International Journal of Applied Engineering Research ISSN 0973-4562 Volume 14, Number 23 (2019) pp. 4209-4220

Access Control Schemes in Cloud: Taxonomy and Performance

Sabitha, S.

Dept. of Computer Science and Engineering, College of Engineering Trivandrum, Kerala, India.

Rajasree, M. S.

APJ Abdul Kalam Technological University, Ambady Nagar, Thiruvananthapuram, Kerala 695016, India.

Abstract

Most of the outsourced and shared data in the cloud are sensitive. Dis- closure of sensitive data leads to identity theft and violation of privacy. The Cloud Service Provider (CSP) may be untrusted or curious; it will try to dis- close/misuse the data. It is necessary to provide access control and security over the outsourced and shared data to hide it from the CSP and unauthorized users. Traditional access control schemes are prone to security threats in the cloud environment. Attribute-based access control (ABAC) schemes are more suitable for the cloud environment. Attribute-based encryption (ABE) provides fine- grained access control and security over the shared data to protect it from the CSP and unauthorized users. It preserves the privacy of users and the security of data being shared. Users can decrypt the data only if their attributes are satisfied with the access policy associated with the ciphertext. This paper presents a comprehensive survey of access control schemes in cloud. Performance comparison of various ABE schemes based on different parameters and thematic taxonomy of IBE are major contributions. Taxonomy and applications of ABE schemes are also dealt with. Thus, the survey opens up very interesting avenues for further research in this area, which are also discussed.

Keywords: Cloud Computing, Attribute-Based Encryption, Access Control, Data Sharing, Access Policy

1. INTRODUCTION

Cloud computing becomes more popular due to the features such as multi- tenancy, virtualization, and elasticity. Modern development in IT industry is focusing on big data residing in the cloud environment and its utilization is increased by sharing and collaboration. Its importance will be increased in the near future since the cloud data can be remotely stored, shared and processed. But most of the outsourced/shared data may be sensitive; disclosing it to others will violate the privacy. Privacy breaches could also lead to identity theft; destroy a person's finances, credit, and reputation. Unauthorized access of critical/sensitive data leads to data disclosure. Improper security and lack of access control lead to the disclosure of sensitive data. It is more challenging to ensure the security of data in a perimeter-less environment like the cloud. Encryption is a cryptographic solution to protect data in the cloud, unauthorized access can also be prevented by introducing access control [1].

Infrastructure-as-a-Service(IaaS) based cloud platform used for outsourcing the data and computation needs a comprehensive and fine-grained access control mechanism due to the dynamic, scalable and configurable security requirement of cloud customers. Identity and access management (IAM) is the access control mechanism used in Amazon Web Service (AWS)[2] whereas Google Cloud Storage [3] use IAM and access control list (ACL). IAM is less scalable, more complex and expensive. It cannot distinguish regular users and administrators. Session management is also missing so that users are always possessing all user permissions [4], [2]. It is not a better access control mechanism for scalable cloud applications since the cloud applications are more scalable and should be deployed within a limited interval of time. Hence, the security and access control mechanism provided by the existing IaaS cloud providers can be enhanced by the ABE scheme. IDaaS (Identity and Access-control as-a-Service) [5] violates an individual's privacy by disclosing their identity.

The ABE scheme is used to provide access control as well as hiding data residing in the cloud. Data owner can predetermine the recipient groups in this scheme. It is a fine-grained access control mechanism and better than the role-based access control(RBAC) scheme. The RBAC is not suitable for fine- grained access control [6]. In this scheme, permissions are associated with roles that are assigned to users. Roles may change depending on the situation and time [6].Setting up an initial role structure is difficult and inflexible in rapidly changing domains.

Identity is directly disclosed in IAM but that never happened in ABAC. ABAC is a fine-grained and non-colluding access control mechanism [7]. It can be used as a pluggable access control mechanism for data storage and selective sharing of documents in the public cloud. It can be incorporated into cloud storage and sharing services such as Google drive [3], Dropbox, iCloud etc. With the help of ABE scheme, bloggers allow their selected friends to view some part of securely placed private documents, organizations permit some selected employees to view or modify a part of securely placed sensitive data. We have analyzed various access control mechanisms which provide security, privacy, authentication and access control in the cloud environment. Out of which ABAC is a better solution to incorporate all the above features. It can overcome all the problems associated with privacy, security, and access control. In this scheme, only authorized users access the data and others are not permitted to access it. Access policies are embedded in the ciphertext.

The rest of the paper is organized as follows. Section 2 addresses access control over encrypted data, which includes traditional encryption schemes, IBE, and ABE. Classification based on the architecture of ABAC scheme is described in section 3. Section 4 describes the taxonomy and performance analysis of ABE scheme based on security, privacy, space, and time complexity. Applications of ABE scheme is discussed in section 5. Section 6 discusses the future research directions in ABE. Section 7 concludes the survey.

2. ACCESS CONTROL OVER ENCRYPTED DATA

Traditional encryption schemes such as public key and symmetric key cryptosystems are used to encrypt data before outsourcing it to the cloud. They suffer from performance overhead and lack of access control [8]. These schemes are based on the Access Control List (ACL). Computation complexity that grows linearly with the number of data groups or the number of users is a draw- back of schemes based on ACL [8]. A number of access control schemes exist for sharing encrypted data.

2.1. Symmetric key encryption-based access control

A secret key, that is used for encryption and decryption of the entire data is shared to all the users. Key generation, maintenance, and key distribution are the major hurdles in a symmetric key cryptosystem. Once the key gets compromised, all the encrypted information gets decrypted/leaked [8]. An alternative method is to generate a unique secret key for each individual user in order to share the encrypted information. The secret key will not be disclosed to other users. Here, the number of encryption keys increases linearly depending on the number of recipients. Thus, key management is a major problem while incorporating access control for data sharing using a symmetric key cryptosystem [9].

Another strategy to apply this scheme is to classify data with a similar ACL into a data groups. Each data group is then encrypted with a symmetric key and then that key is distributed to all users in the ACL. This ensures that only the users in a particular ACL are allowed to decrypt the corresponding data group [9]. But, the number of keys varies linearly with the number of data groups.

