International Journal on Future Revolution in Computer Science & Communication Engineering
Volume: 4 Issue: 12

ISSN: 2454-4248
126 – 131

A Review on Secure Access to Cloud Storage by using ABE

Dinesh Kumar Malviya
M tech Scholar
Department of CSE
Radharaman Institute of Technology and Science, Bhopal
dineshrgibpl@gmail.com

Manoj Lipton
Professor
Department of CSE
Radharaman Institute of Technology and Science, Bhopal
manojlip@gmail.com

Dr. Ravi Verma
Professor
Department of CSE
Radharaman Institute of Technology and Science, Bhopal
ravi.verma0099@gmail.com

ABSTRACT:Cloud computing is going to be very famous technology in IT enterprises. For an enterprise, the data stored is huge and it is very precious. All tasks are performed through networks. Hence, it becomes very important to have the secured use of data. In cloud computing, the most important concerns of security are data security and privacy. For access control, being one of the classic research topics, many schemes have been proposed and implemented. In this paper, various schemes for encryption that consist of Attribute based encryption (ABE) and its types KP-ABE, CP-ABE is explored. Public Key Encryption acts as the basic technique for ABE where it provides one to many encryptions, here, the private key of users & the cipher-text both rely on attributes such that, when the set of the attributes of users key matches set of attributes of cipher-text with its corresponding access policy, only then decryption is possible.

KEYWORDS:*Cloud computing, Data sharing, Data confidentiality, Security, ABE, Access control*.

*****

I. INTRODUCTION

Cloud environment [1-3] provides the new dimension of utilizing information technology resources in the business. The cloud delivers the resources based on the on-demand and pay by use model i.e. whenever we need the additional resources based on the request, the service will be allotted and charged. The cloud delivers the variety of services such as Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS) to cloud users.

SaaS provides the application to the user such as webmail, program interface, and web browser. PaaS provides the programming languages, libraries, services, and tools, etc. IaaS provides the infrastructure, such as storage, networks, and other processing and computing resources. There are various deployment models such as private, public, community, and hybrid cloud. Private cloud is owned by a single organization, whereas the public cloud is shared by multiple consumers. Community cloud means the same kind of community consumers can join and use this service. Hybrid cloud is the combination of any two above-said deployment models of the cloud. Based on the user need and requirement, the user may choose specific services and deployment model.

Cloud provides a lot of benefits such as cost savings in investments, less maintenance, flexibility, less environment impact, scalability, access anywhere, etc. Even though the cloud provides a lot of benefits, the businesses or organizations are not moving to the cloud, especially storing big data in the cloud due to security and privacy issues [4, 5].

Cloud storage [6] is mainly used to store and manage the data remotely, it allows storing the data through the internet so that users can access the data from anywhere in the world irrespective of the device and location. Cloud storage also helps to store big data for managing, processing and analyzing of data, which is quite simple without investing much because it supports the entire requirement for the same.

However, the problem with cloud storage is data privacy and access control, because storing data in the cloud means it is stored in third party Cloud Service Provider (CSP) who may not trusted. Therefore, the cloud service provider may access or disclose the sensitive data and they may share the stored data to unauthorized users for business purposes. Consider the privacy and security of the users the data must be encrypted before storing in to the cloud. Even though we encrypt the data it can be accessed by all the users, so the data access should be restricted based on user's access level and rights. Henceforth, there are two main things to be considered while storing the data in the cloud i.e. privacy of the big data and user access control [7].

The traditional symmetric and asymmetric key encryption cryptographic techniques are used for encryption. The symmetric key means the same key is used for both encryption and decryption. The asymmetric key means the public key is used for encryption and the private key is used for decryption i.e. different keys are used for both encryption and decryption. However, these encryption techniques provide the privacy, but not the access control.

The Attribute Based Encryption (ABE) is a public key cryptographic technique [8] that provides the secure data sharing among multiple users which can achieve both privacy and access control. In ABE, data is encrypted using attributes and decrypted using the secret key of a user which is associated with an access policy. The user can only decrypt when the user credentials satisfy the access policy, and it does not only

 ISSN: 2454-4248
126 – 131

provide the finegrained access control, but also provides revocation, collusion resistant, and scalability. The ABE is mainly classified into two types, Key Policy Attribute Based Encryption (KPABE) and Cipher Policy Attribute Based Encryption (CPABE).

