each attribute group for achieving the fine-grained access control. The user access control is done in system level rather by each attribute level. They also employ the stateless group key distribution technique using binary tree for reducing and resolving scalability and stateless receiver problem. Since the data service manager do the rekeying straight away, the user or the attribute can be withdrawn at any point of time even earlier to the expiration time. It achieves the fine grained access control at each level of attribute instead of the system level. As long as the user holds the attributes, they will be able to access to the data.

Goyal et.al[5] proposed a scheme called Key Policy Attribute Based Encryption **(**KP-ABE**)** based on the Sahai and Waters concept of Attribute Based Encryption. In the KP-ABE, the data owner or the encryptor encrypts the data by associating it with the set of descriptive attributes and the access structure is linked with the decryption key. The access tree has leaf nodes and non-leaf nodes. The leaf nodes acts as the attributes and the non-leaf nodes acts as the threshold gates. Only when the attributes linked with the cipher text matches with the access structure of the decryption key, the user will be capable of decrypting the cipher text. The disadvantages of the KP-ABE scheme are : the data owner is not sure about who can decrypt the cipher text apart from choosing a collection of attributes which describes the data, the data owner is in a situation to fully trust the key-issuer and also the scheme couldn't express the negative attributes because it has adopted a monotonic structure pattern for expressing access structure.

1. Setup (m):

Let $\{r_1, r_2, \ldots, r_n\} \in Z_q$ be the random positive integers.

Let $x \in Z_q$ be the integer.

The

$PK = \{R_1 = g^{r_1}, R_2 = g^{r_2}, \ldots, R_n = g^{r_n}, X = e(g,g)^x\}$

be the public key and $MK = \{r_1, r_2, \ldots, r_n, x\}$ be the master key.

2. Key generation (AUKP, PK, MK):

The leaf node of access structure be denoted by y.

$UPK_y = (\frac{q_y(i)}{r_i})$ be the private key. Here i equal the access structure leaf node.

3. Encrypt (M.ACT.PK):

Let M be the message in G_2.

Let p be the random number in Z_q.

Message is encrypted by,

$E = MX^p = e(g,g)^{xp}, E_i = g^{r_i p}$ for each user i.

4. Decrypt (CT, D):

$e(D_y, E_i) = e(g,g)^{pq_i(0)}$ if I equal to leaf node and i is in access structure.

If i is not access structure then invalid.

If i is not equal to leaf node then $e(D_y, E_i) = e(g,g)^{pq_y(0)}$.

Then $e(g,g)^{xp} = X^p$ if ACT equals to access structure of private key. So, $M = EX^{-p}$.

Bethencourt et al [6] proposed a scheme called Ciphertext policy based Encryption (CP-ABE) which is conceptually closer to the KP-ABE scheme and the strategy is straight opposite to the KP-ABE. In the CP-ABE scheme, the access structure is related with the data while the collective set of attributes is related with the decryption key. Since the access policy is linked with encrypted data, even if the cloud server is an untrusted party, the confidentiality of the data cannot be revealed. This scheme overcomes the limitation of KP-ABE scheme by deciding who can decrypt the ciphertext whereas in KP-ABE, the encryptor is not able to decide who is capable of decrypting the Ciphertext. Only when the set of attributes associated with the decryption key complies with the access policy, the user will be capable of decrypting and recovering the ciphertext. The proposed scheme is secure against collusion and plaintext attacks. They also have depicted the decryption efficiency improvements by optimizing the decryption strategy and direct computation of decrypt node. The CP-ABE scheme is closer to the traditional RBAC scheme. The limitations found in this scheme are: The encryption key satisfies only the logically organized set and the user will not be able to combine the attributes from different set. They can only use the combination of single set attributes. The decryption process introduces extra computation overhead to the users.

1. Setup:

Let $e_1, e_2 \in Z_q$ be two exponents.

The public key PK=

$\left\{ G_0, g, h_1 = g^{e_1}, h_2 = g^{\frac{1}{e_2}}, e(g,g)^{e_1} \right\}$.

The master key MK= $\left\{ e_2, g^{e_1} \right\}$.

2. Key Generation (AU, MK):

UPK=

$\left\{ D_k = g^{\frac{(e_1+p)}{e_2}}, D_j = g^p, H(j)^{p_j}, D_j^* = g^{p_j} \right\}$

for each user.