2.2. Public key encryption-based access control

The data owner's private key is used to encrypt the data. All the users can decrypt the ciphertext with the corresponding public key. This scheme does not allow the sharing of data among selected users. Another method is to encrypt the data using the public key of each user. The intended users can then decrypt the data using their own private key. In this case, multiple ciphertext copies of the same data are generated and stored. Another approach is the combined use of the symmetric key and the public key cryptosystem. In this approach, data is initially encrypted with a symmetric key. The key is then further encrypted with the public key of users in the ACL [8]. Only the users in the ACL can decrypt the data with their private key. But, cost of symmetric key encryption varies linearly with the number of users in the ACL.

2.3. Role-Based Access Control (RBAC)

In this method, permissions are associated with roles and roles are assigned to users. The users are permitted to access the resources based on their roles. Roles may frequently change depending on the time and situation [6], [10]. Establishment of initial role structure and privilege management is difficult due to the dynamic nature of privileges. Hence, RBAC is not an appropriate solution for providing fine-grained access control [6] to a role in the distributed environment. Zhou et al. proposed a secure cloud storage system to enforce access control policies using RBE[11]. Wang et al. proposed a framework for dynamic RBAC by integrating trusted computing with RBAC in cloud computing [12].

2.4. Identity-Based Encryption (IBE)

IBE is a public key cryptosystem proposed by Shamir [5] in 1984 to simplify the certificate management scheme in e-mail systems. This scheme does not require the receiver's public key. The Certification Authority (CA) verifies the receiver's authenticity and he gets the private key from the Key Generation Center (KGC). Later, Boneh and Franklin [13] improved the scheme using bilinear map based on groups. In that scheme, data is encrypted using the identity of an individual. The identity should be disclosed to the KGC to get the secret key. It can be any of the biometric identifiers of an individual [13]. Once the identity of a user has been authenticated by the KGC, the user will be able to retrieve the private key. Since identity is disclosed to the public, privacy cannot be preserved [14]. This scheme cannot provide fine-grained access control. IBE leads to difficulties such as privacy disclosure and the key escrow problem.

The variations of IBE schemes are Distributed KGCs based IBE, Account- able IBE, and Anonymous IBE. The master secret key is distributed among multiple KGCs in Distributed IBE [13]. So, the user has to authenticate with all KGCs, which results in a heavy workload on the user. If the KGC maliciously generates the key, it will be traced by the Accountable IBE [15]. In Anonymous IBE [16], the recipient is not able to distinguish the identity used to encrypt the message from the ciphertext.

Lin et al. [17] proposed a secure threshold multi-authority fuzzy IBE without a central authority. Li et al. [18] proposed a method to tackle the identity revocation issue by introducing outsourced computation. It is a collusion-resistant revocable IBE scheme with server-aided settings. Single private key generator (PKG) performs key generation and distribution, which exerts a heavy workload on the PKG for a large network and during user revocation. In order to reduce the workload on a key generation center, an identity-based proxy re-encryption has been introduced [14]. It can be efficiently utilized for secure e-mail, attribute- based delegation etc. One of the drawbacks of the scheme is the involvement of a semi-trusted proxy server.

Figure 1 shows the thematic taxonomy of IBE schemes for accessing data in the cloud. The methods are classified based on the architecture and features:

2.4.1. Hierarchical Identity-Based Encryption (HIBE)

Gentry et al. [19] introduced the HIBE to reduce the workload on a PKG. It is a collusion-resistant scheme. Later, an efficient HIBE scheme with a constant size ciphertext proposed by Boneh et al. [20]. Gentry and Halevi [21] introduced a fully secure HIBE scheme. Later, unbounded HIBE was introduced by Lewko and B. Waters [22]. Lee et al. [23] proposed an anonymous HIBE scheme. It offers message-hiding and identity-hiding features. The scheme is based on prime order (asymmetric) bilinear groups and the size of the ciphertext is also short. Here, access control is determined by the user's identity, which means that privacy cannot be preserved in this scheme.

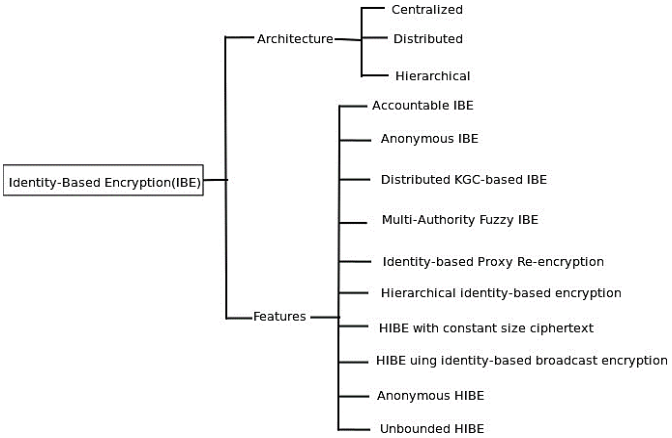

Figure 1: Thematic taxonomy of IBE

2.5. Proxy Re-Encryption (PRE)

Proxy re-encryption is a cryptographic method to convert a ciphertext in- tended for one party to the encryption of the same plaintext using different key of intended recipients with the help of proxy. It can turn a ciphertext intended for one person to another using the different key. Re-encryption is done by a proxy. The major drawback of this method is that the proxy should be trusted since the secret keys are disclosed to the proxy [24]. This scheme was further improved by ElGamal cryptosystem without disclosing a secret key [25].

2.6. Attribute-Based Encryption(ABE)

ABE is used not only for access control but also for hiding data. The data owner pre-determines the recipient groups by deciding the access policy to encrypt the data which in turn determines the attributes that users should possess to decrypt the data. Sahai and Waters [26] proposed an ABE scheme in 2005. Access control provided by a single Key Distribution Center (KDC) in this ABE scheme leads to a single point of failure [27]. Two variations of the ABE scheme based on access control are KP-ABE [28] and CP-ABE [29].

2.6.1. Key-policy attribute-based encryption (KP-ABE)

It is a public key cryptosystem used to share data among a set of users. In KP-ABE, the user's private keys determines access policy while a set of attributes are associated with ciphertexts. The access policy is represented as an access tree with attributes as the leaf nodes and the threshold gates as the interior nodes. Users can decrypt the ciphertext if and only if the access policy is satisfied by the attributes associated with the ciphertext. Goyal et al. [28] proposed a KP-ABE scheme with monotonic access formula. Later, Ostrovsky et al. [30] proposed a non-monotonic access structure based KP-ABE scheme. Wang et al.[31] proposed a KP-ABE scheme with a constant size ciphertext. ABE with fast decryption was suggested by Hohenberger et al. [32] in which policies are sent in clear text form.