A. Applications of ABE

A straight forward application of KP-ABE includes downloading the encrypted data from the cloud by data holder, and decrypting it to extract the unique data, then again re-encrypting it beneath the new access policies and yet again uploading it for the end user. The task becomes intimidating when the quantity of data involved is massive. Hence, KP-ABE is broadly practiced in applications of data distribution such as, Facebook, Amazon, Google Drive, and Drop box etc., where remote servers are semi-trusted, so as the access control method is insured by the encryption technique and not by the cloud storage server.

B. Advantages & Limitations of ABE

There are few common advantages & limitations of Attribute based Encryption schemes & their types which could need the enhancement in it.

Advantages

In ABE, it provides well security & privacy with fine grained access but less than KP-ABE method. Also, for huge storage of records it offers elasticity. Ultimately, advantage of ABE is that there is no one-to-one relationship in its encryption and decryption keys; means an encryption key can correspond to multiple keys for decryption. In the ABE technique, specific access policies and attribute sets could differ according to time, which is a versatile nature of the scheme. Whereas, KP-ABE has more advantage then ABE. It is further reconstructed with different techniques which provide better access control such as when it's combined with Re-encryption method. Also, it offers well security & privacy than ABE which is thus more efficiently available in version of expressive KP-ABE scheme where public parameters of constant size had been shown. Now-a-days, more feasible experiences had also been explained by adopting ABE on resource-controlled devices with IOT applications. Some advantages could be described in CP-ABE kind of encryption where it affords fine grained access alike KP-ABE. It has better efficiency in its security methods but consumes time. Similar to KP-ABE, also it can be merged to re-encryption techniques & hidden policy variants which provide adequate access control method & good security to the schemes.

Limitations

In ABE the public key of every authorized user is essential for the data owner but it prohibited in actual environment. As in ABE it suffers from high computational overhead whereas KP-ABE possesses less. And in KP-ABE, decryption of the encrypted text couldn't be decided by the person which encrypts it. It is more complex than ABE, as it is incompatible in some application because a data owner necessarily should trust the key issuer. Therefore, in CP-ABE, compared to ABE cons are limited, but in its variant of verification built on a collision-resistance hash function provides large computation overhead which is required to minimize.

II. KEY POLICY ATTRIBUTE BASED ENCRYPTION(KP-ABE)

To enable more general access controla key-policy attribute-based encryption (KP-ABE) scheme was introduced. It is the modified form of classical model of ABE. Exploring KP-ABE scheme, attribute policies are associated with keys and data is associated with attributes. The keys only associated with the policy that is to be satisfied by the attributes that are associating the data can decrypt the data. Key Policy Attribute Based Encryption (KP-ABE) scheme is a public key encryption technique that is designed for one-to-many communications. In this scheme, data is associated with the attributes for which a public key is defined for each. Encrypter, that is who encrypts the data, is associated with the set of attributes to the data or message by encrypting it with a public key.

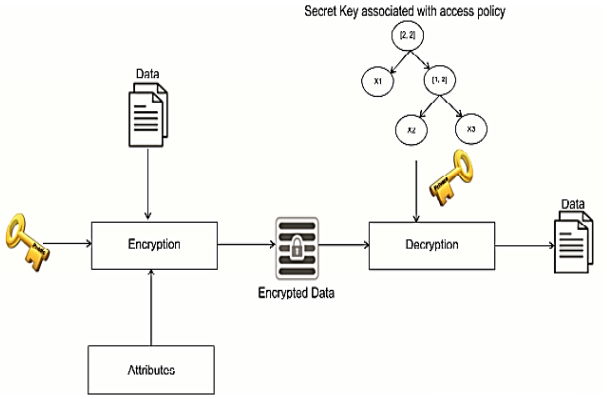

Figure 1: Key Policy Attribute Based Encrytion

Users are assigned with an access tree structureover the data attributes. The nodes of the access tree are the threshold gates. The leaf nodes are associated with attributes. The secret key of the user is defined to reflect the access tree structure. Hence, the user is able to decrypt the message that is a ciphertext if and only if the data attributes satisfy the access tree structure. In KP-ABE, a set of attributes is associated with ciphertext and the user's decryption key is associated with a monotonic access tree structure [5].