3. Encrypt (PK, M, ACTCP):

Let p be a random numbers.

Let $q_r(0) = p$ where r is the root node.

Let I be the leaf node set.

CT= $C_1 = Me(g,g)^{e_1 x}, C = h^x$, and $C_i = g^{q_i(0)}, C_i^* = H(ai)^{q_i(0)}$ for each user i.

4. Delegate (D, AV!):

User private key D and attributes in AV! To create a new private key D1.

5. Decrypt (CT,D):

If y is leaf node and attribute of y is in AU then,

Decrypt node= $\frac{e(D_k, C_y)}{e(D_k^*, C_y^*)} = e(g,g)^{pq_y(0)}$.

If attribute of node is not in AU,

Decrypt node=invalid.

If x is not leaf node,

Decrypt node= $e(g,g)^{px}$ and M= $\frac{C1e(g,g)^{px}}{e(C, DK)}$.

Wang et.al [7] proposed a scheme called Hierarchical Attribute-Based Encryption (HABE). This scheme is the combination of hierarchical identity-based encryption (HIBE) and ciphertext-policy attribute based encryption (CP-ABE) concepts. It maintains the fine grained access control and the computational tasks are fully delegated. This scheme uses the disjunctive normal form policy and assumes that the attributes in one conjunctive clause will be managed by the same domain master. The limitation in this scheme is that it is not able to support the compound attribute and multiple attribute allocation. It is difficult to implement this HABE scheme in practice.

Wang, Liu and Deng proposed [8] the new scheme called Hierarchical Attribute Set Based Encryption (HASBE) an extended version based on the combination of Ciphertext-policy attribute set based encryption and the user structure in hierarchical pattern. The main advantage of the scheme is to set free the data owner to be online. The overhead is also reduced for data consumer, reasonably only the cloud service provider, trusted authority and the domain authorities are expected to be online constantly. Recursive set based key structure is used and followed in HASBE. Efficiency is achieved by means of assigning multiple values for the access expiration time. All the involved parties such as Trusted Authority, Domain authority, Data owners, data consumers or users and cloud service provider are arranged in a hierarchical manner. The Trusted authority is responsible for administrating the lower level domain authorities and the domain authorities are responsible for sub-domain authorities and users. At each level the authority or users will be given a privilege upon successful authentication. The implementation of HASBE is simple as compared to others. The limitations of this scheme are also the lack of efficiency in the decryption process done by the users.

Bobba et.al[9] proposed a scheme called Attribute Set-Based Encryption (ASBE) by extending and enhancing the existing CP_ABE scheme. In this proposed ASBE scheme, the user attributes are organized in a recursive set formation. This scheme has proven better than the existing CP_ABE scheme by assigning multiple values to the single attribute for resolving the attribute revocation problem i.e by assigning different values to the expiration time attribute. Hence there is no need to recompute the encrypted data for each user revocation. But the limitation found in this scheme is inefficiency of the decryption process and no proper delegation.

B. *Multi Authority Based ABE*

Melissa Chase proposed the scheme called Multi authority ABE [10]. The ABE scheme [1] by Sahai and Waters proposed a single authority Attribute Based encryption scheme. But they did not state whether the ABE scheme is applicable to multi authorities or not and it is impractical to have a single authority to manage and issue the secret keys to the number of users .When number of users increases, the difficulty in managing multiple attributes by a single authority will get increased. So these problems have been solved in this proposed concept. In the proposed scheme, there can be any number of authorities employed for managing and issuing the secret keys. Each authority can distribute secret keys for different set of attributes. It will also be able to bear with arbitrary number of corrupted authorities. Also a single user can have different set of attributes from multiple authorities and the requests will be processed together. The limitation of this scheme comes in the attribute and user revocation. Hence the implementation possibility of this scheme is medium. Yongdong Wu, Zhuo Wei, and Robert H. Deng proposed a scheme called Mediated ciphertext policy (MCP-ABE)[11]. This proposed scheme can be employed to frame an access control scheme for scalable sharing media. The existing CP-ABE schemes are not able to support scalable media sharing, but MCP-ABE scheme supports the scalable media. Here multiple messages are encrypted into a single ciphertext. The proposed concept can be applied to the content delivery services. In accordance with each user's privilege, key graph will be generated and the media units are encrypted using the generated key and then the key graph will be encrypted using MCP-ABE scheme. The decryption can be done only when the user has required attributes matching with the user privileges. In mobile devices, there is a problem of resource limitation and they provide solution to this particular problem by outsourcing the computational processes to the cloud service providers. This outsourcing increases the overall process efficiency while maintaining the privacy and integrity of data.