2.6.2. Ciphertext-policy attribute-based encryption (CP-ABE)

CP-ABE is a cryptographic scheme to maintain the data confidentiality against untrusted cloud service provider and unauthorized users [29]. In this scheme, access policies are associated with ciphertext whereas the user's private key is determined by their attributes. The data owner/encryptor determines the access policy to be associated with the ciphertext during the encryption process. The user's credentials are represented using the attributes. The secret key corresponding to these attributes is generated and distributed by the key distribution center. Users decrypt the ciphertext only if their attributes satisfy the access policy associated in the ciphertext. Ge et al. proposed a CP-ABE scheme with constant size ciphertext [33].

The access policy is represented in the form of an access tree. The enforcement of access policy and policy updates are the main challenges here. Key revocation problem also exists in CP-ABE. Cheung and Newport [34] suggest a policy construction for CP-ABE with AND gates only. With this, the data would be shared among the group of users who have the same set of attributes. This scheme is more suitable for cloud data storage and sharing. However, it leads to many security issues like backward secrecy issue and forward secrecy issue. (1) Backward secrecy issue refers to the situation in which a new user is able to access and decrypt the messages which are encrypted and shared before he/she joins the system. (2) Forward secrecy issue refers to the situation in which a user who has left a group or revoked an attribute is able to access or decrypt future data. CP-ABE has the following advantages and disadvantages.

Pros

- Ensures better security and access control when compared to standard encryption schemes.
- Less overhead for key management.
- It provides not only access control but also encryption of data.

Cons

- The size of the ciphertext grows linearly depending upon the number of attributes in the access policy.

- The computational complexity of bilinear pairing is higher.

3. ATTRIBUTE-BASED ACCESS CONTROL (ABAC) SCHEMES

Identity is directly disclosed in IAM but that never happened in ABAC. The ABAC is a fine-grained and non-colluding access control mechanism [7]. It can be used as a pluggable access control mechanism for data storage and sharing in the cloud. It can also be incorporated into cloud storage and sharing services such as Google drive [3], Dropbox, iCloud etc. With the help of an ABE scheme, bloggers can allow their selected friends to view certain parts of the securely placed private documents. It helps the organizations to permit some selected employees to view or modify a part of securely placed sensitive data. Analysis of various access control mechanisms which provide security, privacy, authentication and access control in the cloud environment has been carried out. ABAC is the best solution among these mechanisms. It overcomes all the problems associated with privacy, security, and access control. In this scheme, only authorized users are allowed to access the data while others are not permitted to do so.

3.1. Centralized attribute-based access control

The architecture of centralized ABAC scheme for data storage and sharing in cloud consists of four important entities (1) Data owner: He/she is the owner of the original files to be shared for collaboration. The data owner decides the access policy before encrypting the file. The file to be shared is encrypted using a symmetric key, then that key is encrypted using the access policy and a CP- ABE scheme. (2) User: The decryption of ciphertext by the user is possible, only if their attributes satisfy the access policy associated in the ciphertext.(3) Cloud service provider(CSP): A CSP is the manager of the cloud server that provides many services such as data storage, sharing, and collaboration. It is a semi-trusted entity. Outsourced data is stored on cloud servers. (4) Centralized attribute authority: An Attribute Authority(AA) is a trusted agent in the centralized access control scheme. Revocation and modification of attributes of users are done by the AA. It is responsible to create public and private parameters for the systems and grants access permissions to users based on their attributes. But in a distributed environment, authorities may fail or be corrupt. Hence, centralized access control is not feasible in such an environment. Figure 2 shows the architecture of centralized ABAC for cloud data storage and sharing in the cloud. A single point of vulnerability is one of the disadvantages of this system.

Bethencourt et al.[29] introduced CP-ABE in 2007 in which, user's creden- tials are determined by their attributes. Liang et al.[35] proposed a provably secure CP-ABE scheme. Most of the ABE schemes generate variable sized ci- phertext depending on the number of attributes in the access structure. In many of the data sharing scenarios, the user's privilege may change after a period of time. So the data owner has to dynamically control the user privi- leges. Zhao and Li [36] proposed an efficient framework for data sharing that helps to achieve the dynamic privileges; the data owner can change the service class and the structure of privileges of each user dynamically. The data owner can also assign different privileges to different classes of members. Dynamically updating the privileges is also possible in this scheme. Hur [37] proposed an attribute-based data sharing scheme with hidden policies in smart grid.

The most important challenge in this scheme is to manage attributes and user revocation. When users join or leave the system other users' attribute keys have to be renewed to ensure forward and backward secrecy. It results in high computation cost and overhead on users, especially for those users with limited computing resources.

Different revocation methods like timed re-keying revocation, proxy re-encryption revocation, lazy revocation, and revocable-storage ABE have been suggested over the years. Hur and Noh [38] proposed an efficient CP-ABE scheme with attribute revocation. It resolves forward and backward secrecy issues using the re-encryption method. Lazy revocation further reduces the overhead of access revocation. In order to improve the performance of the system, it reduces the number of required re-encryption operations and the re-encryption is postponed until the next write access request.

3.2. Decentralized attribute-based access control

Decentralized access control mechanism resolves the risk of a single attribute authority in centralized access control. Figure 3 shows the architecture of decentralized ABAC for data storage and sharing in the cloud. A decentralized access control scheme has been introduced by deploying more number of attribute authorities. The distribution of attributes among users is not managed by a trusted central authority. Multiple attribute authorities have disjoint sets of attributes which are distributed among authorized users based on their request by verifying the identity. Users can receive any number of attributes from any attribute authorities. Attribute authorities distribute secret keys among users based on the attributes possessed by each user.