When the attributes associated with the ciphertext satisfy the access tree structure, then the user can decrypt the ciphertext. In the cloud computing, for efficient revocation, an access control mechanism based on KP-ABE and a re-encryption technique used together. It enables a data owner to reduce most of the computational overhead to the servers. The KP-ABE scheme provides fine-grained access control. Each file or message is encrypted with a symmetric data encryption key (DEK), which is again encrypted by a public key, that is corresponding to a set of attributes in KP-ABE, which is generated corresponding to an access tree structure. The

 ISSN: 2454-4248
126 – 131

encrypted data file is stored with the corresponding attributes and the encrypted DEK. If and only if the corresponding attributes of a file or message stored in the cloud satisfy the access structure of a user's key, then the user is able to decrypt the encrypted DEK.

That can be used to decrypt the file or message. KP-ABE scheme consists of the following four algorithms:

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

A. Access structures

In [1] the access tree in KP-ABE scheme defines the access scope of a user's private key. Each non-leaf node of an access structure is labelled as children of a root node. Here, every non-leaf node represents a Threshold Gate which has its own threshold value corresponding to it. Suppose a node x has number of children represented as num(x) correspondingly it has its onset value, say kx, then 0<kx<num(x).

Hence in every access tree or an access structure, each leaf node of the tree is termed by an attribute and it has its onset value kx =1. Therefore, for different onset values of an attribute provides a unique Threshold Gate. Such as for kx =1, OR gate is a Threshold Gate, whereas for kx =num(x) it provides AND gate as a Threshold Gate.

Therefore, to enable working of an access tree, there are few functions to describe its operations i.e.

- parent (x): signifies the parent of the node x in the tree i.e. we can say as root node.
- att (x): it is defined only if x is a leaf node, and indicates the attribute connected to the leaf node x in the tree.
- index(x): it represents the order of the root node x between its brothers. The nodes are numbered from 1 to num.

Here, maximum in all the schemes they have focused on the monotonic access structure. For satisfying an access structure, Let $\boldsymbol{x} = \{\boldsymbol{x1} \ldots\ldots \boldsymbol{xn}\}$be a group of events. A collection of party A ⊆ 2x is monotone for ∀B and C, if B ∈ A, B ∈ C, then C ∈ A. An access structure (respectively, monotone access structure) is a monotone collection. A of nonempty subsets of x1... xn, i.e., A ⊆ 2P\{∅}. The arrays in A are termed as authorized arrays, and the absent sets in A are called unauthorized set.

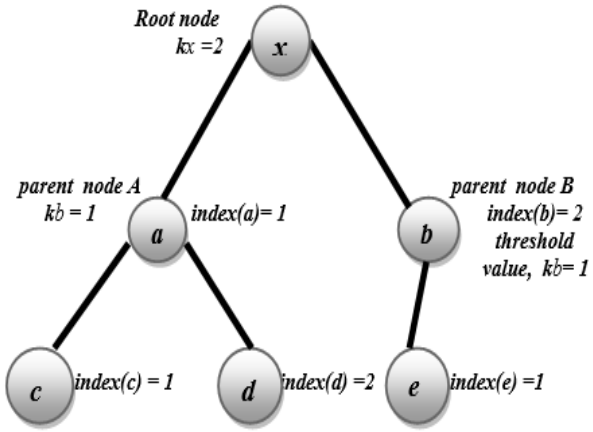

Fig: 1 Access Tree Structure

Linear secret sharing schemes

B. Limitations of KP-ABE

Encryptor cannot decide who can decrypt the encrypted data. It can only choose descriptive attributes for the data, and has no choice but to trust the key issuer. KPABE is not naturally suitable to certain applications. For example, sophisticated broadcast encryption [6], where users are described by various attributes and in this, the one whose attributes match a policy associated with a ciphertext, it can decrypt the ciphertext. KP-ABE scheme supports user secret key accountability. It is providing fine grained access but has no longer with flexibility and scalability.

III. CIPHER TEXT POLICY ATTRIBUTE BASED ENCRYPTION

In CP-ABE scheme, attribute policies are associated with data and attributes are associated with keys and only those keys that the associated attributes satisfy the policy associated with the data are able to decrypt the data. CP-ABE works in the reverse way of KP-ABE. In CP-ABE the ciphertext is associated with an access tree structure and each user secret key is embedded with a set of attributes. In ABE, including KP-ABE and CP-ABE, the authority runs the algorithm Setup and Key Generation to generate system MK, PK, and user secret keys. Only authorized users (i.e., users with intended access structures) are able to decrypt by calling the algorithm Decryption. In CP-ABE, each user is associated with a set of attributes. His secret key is generated based on his attributes. While encrypting a message, the encryptor specifies the threshold access structure for his interested attributes. This message is then encrypted based on this access structure such that only those whose attributes satisfy the access structure can decrypt it. With CP ABE technique, encrypted data can be kept confidential and secure against collusion attacks.