Jin Li et.al proposed [12] a scheme by overcoming some challenges found in ABE scheme. Though the ABE scheme provides a standard encryption based access control, there is a chance for the malicious users to leak the decryption keys to the other users if there is no traceability and accountability. Hence in this paper, they mainly concentrate on the traceability factor for identifying the credentials about the malicious users who leaks the key information and thereby provides a way to account the details of that identified user to reduce the further illegal activities. They combined the multi authority CP-ABE scheme with accountability. They have also proposed their own algorithm for tracing. In this paper, the Encryption of message or data is not done in a usual way, instead they use a special attribute called Global identity (GID) and they encrypt the data with the received user's identity set. This identity will be embedded with the access policy and is retrieved in case of any malicious activity of user by inputting the access policy which is embedded with the GID.

Yang et al proposed [13] the scheme called DAC-MACS to achieve and increase the efficiency of the attribute revocation and user decryption operations. The proposed scheme concentrates on the multi authority cloud storage system because of the chances of users having attributes issued by different authorities and there should be effective mechanism to process the different attributes together. This achieves both forward and backward security by framing efficient attribute revocation method through the assignment of version number for each attribute. It also attains the decryption efficiency by means of token based model. The global unique ID's issued for the user helped in resisting the collusion attack. This scheme also prevents the unauthorized access of the data by certificate authorities by including the public keys of the attribute authorities (AAs) in the encryption of data. The cipher text update process is delegated to the cloud server itself. The DAC-MACS concept can be very applied to the real time critical applications with variety of users and clients.

C. *Outsourced Decryption*

Green et.al [14] proposed a new method for reducing the overhead in the process of decryption by outsourcing the task decryption of ciphertext to the cloud service providers (CSP), so that the users will be benefited in saving time and efficiency. Here the users will provide the transformation key to the CSP and the CSP will in turn use that key to decrypt the ABE-ciphertext into simple ciphertext. Then it is easy for users to transform the simple ciphertext into the original message and the adversary will not be able to access the data content. But the drawback in this proposed method is that there is no way to check the accuracy of the transformed ciphertext. Hence there is a chance for the occurrences of vulnerable attack in between.

Junzuo Lai, Robert H. Deng, Chaowen Guan, and Jian Weng[15] enhanced and overcame some problems of the[11]. This proposed concept achieves the verifiability property by introducing some extra algorithms for checking the correctness of the ciphertext transformed by the adversary. The decryption algorithm for the transformed ciphertext has been changed to take both the original ciphertext and transformed ciphertext as input for verifying correctness. Hence any fraud activity happening in between can be found easily by this kind of verification. It also helps in achieving the data integrity property.

IV. Usage of ABE

The overall survey of different ABE schemes have made a strong establishment that, it is sufficient to be an optimal access control technique for cloud computing. There are several applications that are stored in Cloud .Due to the criticality factor of the cloud, in terms of the security and the increase in vulnerabilities [26] over the last few years, more of non-critical application data are stored and processed in the cloud, when compared to critical applications. This has been a big blow to the growth of the cloud, which otherwise has been the best innovation of the decade. The process of converting the cloud to be a place for storing critical applications will be possible with the advent of newer security features and algorithms in the terms of access control, cloud data encryption/decryption algorithms, auditing techniques and digital signature for data integrity. The different ABE schemes have played a vital role in giving fine grained access to data users and its usage for giving access control to critical applications which have been discussed in previous works.

In [16] the authors had made use of a modified ABE for achieving finer search of files over the cloud during access. The have considered an example of an application, where data is huge and expands exponentially .The work proves the infinite expressive property of the ABE scheme with Boolean expressions. The ABE scheme has also been proved to accomplish privacy of the user by hiding the vital query information of data owner and user. The modified ABE scheme mentioned had been given privilege to search on encrypted data, thereby preserving privacy to the fullest extent suitable for financial, medical and military files and charts. The possibility of experiencing the same security performance with other access control algorithms is expensive in terms of computational, storage and communication overheads. These features have confined the edge of ABE security over other access control schemes like RBAC [24] and DAC [25] for cost effective critical cloud application usage.