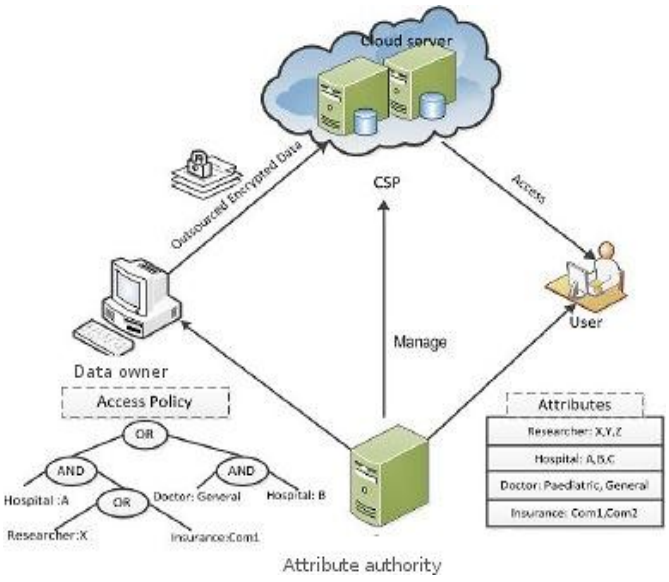

Figure 2: Architecture of centralized ABAC

Multiple attribute authorities distribute attributes and secret keys among the users in multi-authority ABE scheme proposed by Chase et al.[39]. But all the attribute authorities are coordinated by a trusted authority. However, this scheme fails to distribute control among multiple authorities as there is a central authority that can decrypt every message. User privacy is not preserved in this scheme as the Global IDentifier(GID) is assigned to each user. Later, the scheme was improved by eliminating the trusted authority [40]. Muller et al [41] developed an efficient distributed ABE scheme with the Disjunctive Normal Form (DNF) policy.

Lewko and Waters [42] proposed a fully decentralized ABE with multiple key distribution centers(KDCs) which do not need a trusted server. Users can get any number of attributes from any KDC. However, decryption on the user side needs more computation because of which mobile phone users face some issues while accessing information. Ruj et al. [43] proposed a distributed access control for data storage in the cloud. In this model, KDCs distribute attributes among users. The access policy is represented by an LSSS matrix and it supports user revocation without redistributing the keys after a user has been revoked. It is a collusion-resistant scheme. Fully anonymous ABE was developed by Taeho et al.[44]. It is a decentralized approach and concentrates on privilege control and identity privacy preservation. Yang et al.[45] attempted the secure sharing of video content during a specified time interval among a group of people in a cloud-based system. It is a time-domain decentralized ABAC scheme. Users who possess valid attributes and privileges during the specified time interval would be able to decrypt the ciphertext.

3.3. Hierarchical attribute-based access control

To securely delegate the key generation capability of root authority to the domain authorities, hierarchical attribute-based encryption (HABE) was pro- posed. Gentry et al.[19] initially proposed hierarchical ID-based encryption. In this scheme, a root private key generator securely delegates key generation to the lower level private key generator in order to create the private key for users. User revocation is the major problem associated with all the access con- trol mechanisms. Wang et al. [46] proposed the HABE to resolve the revocation of access rights of unauthorized users. It is achieved by utilizing the features of HIBE in a CP-ABE scheme. Scalable revocation is achieved by combining proxy re-encryption (PRE) and lazy re-encryption with HABE. HABE consists of four entities viz. (1) Root authority (2) Domain authority (3) Cloud service provider and (4) User.

HABE proposed by Wang et al. [47] is based on a trusted authority that re- lies on CP-ABE and HIBE. Hierarchical Attribute-Set-Based Encryption (HASBE) introduced by Zhiguo et al.[48] addressed the limitations of HABE. Most of the HABE schemes are affected by the hierarchical relationship between attributes in the same category. Wang et al.[49] proposed a Ciphertext-Policy Hierarchical Attribute-Based Encryption (CP-HABE). Teng et al.[50] resolved the scalability and flexibility issue in CP-HABE by the constant size ciphertext generation. Wang et al.[51] developed an FH-CP-ABE by modifying the CP-ABE method using the layered structure of access policy. In order to encrypt a file in the same hierarchical structure, the FH-CP-ABE scheme integrates various access structures of files into a single access structure. Figure 4 and 5 show the architecture of hierarchical ABAC and ciphertext policy hierarchical ABAC for data storage and sharing in the cloud.

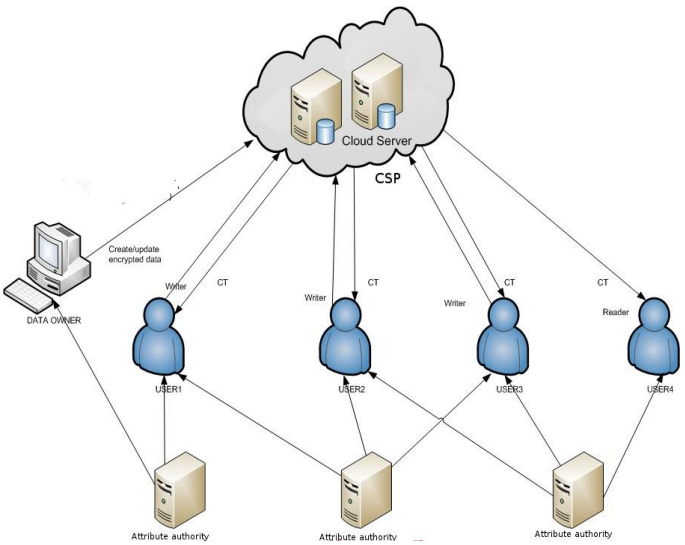

Figure 3: Architecture of decentralized ABAC

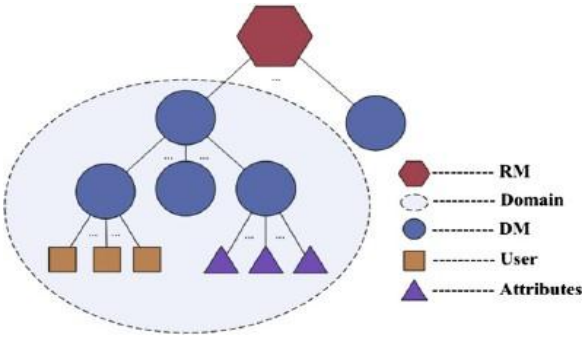

Figure 4: Architecture of hierarchical ABAC[46]

4. TAXONOMY AND PERFORMANCE OF ATTRIBUTE-BASED ENCRYPTION

The essential features required for ideal ABE schemes are listed below:

1. Confidentiality: Unauthorized users and cloud service providers are not allowed to decrypt the data.
2. Fine-grained access control: Different access rights can be given to users within the same group.
3. User revocation: Once the users exit the system, their access rights are revoked, after which they are not allowed to access the data.
4. Scalability: Irrespective of the increase in the number of users, the per- formance of the system never degrades.