 ISSN: 2454-4248
126 – 131

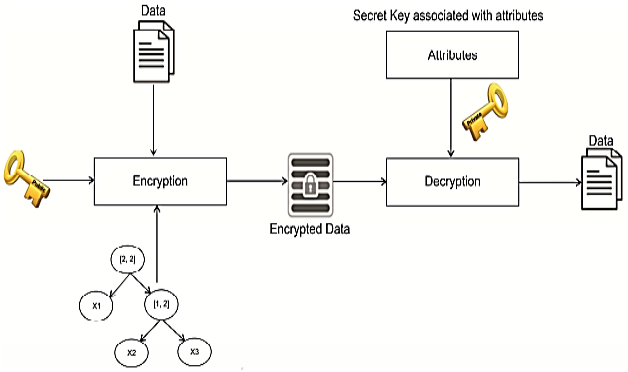

Figure 2: Ciphertext Policy Attribute Based Encryption

CP-ABE scheme consists of following four algorithms:

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

A. Limitations of CP-ABE

However, basic CP-ABE schemes are still not fulfilling the enterprise requirements of access control which require considerable flexibility and efficiency. CP-ABE has limitations in specifying policies and managing user attributes. In a CP-ABE scheme, decryption keys only support user attributes that are organized logically as a single set, so users can only use all possible combinations of attributes in a single set issued in their keys to satisfy policies. For realizing complex access control on encrypted data and maintaining confidential-ability, CP-ABE can be used. Encrypted data can be kept confidential even if the storage server is un-trusted; moreover, our methods are secure against collusion attacks. KP-ABE uses attributes to describe the encrypted data and built policies into user's keys. In other hand CP-ABE, attributes are used to describe a user's credentials. Data encryptor determines a policy for who can decrypt.

IV. LITERATURE REVIEW

Under survey cryptographic techniques proposed byvarious authors has been reviewed and a brief review on eachof them are included below.

In [2] priya et al. discussed about the various security techniques and relations based on Attributes Based Encryption, especially, the type KP-ABE over data attributes which explains secured methods & its schemes related to time specifications.

In Sadia et al. [7]analysis of security problem incloud identifies the threats mainly as inside and outsideattackers. Inside attackers includes malicious employees atclient side, malicious employees at cloud provider side andcloud provider itself. They arrived at findings that client dataon cloud data base must in the form cipher text [8].

In [9] the authors had done a survey on the variousproposed security models for cloud and found that the insiderthreats from cloud provider itself and also the use of high costpairing operations in most of security models as the demerits insecure cloud models.

Vidhate et al. [10] propose a scheme that integratescryptography with Role Based Access Control (RBAC).AES isthe encryption technique used. The scheme uses private cloudto get parameters regarding the roles for which the encryptiondocument is accessible. The owner then uploads the cipher textinto cloud by seeking a dedicated server for performingencryption. During decryption public cloud forward the requestto the private cloud; if the roles are having permission to accessthe ciphertext they will be forwarded to the dedicated server toperform decryption. Advantages of the proposed systemincludes single key for decryption and a role based access. Thesystem takes greater amount of time for role checking since ithas to wait for the replies from private cloud regarding rolebased access permission.

Chu et al. [11] proposed a key aggregate cryptosystem(KAC) to decrypt a subset of ciphertexts by generating an aggregate key for secret keys of different classes. In thisproposal sender can broadcast the document to be shared bytransferring a secret key through a public key cryptosystem.

Here, we compare different ABE schemes with advantages and disadvantages and it is shown inTable 1.