In [17] an attribute based encryption scheme without pairings is presented by improvising CP-ABE. The performance of the proposed practical attribute based encryption scheme without pairings (CP-ABE-WP) is proved to be better than KP-ABE and CP-ABE. The main contribution of the work is a Secure File Sharing System (SFSS) than can be executed over cloud. The file sharing allows the cloud users to do operations like create, read, write, delete and modify same files stored as chunks on the cloud. The concept enables the user to achieve security properties like confidentiality, availability and integrity by means of the CP-ABE-WP. The whole concept can be aptly used for e-commerce applications on the cloud to achieve the ACID properties like Atomicity, Consistency, Isolation and Durability properties [18].This proves the ABE can implement access mechanisms with data consistency properties.

The concept of ABE (attribute based encryption) was first introduced by Amit Sahai et al., [19], later they have come out with several ABE based works [20, 21, 22, and 23].In [20] a new method for constructing ABE system for circuits using multi linear maps had been proposed and proved to be better than both CP-ABE and KP-ABE. The construction is done using GGH graded algebras [30] and has four phases setup, encrypt, decrypt and keygen. Already the advent of GGH algebra have been a proven technique in signal processing, statistical applications and neural networks. Here the cryptographic applications of GGH algebras are put to use with ABE and security extensions in terms of access control are completed. In [21] Amit Sahai has yet again extended the properties of ABE through IBFHE (Identity-based fully homomorphic encryption).The purpose of the evaluation keys has been removed and the evaluator only needs certain parameters of the scheme. The scheme had been proved faster than most of the ABE based schemes.

Another prominent usage of ABE is its prominence, when combined with RBAC [29].RBAC compatible ABE is flexible, user-friendly and manageable security algorithm. The scheme is made possible by combining RBAC with Access List (ABE-AL).This reduces the problem of role explosion that prominently happens in RBAC, in large enterprises.

V. Hierarchical diagram and comparison table

A. Hierarchical Diagram

A hierarchical diagram depicting different types of access control algorithms and techniques are shown in figure 2. There are almost fifteen derivatives of ABE and each of them have evolved from the basis of ABE concept and had been tailor designed for specific usage and applications .They are majorly divided in to four categories in terms of outsourced decryption, derivatives of ABE,hierarchical ABE and multi-authority based ABE.