5. Collusion resistance: Unauthorized users cannot collude with each other to get the data if they are not individually authorized to access it.

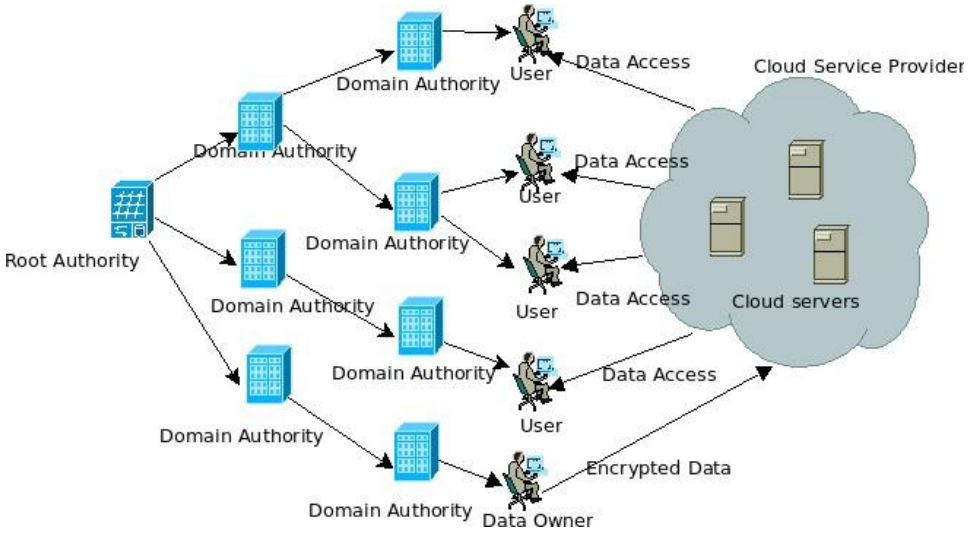

Figure 5: Architecture of ciphertext-policy hierarchical attribute-based access control

The taxonomy of ABE schemes based on the essential features supported in various literature is described in Figure 6. It gives a clear understanding of various developments in ABE. Table 1 describes the notations used for the following comparisons. Table 2 shows the strength of each scheme on the basis of security and privacy. Outsourcing the decryption reduces the overhead on the user. In some schemes, privacy is preserved by keeping the identity anonymous. Collusion possibility is eliminated by the distributed approach. Security of the scheme is proved by the Decisional Bilinear Diffie-Hellman assumption (DBDH). In order to reduce the overhead on the recipient side, mobile users can utilize the scheme with decryption-outsourcing capability. The anonymity providing schemes are useful in privacy critical applications.

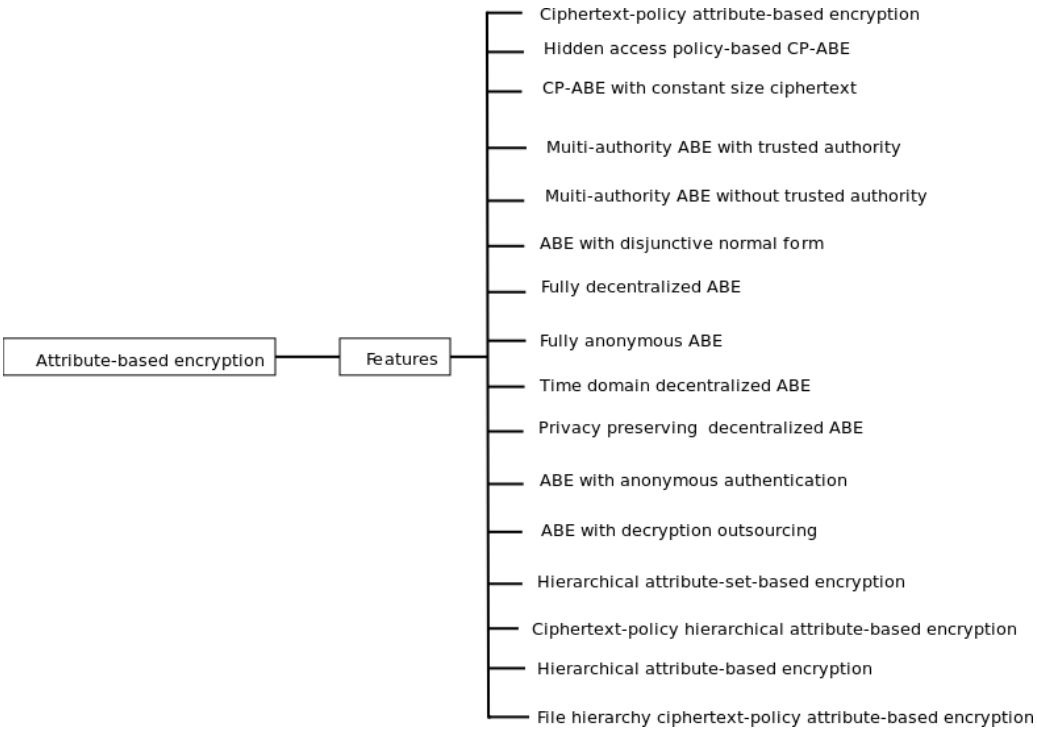

Figure 6: Taxonomy based on features of ABE

Table 3 compares the performance in terms of storage cost of existing ABAC schemes in the cloud. It describes the efficiency of various ABE schemes. It can be used to select the appropriate scheme depending on the users' requirement. The scheme which utilizes less storage space will be a viable solution for mobile users.