 ISSN: 2454-4248
126 – 131

Table 1: Comparative Review of ABE

Author name	Description	Advantages	Disadvantages	Security Model
Goyal et al. [12]	KPABE	Tree access structure defined on userprivate key which helps to improve thecomputational complexity than Fuzzy IBE.	Does not represent the negative constrains	Selective
Ostrovsky et al. [13]	KPABE	Access structure that includes the negativeAttributes.	More computational overhead	Selective
Lewko et al. [14]	KPABE	Achieved the user revocation with small size private keys.	The size of the ciphertext is increased linearly which depends on a number of attributes.	Adaptive
Lai et al. [15]	KPABE	Achieved the fully secure constant size ciphertext and fast encryption	The size of private key is quadratic about the number of attributes	Fully
Emura et al. [16]	CPABE	Achieved the constant ciphertext length and constant number of bilinear pairing operations.	It was less expressive and used only AND-gate.	Selective
Lewko et al. [17]	CPABE	Proposed the decentralized multiauthority CPABE.	User's attributes might be found by tracking his/her global identifier	Fully
Nishide et al.[18]	CPABE	Proposed the hidden policy scheme to maintain the policy privacy	This model proved under selectively secure	Selective

V. PROPOSED SYSTEM

According to the proposed methodology, the model explains about the flourishment of data security, its confidentiality & its integrity by using KP- ABE scheme for fine grained access in cloud computing. The proposed methodology works in following steps:

Step (1): Cloud Authority Server -- CAS when distributes PUK to cloud users then he send his PUK to Data owner.

Step (2): Data Owner --Then data owner generates SK by Elgamal algorithm and encipher it and transfers the encrypted data CT1 to CSP.

Step (3): Cloud Service Provider -- CSP thus alters the enciphered cipher-text, re-encrypts it into another cipher CT2.

Step (4): Data Centre --Then the data send by the data owner to the CSP is saved into Data centre.

Step (5): Authority Server—Hence, Authority Server generates the license for data user and after generation of license he sends it to CSP with PUK and timer starts running.

Step (6): Data User -- Thereafter Data user sends a request for retrieval of data from authority server and unless until he gets permission to retrieve by satisfying his authentication, end user cannot decrypt it.

Step (7): CSP and Timer Expires --When the data user credentials are satisfied then CSP provides encrypted data to the data end user, it generates two conditions; if Timers gives NO condition then data end user has authenticated himself as

 ISSN: 2454-4248
126 – 131

an authorized user and has time decrypt data in that interval of time and if Timers YES condition comes, then it seems that user had not decrypted the data in a certain time interval and data is self-destructed.

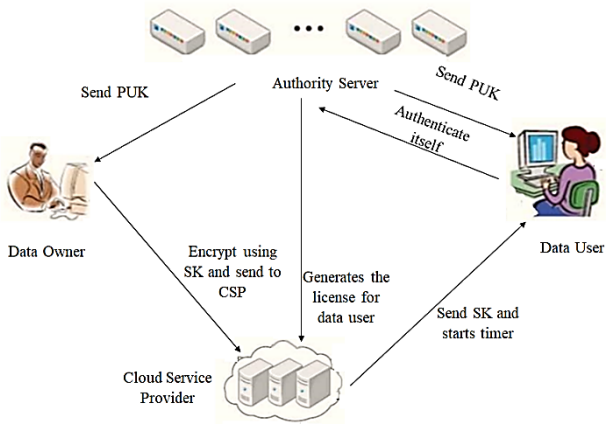

Figure 2: Flowchart of Proposed Methodology

VI. CONCLUSION

Cloud environment and ABE is a widely used prominent cryptographic technique to provide that privacy and the fine-grained access control. In this paper a comprehensive survey is given on the attribute based encryption schemes based on various characteristics and parameters such as access control, multiauthority, hidden policy in CPABE, proxy re-encryption in CPABE, revocation mechanism in CPABE and HABE. Furthermore, the advantages, disadvantages, functionalities and security model of different ABE schemes are discussed. Some of the observations and findings of different ABE schemes are as follows.

- CPABE performs better than KPABE by giving full control to data owner on their data.
- Maximum ABE algorithms were proposed based on bilinear map with variant of decisional bilinear Diffie-Hellman assumption. The most ABE schemes are selectively secure under either chosen-plaintext attack or chosen-ciphertext attack. The general method followed to prove the security is game model between challenger and adversary.
- Most commonly used access structures in CPABE schemes are tree.

Finally, it is concluded that there are some open challenges that needs to be investigated further such as efficiency and security improvements required in CPABE schemes for big data, mobile and IoT applications and develop the practical application based on ABE.