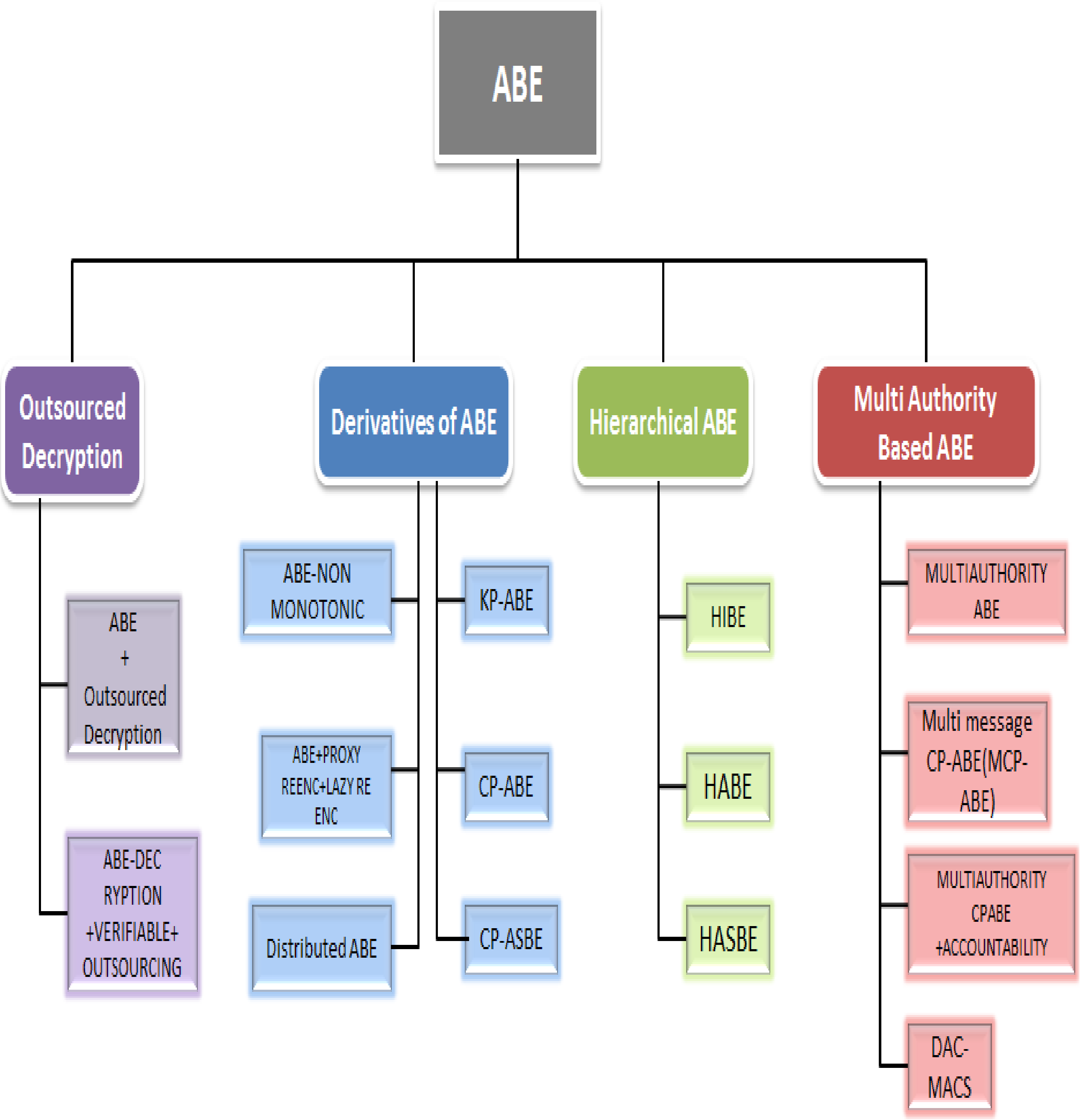
ABE
Outsourced Decryption
Derivatives of ABE
Hierarchical ABE
Multi Authority Based ABE
ABE + Outsourced Decryption
ABE-DEC RYPTION +VERIFIABLE+ OUTSOURCING
ABE-NON MONOTONIC
ABE+PROXY REENC+LAZY RE ENC
Distributed ABE
KP-ABE
CP-ABE
CP-ASBE
HIBE
HABE
HASBE
MULTIAUTHORITY ABE
Multi message CP-ABE(MCP-ABE)
MULTIAUTHORITY CPABE +ACCOUNTABILITY
DAC-MACS

Figure 2. Hierarchical diagram showing the different derivatives of ABE scheme

B. *Comparison Table*

TABLE1.
COMPARISON OF ABE SCHEMES

Algorithms	**Features**					
	Computation Overhead	**Decryption and User revocation Efficiency**	**Collusion resistant**	**Application Relevancy**	**Association of Attributes**	**Association of Access Policy**
ABE[1]	Average	Average	Below Average	Supports users with similar attributes	With Ciphertext	With Key
ABE-NON MONOTONIC[15]	Above Average	Average	Below Average	Supports users with similar positive as well negative attributes	With Ciphertext	With Key
ABE+PROXY REENC+LAZY REENC[2]	Above Average	High	Above average	Supports users with different attributes	With Ciphertext	With Key
DISTRIBUTED ABE[3]	Average	Average	Below Average	Supports distributed users with different attributes	With Ciphertext	With Key
ABE+OUTSOURCED DECRYPTION[13]	Low	High	Below Average	Supports users with less computational resource	With Ciphertext	With Key
ABE+VERIFIABLEOUTSOURCING DECRYP[14]	Low	High	Below Average	Supports users with less computational resource	With Ciphertext	With Key
KP-ABE[5]	High	Low	Average	Supports users with different attributes based on key policy	With Ciphertext	With Key
CP-ABE[6]	High	Low	Yes	Supports users with different attributes organized in single set	With Key	With Cipher text
CP-ASBE[7]	Above Average	Above Average	Average	Supports users with recursive set of attributes	With Key	With Cipher text
HABE[8]	High	Average	Average	Supports users with different attributes organized in single set in hierarchical way	With Key	With Cipher text
HASBE[9]	High	Average	Above Average	Supports users with compound attributes in a hierarchical way	With Key	With Cipher text
MULTIAUTHORITY-ABE[9]	High	Above average	Above Average	Supports multiple levels of attribute authorities and users	With Ciphertext	With Key
MCP-ABE[10]	Above average	Average	Average	Supports users with different attributes	With Key	With Cipher text
MULTIAUTHORITY CPABE+ACC[11]	Above average	Above average	High	Supports multiple levels of attribute authorities and users	With Key	With Cipher text
DAC-MACS[12]	Low	High	High	Supports multiple levels of attribute authorities and users	With Key	With Cipher text