5. APPLICATIONS OF ATTRIBUTE-BASED ACCESS CONTROL SCHEMES

The ABE scheme is mainly used for secure data storage and sharing in the cloud. Besides this, it can be used for various other applications:

- Location-based systems: ABE scheme can be used to permit the users with a specific global position to access sensitive and secure data.
- Time-constrained applications: Operations involving denying access to data after a certain period of time and self-destruction of data are per- formed on the basis of the time attribute [45], [62].
- Big data in the cloud: Enables access control and encryption of big data in the cloud. Dynamic updates of attributes are possible [31], [32].
- Internet of Things (IoT): Patients can use a Smart Watch to collect their periodical health report to securely communicate with their concerned doctor. Secure communication is done using an ABE scheme. Patients can undergo periodical health checkup without physically visiting the doctor.
- Underwater sensor applications: Secure information exchange in an un- derwater sensor environment.
- Electronic Health Record (EHR) sharing in the cloud: Cloud computing is in compliance with HIPAA (Health Insurance Portability and Account- ability Act). HIPAA was designed to regulate the use and disclosure of Personal Health Information (PHI) by health care providers[1]. It pro- tects and restricts access to sensitive data. Healthcare providers widely use cloud computing for secure storage and sharing of Electronic Health

Table 1: Description of notations used

Notations used	Purpose
$\|tt1\|, \|ttT\|$	Bit length of an element in group $tt1$, ttT respectively
$\|Zp\|$	Bit length of an element in Zp
$r1, r2$	Set of attributes associated with ciphertext and secret key respectively
$\|msg\|$	Size of the message
n	Number of elements
m	Number of attributes in access structure
u	Size of an attribute universe
N'	Total number of possible statements of attributes
l	Number of attribute type in public domain (PUD)
N	Number of attribute authority(AA) in public domain(PUD)

Table 2: Security and privacy analysis of attribute-based access control schemes

Scheme	Security	Keyescrow problem	Distributed access control	Decryption outsourcing	Anonymity	Security assumption
RNS[43]	Against $\|A\| - 1$ AA collusion	Solved	Yes	No	No	DBDH
BSW[29]	Collusion resistant	Not solved	No	No	No	Generic group model
YWRL[27]	No distinct KDC	Not solved	No	No	No	DBDH
LYRL[52]	Against $\|A\| - 2$ AA collusion	Solved	No	No	No	DBDH
LYZRL[53]	Against $\|A\| - 2$ AA collusion	Solved	No	No	No	DBDH
SW[26]	Collusion resistant	Not solved	No	No	No	DMBDH
GPSW[28]	Secure against CPA	Not solved	No	No	No	DBDH
CN[34]	Secure against CPA, CCA	Not solved	No	No	No	DBDH
GHW[54]	CPA, RCCA secure	Not solved	No	Yes	No	DBDH
W[55]	CPA secure	Solved	No	No	No	DBDH
HUR[56]	Collusion resistant	Solved	Yes	No	Yes	Backward, for ward secrecy
RSN[57]	Collusion and replay attack resistant	Solved	Yes	No	Yes	DBDH
YJR[58]	Collusion resistant	Not solved	Yes	Yes	No	Backward, for ward secrecy
ZNS[59]	Collusion and replay attack resistant	Not solved	No	No	No	DBDH

Table 3: Performance comparison in terms of storage cost of ABE schemes in cloud

Scheme	Public Key Size	Master Key Size	Secret Key Size	Ciphertext Size
SW[26]	$n\|tt1\| + \|ttT\|$	$(n+1)\|Z_p\|$	$r2\|tt1\|$	$r1\|tt1\| + \|ttT\|$
GPSW[28]	$n\|tt1\| + \|ttT\|$	$(n+1)\|Z_p\|$	$r2\|tt1\|$	$r1\|tt1\| + \|ttT\|$
CN[34]	$(3n+1)\|tt1\| + \|ttT\|$	$(3n+1)\|Z_p\|$	$(2n+1)\|tt1\|$	$(n+1)\|tt1\| + \|ttT\|$
BSW[29]	$3\|tt1\| + \|ttT\|$	$\|Z_p\| + \|tt1\|$	$(2n+1)\|tt1\|$	$(2r_1+1)\|tt_1\| + \|tt_T\| + \|Z_p^*\|$
NYO[60]	$(2N^j+1)\|tt1\|+\|ttT\|$	$(2N^j+1)\|Z_p\|$	$(3n+1)\|tt1\|$	$(2N^j+1)\|tt1\| + \|ttT\|$
W[55]	$2\|tt1\| + \|ttT\|$	$\|tt1\|$	$(1+n+r2)\|tt1\|$	$(1+r1n)\|tt1\| + \|ttT\|$
KAKM[61]	$(2N^j+3)\|tt1\|+\|ttT\|$	$(N^j+1)\|Z_p\|$	$2\|tt1\|$	$2\|tt1\| + \|ttT\|$
YWRL[27]	$(3u+1)\|tt1\| + \|ttT\|$	$--$	$r2+(2u+1)\|tt1\|$	$mlog\|tt1\| + \|ttT\| + \|msg\|$
LYRL[52]	$(\|u\| + N - 1)\|tt1\|$	$(n+1)\|Z_p\|$	$(r2+l+1)\|tt1\|$	$mlog\|tt1\|+\|ttT\|+mlogm+\|msg\|$
RNS[43]	$\|u\|(\|tt1\| + \|ttT\|)$	φ	$r2\|tt1\|$	$m(2log\|tt1\|+\|ttT\|)+m+\|msg\|$
HUR[56]	$\|tt1\| + \|ttT\|$	$\|Z_p\| + \|tt1\|$	$(2n+2)\|tt1\|$	$(2m+1)\|tt_1\| + \|tt_T\|) + \|Z_p^*\|$
HN[7]	$2(\|tt1\| + \|ttT\|)$	$\|Z_p\| + \|tt1\|$	$(2r_2 + 1)\|tt_1\| + 2S_k$	$(logN_u)\ (2r_1+1)\|tt_1\| + \|tt_T\| + \|Z_p^*\|$
LYZRL[53]	$(\|u\| + N - 1)\|tt1\|$	$(n+1)\|Z_p\|$	$(r2+l+1)\|tt1\|$	$(r1+l+N-1)\|tt1\| + \|ttT\| + m$
RSN[57]	$\|u\|(\|tt1\| + \|ttT\|)$	φ	$2r2\|tt1\|$	$2mtt0\|+m\|ttT\|+m+\|msg\|+(l+t+2)\|tt1\|$

Record (EHR). It promotes remote monitoring and diagnosis of patients by the doctor.

6. RESEARCH DIRECTIONS

Research gaps with respect to ABAC scheme are identified. Various research scopes and open problems still exist in the ABAC scheme. Some of them are listed below:

1. Designing an efficient ABAC scheme with less communication and computation complexity while preserving forward and backward secrecy.
2. Access policies are sent in plaintext form, which discloses the user's at- tributes. Thus recipients' privacy is not preserved. Hence devising a solution to hide the access policies needed to preserve the privacy of recipients is crucial.
3. All users whose attributes satisfy the access policies are considered as authorized users which in turn leads to insider data theft. Developing a solution to avoid the possibility of insider data theft is necessary.
4. Efficiently managing dynamic data updates, dynamic updates of attributes and user revocation without redistributing the keys.