REFERENCES

[1] Maithilee Joshi, Karuna P. Joshi and Tim Finin, "Attribute Based Encryption for Secure Access to Cloud Based EHR Systems", IEEE, International Conference on Cloud Computing, 2018.
[2] Priya, A., and Tiwari, R., "A Survey: Attribute Based Encryption for Secure Cloud", IJOSTHE, 5(3), 12, 2018. Available at: https://www.ijellh.com/OJS/index.php/OJS/article/view/9467.DOI :https://doi.org/https://doi.org/10.24113/ojssports.v5i3.70.
[3] Yong Yu, Yannan Li, Bo Yang, Willy Susilo, Guoming Yang and Jian Bai, "Attribute-Based Cloud Data Integrity Auditing for Secure Outsourced Storage", IEEE Transaction on Emerging Topics in Computing, Vol. 14, No. 8, 2017.
[4] Y. Li, Y. Yu, G. Min, W. Susilo, J. Ni, K-K. R. Choo. "Fuzzy Identity-Based Data Integrity Auditing for Reliable Cloud Storage Systems". IEEE Transactions on Dependable and Secure Computing, 2017.
[5] Ming-quan Hong,Wen-bo Zhao, Peng-yu Wang, "Homomorphic Encryption Scheme Based on Elliptic Curve Cryptography for Privacy Protection of Cloud Computing", IEEE, 2016.
[6] Yong Yu · Man Ho Au · Yi Mu · Shaohua Tang · Jian Ren · Willy Susilo · Liju Dong, "Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage", Springer, 2014.
[7] Sadia Marium, Qamar Nazir, Aftab Ahmed, Saira Ahthasham Mirza Aamir Mehmood," Implementation of Eap with RSA for Enhancing The Security of Cloud Computing", International Journal of Basic and Applied Sciences, pp 177-183, 2012.
[8] Saira Varghese, S.Maria Celestin Vigila," A Comparative Analysis on Cloud Data Security", Proceedings of 2015 Global Conference on Communication Technologies, pp 507-510,IEEE, 2015.
[9] Rohini Vidhate, V.D. Shinde," Secure Role-Based Access Control on Encrypted Data in Cloud Storage using Raspberry PI" International Journal of Multidisciplinary Research and Development, Volume: 2, Issue: 7, pp 20-27,July 2015.
[10] Cheng-Kang Chu, Sherman S.M. Chow, Wen-Guey Tzeng, Jianying Zhou, and Robert H. Deng, "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage", IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 2,pp 468-477, February 2014.
[11] G. Yamamoto, S. Oda, K. Aoki. "Fast integrity for large data". Proc. ECRYPT workshop Software Performance Enhancement for Encryption and Decryption. Amsterdam, Netherlands 2007, 21-32.
[12] V. Goyal, O. Pandey, A.Sahai, B. Waters, Attribute-based encryption for fine-grained access control of encrypted data, in: Proceedings of the 13th ACM Conference on Computer and Communications Security, ACM, 2006, pp. 89-98.
[13] R. Ostrovsky, A. Sahai, B. Waters, Attribute-based encryption with non-monotonic access structures, in: ACM Conference on Computer and Communications Security Computer and communications security, ACM, 2007, pp. 195-203.
[14] A. Lewko, A. Sahai, B. Waters, Revocation systems with very small private keys, in: Security and Privacy (SP), IEEE, 2010, pp. 273-285.
[15] J. Lai, R. H. Deng, Y. Li, J. Weng, Fully secure key-policy attribute-based encryption with constant-size ciphertexts and fast decryption, in: Proceedings of the 9th ACM Symposium on Information Computer and Communications Security, ACM, 2014, pp. 239-248.
[16] K. Emura, A. Miyaji, K. Omote, A. Nomura, M. Soshi, A ciphertext-policy attribute-based encryption scheme with constant ciphertext length, Int. J. Applied Cryptography, 2(1) (2010) 46–59.
[17] A. Lewko, B. Waters, Decentralizing attribute-based encryption, in: Theory and Applications of Cryptographic Techniques, vol. 6632, Springer Berlin Heidelberg, 2011, pp. 568-588.
[18] T. Nishide, K. Yoneyama, K. Ohta, Attribute-based encryption with partially hidden encryptor specified access structures, in: International Conference on Applied Cryptography and Network Security, Springer Berlin Heidelberg, 2008, pp. 111-129.