C. *Overall Observation*

The overall observation shows that the ABE [1] scheme forms a strong foundation for encryption and access control. Figure 2 shows the Hierarchical diagram of different derivatives of ABE scheme. Having ABE as a base, many ABE based schemes were proposed by enhancing, extending and modifying it. And next to the ABE scheme, the CP-ABE[6] the derivative of ABE proved as an prominent scheme by deciding who can decrypt the data stored at cloud server. Following that there were other schemes which focused on scalability, fine-graininess and multi authority based concepts. Some schemes focused on reducing the decryption overhead by outsourcing the decryption process to the third party or to the cloud service providers [4]. Then the scheme such as DAC-MACS [13] was proposed by increasing the efficiency of both attribute revocation and decryption process through their own token generation algorithm and this DAC-MACS scheme is considered as latest version of the ABE with high efficiency.

VI. Conclusion

Attribute based encryption is an extensively used technique for access control. It has been used to refine users from accessing information .The primary advantage of ABE is key strength, enabling users to have a stronger encryption, than other encryption. Cryptanalysis has revealed that the complexity of the algorithm is of good order and cannot be made vulnerable. The paper has distinctly identified different ABE techniques and categorized according to its functionalities. The validation of the ABE algorithms is also done. We have also given a comparison table of different ABE based schemes based on various features such as computation overhead, decryption and user revocation efficiency, collusion resistant, application relevancy, association of attributes and association of access policy in a five scale rating form. We have done our survey upon extensive derivatives of ABE scheme.

References

[1] A.Sahai and B.Waters,"Fuzzy Identity Based Encryption,"In Proc. Advances in Cryptology-Eurocrypt,2005, vol.3494,pp.457-473.

[2] Schucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou," Achieving secure, scalable, and fine-grained data access control in cloud computing,"in Proc IEEE INFOCOM, 2010.

[3] S.Muller, S.Katzenbeisser, and C.Eckert," Distributed attribute-based encryption,"in Proc.11th Int.Conf.Information Security and Cryptology, 2008,pp.20-36, Springer.

[4] J.Hur and Dong Kun Noh," Attribute-Based Control with Efficient Revocation in Data Outsourcing systems," IEEE Transactions on Parallel and Distributed Systems,Vol.22, No.7,July 2011.

[5] V.Goyal, O.Pandey, A.Sahai and B.Waters, "Attribute-based encryption for fine-grained acess control of encrypted data," in Proc.ACM Conf.Computer and Communications(ACM CCS), Alexandria,VA,2006

[6] J.Bethencourt, A. Sahai, and B.Waters, "Ciphertext-policy attribute based encryption," in Proc.IEEE Symp. Security and Privacy, Oakland, CA,2007

[7] R.Bobba, H.Khurana and M.Prabhakaran," Attribute-sets: A practically motivated enhanced to attribute-based encryption," in Proc.ESORICS, Saint Malo, France, 2009.

[8] G.Wang, Q.Liu, and J.Wu," Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in Proc.ACM Conf. Computer and Communication security(ACM CCS), Chicago.IL,2010

[9] Zhiguo Wan, Jun'e Liu, and Robert H.Deng,"HASBE: A Hierarchical Attribute Based solution for Flexible and Scalable Access Control in Cloud Computing,"IEEE Transaction on Information Forensics and Security, Vol.7,No.2, April 2012.

[10] M.Cahse," Multi-authority attribute based encryption," in Proc.TCC'07, 2007,pp.515-534, Springer

[11] Yongdong Wu, Zhuo Wei, and Robert H.Deng,"Attribute-Based Access to Scalable Media in Cloud-Assisted Content Sharing Networks," IEEE TRANSACTION ON MULTIMEDIA,Vol.15, No.4, June 2013.