7. CONCLUSION

A comprehensive literature survey has been done on access control schemes in cloud. IBE and its thematic taxonomy are presented in this paper. The limitations of IBE schemes and all other access control schemes are also explored. The limitations of Identity and Access Management (IAM) scheme used by some cloud service providers are also briefed. We have analyzed the ABE schemes based on the essential requirements of an efficient access control mechanism. The ABE schemes are

classified into three major categories based on the architecture of the schemes. A taxonomy of available ABAC schemes is presented. Various ABE schemes are analyzed and compared based on the important features such as security, privacy, efficiency, performance etc. Compared to the traditional access control schemes, ABAC schemes are more suitable for the cloud computing environment. Application areas of ABE schemes are explored. A comprehensive analysis of ABE schemes thus presented open up several interesting and challenging research directions. These future research directions are also discussed.

REFERENCES

[1] W. Jansen, T. Grance, Guidelines on security and privacy in public cloud computing, NIST Special Publication.

[2] AWS identity and access management. URL http://docs.aws.amazon.com/IAM/latest/UserGuide/

[3] Google cloud platform - access control. URL https://cloud.google.com/storage/docs/access-control

[4] R. Wu, X. Zhang, G.-J. Ahn, H. Sharifi, H. Xie, Design and implementation of access control as a service for IaaS cloud, SCIENCE 1 (3).

[5] A. Shamir, Identity-based cryptosystems and signature schemes, Advances in Cryptology - Crypto 84, LNCS, Springer-Verlag 196 (1984) 47–53.

[6] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, C. E. Youman, Role-based access control models, IEEE Computer 29 (2) (1996) 38–47.

[7] J.Hur, D.K.Noh, Attribute-based access control with efficient revocation in data outsourcing systems, IEEE Transactions on parallel and distributed systems 22(7) (2011) 1214–1221.

[8] E. J. Goh, H. Shacham, N. Modadugu, D. Boneh, Sirius: securing remote untrusted storage, In Network and Distributed Systems Security Sympo- sium (NDSS) (2003) 131–145.

[9] M. Kallahalla, R. S. E Riedel, Q. Wang, K. Fu, Plutus: scalable secure file sharing on untrusted storage, In USENIX Conference on File and Storage Technologies (FAST) (2003) 29–42.

[10] D. R. Kuhn, E. J. Coyne, T. R. Weil, Adding attributes to role-based access control, IEEE Computer 43 (6) (2010) 79–81.

[11] L. Zhou, V. Varadharajan, M. Hitchens, Achieving secure role-based access control on encrypted data in cloud storage, IEEE transactions on informa- tion forensics and security 8 (12) (2013) 1947–1960.

[12] W. Wang, J. Han, M. Song, X. Wang, The design of a trust and role based access control model in cloud computing, in: Pervasive Computing and Applications (ICPCA), 2011 6th International Conference on, IEEE, 2011, pp. 330–334.

[13] D. Boneh, M. Franklin, Identity-based encryption from the weil pairing, SIAM Journal of Computing 32(3) (2003) 586–615.

[14] M. Green, G. Ateniese, Identity-based proxy re-encryption, International Conference on Applied Cryptography and Network Security (ACNS) (2007) 288 – 306.

[15] V. Goyal, A. Sahai, B. Waters, Black-box accountable authority identity- based encryption, Proc. of 15th ACM conf. on Computer and communica- tions security (2008) 427–436.

[16] C. Gentry, Practical identity-based encryption without random oracles, EUROCRYPT (2006) 445–464.

[17] H. Lin, Z. Cao, X. Liang, J. Shao, Secure threshold multi authority at- tribute based encryption without a central authority, LNCS INDOCRYPT 5365 (2008) 426–436.

[18] J.Li, J.Li, C. Jia, W.Lou, Identity-based encryption with outsourced revo- cation in cloud computing, IEEE Transactions on Computers 64 (2) (2015) 425 – 437.

[19] C. Gentry, A. Silverberg, Hierarchical id-based cryptography, ASI- ACRYPT, of Lecture Notes in Computer Science, Springer 2501 (2002) 548–566.

[20] D. Boneh, X. Boyen, E. Goh, Hierarchical identity based encryption with constant size ciphertext, EUROCRYPT 2005, Lecture Notes in Computer Science, Springer-Verlag 3493 (2005) 440–456.

[21] C. Gentry, S. Halevi, Hierarchical identity based encryption with polyno- mially many levels, O. Reingold (Ed.), TCC, Vol. 5444 of Lecture Notes in Computer Science, Springer 5444 (2009) 437–456.

[22] A. B. Lewko, B. Waters, Unbounded hibe and attribute-based encryption,

K. G. Paterson (Ed.), EUROCRYPT, Lecture Notes in Computer Science, Springer 6632 (2011) 547–567.

[23] K. Lee, J. H. Park, D. H. Lee, Anonymous HIBE with short ciphertexts: full security in prime order groups, Designs, Codes and Cryptography 74 (2) (2015) 395 – 425.

[24] J. Shao, Z. Cao, Multi-use unidirectional identity-based proxy re- encryption from hierarchical identity-based encryption, Information Sci- ences 206 (2012) 83–95.

[25] T. ElGamal, A public key cryptosystem and a signature scheme based on discrete logarithms, IEEE transactions on information theory 31 (4) (1985) 469–472.

[26] A. Sahai, B. Waters, Fuzzy identity-based encryption, Int'l Conf. Advances in Cryptology (EUROCRYPT) (2005) 457–473.

[27] S. Yu, C. Wang, K. Ren, W. Lou, Attribute based data sharing with at- tribute revocation, ACM Symp. Information, Computer and Comm. Secu- rity (ASIACCS) (2010) 261–270.

[28] V. Goyal, O. Pandey, A. Sahai, B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, ACM Conf. Computer and Comm. Security (2006) 89–98.

[29] J.Bethencourt, A. Sahai, B. Waters, Ciphertext-policy attribute-based en- cryption, Proc. IEEE Symp. Security and Privacy (2007) 321–334.

[30] R. Ostrovsky, A. Sahai, B. Waters, Attribute-based encryption with non- monotonic access structures, ACM Conference on Computer and Commu- nications Security (2007) 195–203.

[31] C. Wang, J. Luo, A key-policy attribute-based encryption scheme with con- stant size ciphertext, IEEE 8th Int'l Conf. on Computational Intelligence and Security (CIS) (2012) 447–451.

[32] S. Hohenberger, B. Waters, Attribute-based encryption with fast de- cryption, in Public-Key Cryptography. Berlin, Germany: Springer-Verlag (2013) 162–179.

[33] A. Ge, R. Zhang, C. Chen, Threshold ciphertext policy attribute-based en- cryption with constant size ciphertexts, Public Key Cryptography : 13th International Conference on Practice and Theory in Public Key Cryptog- raphy (PKC 2010) LNCS (2012) 336–349.

[34] L.Cheung, C.Newport, Provably secure ciphertext-policy attribute-based encryption, ACM conf. on Computer and Communication Security (2007) 456 – 465.

[35] X. Liang, Z. Cao, H. Lin, D. Xing, Provably secure and efficient bounded ciphertext policy attribute based encryption, Proc. ACM Symp. Informa- tion, Computer and Comm. Security (ASIACCS) (2009) 343–352.

[36] X. Zhao, H. Li, Achieving dynamic privileges in secure data sharing on cloud storage, Security and Communication Networks 7.11 (2014) 2211– 2224.

[37] J. Hur, Attribute-based secure data sharing with hidden policies in smart grid, IEEE Transactions on Parallel Distributed Systems 24 (11) (2013) 2171–2180.

[38] J. Hur, D. K. Noh, Attribute-based access control with efficient revocation in data outsourcing systems, IEEE Transactions on parallel and distributed systems 22 (7) (2011) 1214 – 1221.

[39] M. Chase, Multi-authority attribute based encryption, Proc. Fourth Conf. Theory of Cryptography (TCC) Springer (2007) 515–534.

[40] M. Chase, S. Chow, Improving privacy and security in multi-authority attribute-based encryption, Proc. ACM Conf. Computer and Comm. Secu- rity (2009) 121–130.

[41] S. Muller, S. Katzenbeisser, Distributed attribute-based encryption, ICISC, Lecture Notes in Computer Science, Springer 5461 (2008) 20–36.

[42] A. Lewko, B. Waters, Decentralizing attribute-based encryption, Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT) (2011) 568–588.

[43] S. Ruj, A. Nayak, I. Stojmenovic, DACC: distributed access control in clouds, IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom) (2011) 91–98.

[44] T. Jung, X.-Y. Li, Z. Wan, M. Wan, Control cloud data access privilege and anonymity with fully anonymous attribute-based encryption, IEEE Transactions on Information Forensics and Security 10 (1) (2015) 190–199.

[45] K. Yang, Z. Liu, X. Jia, X. Shen, Time-domain attribute-based access control for cloud-based video content sharing: A cryptographic approach, IEEE Transactions on Multimedia 99.

[46] G. Wang, Q. Liu, J. Wu, M. Guo, Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers, Computers and security, Elsevier 30 (2011) 320–331.

[47] G. Wang, Q. Liu, J. Wu, Hierarchical attribute-based encryption for fine- grained access control in cloud storage services, 17th ACM Conf. Computer and Comm. Security,(CCS) (2010) 735–737.

[48] Z. Wan, J. Liu, R. H. Deng, Hasbe: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing, IEEE transac- tions on information forensics and security 7 (2) (2012) 743–754.

[49] Z. Wang, J. Wang, A provably secure ciphertext-policy hierarchical attribute-based encryption, in: International Conference on Cloud Com- puting and Security, Springer, 2015, pp. 38–48.

[50] W. Teng, G. Yang, Y. Xiang, T. Zhang, D. Wang, Attribute-based access control with constant-size ciphertext in cloud computing, IEEE Transac- tions on cloud computing 99 (2015) 1–11.

[51] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, W. Xie, An efficient file hier- archy attribute-based encryption scheme in cloud computing, IEEE Trans- actions on Information Forensics and Security 11 (6) (2016) 1265–1277.

[52] M. Li, S. Yu, K. Ren, W. Lou, Securing Personal Health Records in Cloud Computing: patient-centric and fine-grained data access control in multi- owner settings, Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm) (2010) 89–106.

[53] M. Li, S. Yu, Y. Zheng, K. Ren, W. Lou, Scalable and secure sharing of personal health records in cloud computing using attribute-based encryp- tion, IEEE Transactions on Parallel and Distributed Systems 24 (1) (2013) 131–143.

[54] M. Green, S. Hohenberger, B. Waters, Outsourcing the decryption of ABE ciphertexts, in: Proc. USENIX Security Symposium, Vol. 3, 2011.

[55] B. Waters, Ciphertext-policy attribute-based encryption:an expressive, ef- ficient, and provably secure realization, Cryptography-PKC 2011. Springer Berlin Heidelberg (2011) 53–70.

[56] J. Hur, Improving security and efficiency in attribute-based data sharing, IEEE Transactions on Knowledge and Data Engineering 25 (10).

[57] S. Ruj, M. Stojmenovic, A. Nayak, Decentralized access control with anony- mous authentication of data stored in clouds, IEEE Transactions on Parallel and Distributed Systems 25 (2) (2014) 384–394.

[58] K. Yang, X. Jia, K. Ren, Dac-macs: Effective data access control for multi- authority cloud storage systems, IACR Cryptology ePrint Archive (2012) 419–429.

[59] F. Zhao, T. Nishide, K. Sakurai, Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems, Seventh Int'l Conf. Information Security Practice and Experience (ISPEC) (2011) 83–97.

[60] T. Nishide, K. Yoneyamma, K.Ohta, Attribute-based encryption with par- tially hidden encryptor-specified access structures, ACNS (2008) 111–129.

[61] E. Keita, M. Atsuko, N. Akito, O. Kazumasa, S. Masakazu, A ciphertext- policy attribute-based encryption scheme with constant ciphertext length, Lecture Notes in Computer Science 5451 (2009) 13–23.

[62] Q. Liu, G. Wang, J. Wu, Time-based proxy re-encryption scheme for secure data sharing in a cloud environment, Information Sciences 258 (2012) 355– 370.