[12] Kan Yang, Xiaohua Jia, KuiRen,Bo Zhang,and Ruitao Xie,"DAC-MACS:Effective Data Access Control for Multiauthority Cloud Storage Systems," IEEE Transaction on Information Forensics and Security, Vol.8,No.11,Nov 2013

[13] M.Green, S.Hohenberger, and B.Waters,"Outsourcing the decryption of ABE ciphertexts," in proc.USENIX Security Symp., San Francisco, CA,USA,2011.

[14] Junzuo Lai, Robert H.Deng, Chaowen Guan ,a nd Jian Weng,"Attribute-Based Encryption With Verifiable Outsourced Decryption," IEEE Transaction on Information Forensics and Security, Vol.8,No.8, Aug 2013

[15] Rafail Ostrovsky, Amit Sahai, Brent Waters: Attribute-based encryption with non-monotonic access structures. ACM Conference on Computer and Communications Security 2007: 195-203.

[16] Dongyoung Koo, Junbeom Hur, Hyunsoo Yoon, Secure and efficient data retrieval over encrypted data using attribute-based encryption in cloud storage, Computers & Electrical Engineering, Volume 39, Issue 1, January 2013, Pages 34-46, ISSN 0045-7906.

[17] Shuaishuai Zhu; Xiaoyuan Yang; Xuguang Wu, "Secure Cloud File System with Attribute Based Encryption," *Intelligent Networking and Collaborative Systems (INCoS), 2013 5th International Conference on* , vol., no., pp.99,102, 9-11 Sept. 2013.

[18] Zhou Wei; Pierre, G.; Chi-Hung Chi, "CloudTPS: Scalable Transactions for Web Applications in the Cloud," *Services Computing, IEEE Transactions on* , vol.5, no.4, pp.525,539, Fourth Quarter 2012

[19] Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters: Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. IACR Cryptology ePrint Archive 2006: 309 (2006)

[20] Sanjam Garg, Craig Gentry, Shai Halevi, Amit Sahai, Brent Waters: Attribute-Based Encryption for Circuits from Multilinear Maps. IACR Cryptology ePrint Archive 2013: 128 (2013)

[21] Craig Gentry, Amit Sahai, Brent Waters: Homomorphic Encryption from Learning with Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based. IACR Cryptology ePrint Archive 2013: 340 (2013)

[22] Amit Sahai, Hakan Seyalioglu, Brent Waters: Dynamic Credentials and Ciphertext Delegation for Attribute-Based Encryption. CRYPTO 2012: 199-217

[23] Allison B. Lewko, Tatsuaki Okamoto, Amit Sahai, Katsuyuki Takashima, Brent Waters: Fully Secure Functional Encryption: Attribute-Based Encryption and (Hierarchical) Inner Product Encryption. EUROCRYPT 2010: 62-91

[24] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, Charles E. Youman: Role-Based Access Control Models. IEEE Computer 29(2): 38-47 (1996)

[25] Almutairi, A; Sarfraz, M.; Basalamah, S.; Aref, W.G.; Ghafoor, A, "A Distributed Access Control Architecture for Cloud Computing," *Software, IEEE* , vol.29, no.2, pp.36,44, March-April 2012

[26] [online]https://cloudsecurityalliance.org/download/cloud-computing-vulnerability-incidents-a-statistical-overview/

[27] Adi Shamir. Identity-based cryptosystems and signature schemes. In Proceedings of CRYPTO 84 on Advances in cryptology, pages 47–53. Springer-Verlag New York, Inc., 1985.

[28] Xin Jin, Ram Krishnan, and Ravi Sandhu. 2012. A unified attribute-based access control model covering DAC, MAC and RBAC. In *Proceedings of the 26th Annual IFIP WG 11.3 conference on Data and Applications Security and Privacy* (DBSec'12), Nora Cuppens-Boulahia, Frédéric Cuppens, and Joaquin Garcia-Alfaro (Eds.). Springer-Verlag, Berlin, Heidelberg, 41-55.

[29] Yan Zhu, Di Ma, Chang-Jun Hu, and Dijiang Huang. 2013. How to use attribute-based encryption to implement role-based access control in the cloud. In *Proceedings of the 2013 international workshop on Security in cloud computing* (Cloud Computing '13). ACM, New York, NY, USA, 33-40.

[30] S. Garg, C. Gentry, and S. Halevi, "Candidate multilinear maps from ideal lattices, " in EUROCRYPT, 2013.