The Research and Prospect of Secure Data Access Control in Cloud Storage Environment

Tengfei Li, Liang Hu, Yan Li, Jianfeng Chu, Hongtu Li, and Hongying Han
Jilin University, Changchun, 130012, China
Email: {tengfei13, yanli13, hanhy2112}@mails.jlu.edu.cn; {hul, chujf, lihongtu}@jlu.edu.cn

Abstract —With the rapid development of cloud computing, users are becoming to move their data to the cloud server to avoid troublesome data management at local machines and enjoy convenient service, which might cause security and privacy protection issues of users' data. To protect data security and user privacy, access control is an effective method. Generally, access control could be realized by cryptographic methods, with which users are able to access data in cloud only when they possess a certain corresponding set of credentials or attributes. In this paper, we mainly discuss the cryptography-based secure data access control for cloud storage, as well as the future prospect. Firstly, we introduce the research background of data access control. Then we study the currently existing ABE-Based schemes of data access control which are state of the art, and make some comparisons of these schemes in detail. Finally, we list some unsolved issues of these existing access control schemes for cloud storage to provide some future development direction about the further improvement.

Index Terms—Data security, cryptography, cloud storage, access control, ABE

I. Introduction

Cloud computing [1] is a set of resources and services offered through the Internet. It has been a hot topic in IT industry. Cloud computing simply means Internet computing, generally speaking, the internet can be seen as a collection of clouds. Resources of Cloud Computing are accessible for consumers as public utility services, such as processing power, storage, software, network bandwidth and so on. Cloud storage is one of the most commonly used applications, which is built on the cloud computing environment. It is a new business solution for remote backup outsourcing, as it offers an abstraction of infinite storage space for clients to host data backups in a pay-as-you-go manner [2].

As a new storage service, cloud storage has the characters of low cost, high performance and scalability, which provide a new management model of mass data storage. With cloud storage technology, individuals and enterprises could store their data remotely to third party cloud storage providers rather than maintaining local computers on their own, which significantly reduces their financial overhead of data management. Most of the data will be stored in a network computing system on top of the cloud, and the same cloud system may exist in different types of customers, enterprises, individuals. While the benefits of using a public cloud infrastructure are clear, it introduces significant security and privacy risks. Moreover, in cloud storage, the Cloud Service Provider (CSP) cannot be unconditional trusted, which is always a potential threat to data security. In order to avoid this threat, access control is a commonly used approach. [3]

For sensitive data stored in cloud, Access control is an effective approach to provide the confidence and the privacy protection. Access control is the process of mediating every request to resources and data maintained by a system and determining whether the access request should be granted or denied [4]. The access control of cloud storage permits authorized users access resources and refuse unauthorized users to access resources on cloud. It can be realized by two means [5], access control model and ciphertext access mechanism. In an access control model, several roles are created according specific access policies. The access control of cloud storage is realized by checking the role of every consumer who wants to access the cloud data. While in ciphertext access mechanism, data should be encrypted by the data owners before stored in cloud, thus the access control can be provided by the key management. Only users with the appropriate keys are allowed to access corresponding data. The former method provides simple access control for non-sensitive data. For sensitive user data, ciphertext access control method provides better and more effective privacy protection for users.

Access control of cloud storage usually adopts cryptography techniques such as symmetric encryption and public key encryption instead of the legal protection offered by contracts when enforcing access control.

The existing traditional access control schemes are generally implemented by flexible and powerful data server systems, such as Access Control List (ACL) based access control, Role-based Access Control (RBAC) [6], Flexible Authorization Framework (FAF) [7] and so on. In ACL based access control, every data object provides a corresponding authorized users list. The implement of this method is easy, but it is not practical for lack of

Manuscript received March 8, 2015; revised Sptember 23, 2015.

This work was supported by the Deep exploration instrumentation and equipment development (SinoProbe-09-01-03) under Grant No.201011078

Corresponding author email: chujf@jlu.edu.cn.

doi:10.12720/jcm.10.10.753-759

extensibility. In RBAC [6], authorizations are associated with roles, and users are made members of appropriate roles thereby acquiring the roles' permissions. This idea has been around since the advent of multi-user computing. FAF [7] can be used to specify different access control policies that can all coexist in the same system and be enforced by the same security server. However, owing to the specificity of cloud computing environment, these access control schemes are only suitable for traditional file storage systems but not applicable for access control of cloud storage.

This paper is structured as follows: Firstly, we introduce the current research of data access control and review some existing typical schemes in Section II. Then we give some related definitions and interpret some concepts in Section III. Next, we present the implementation of CP-ABE based data access control mechanism in Section IV. Finally, we list some unresolved problems and future work about data access control for cloud storage in Section V.

II. Literature Review

FIBE [8] scheme was first proposed by Sahai and Waters proposed in 2005, it is a predecessor of ABE. FIBE can be used for an application that we call “attribute-based encryption”. With this scheme, data is encrypted by data owners and identity can be used to realize the access control of data. Later in 2006, Goyal *et al.* introduced the concept of KP-ABE in [9]. They develop a new cryptosystem for fine-grained sharing of encrypted data with KP-ABE. In the cryptosystem, ciphertexts are labeled with sets of attributes and private keys are associated with access structures that control which ciphertexts a user is able to decrypt. In order to better adapt to applications of access control, Bethencourt *et al.* proposed CP-ABE scheme in [10] in 2007. In this scheme, ciphertexts are associated with sets of attributes, whereas user secret keys are associated with policies, this setting has a number of natural applications. Another possibility is to have the reverse situation: user keys are associated with sets of attributes, whereas ciphertexts are associated with policies. Only when associated attributes satisfy corresponding access control policy, user can decrypt ciphertexts. By using the techniques, encrypted data can be kept confidential even if the storage server is untrusted; moreover, the methods are secure against collusion attacks. Hereafter, series of ABE based improved access control schemes such as [11]-[14] have been proposed.

As the extension and development of IBE and ABE, a public key encryption scheme called Predicate Encryption (PE) [15], [16] was proposed to provide new method for fine-grained access control. In a predicate encryption scheme, secret keys correspond to predicates and ciphertexts are associated with attributes; the secret key SK_f corresponding to a predicate f can be used to decrypt a ciphertext associated with attribute I if and only if $f(I)$ =1. PE can be seen as a special implement of CP-ABE.

Furthermore, there are also other researches for data access control. Hierarchical encryption [17] technology was also developed as an alternate approach of access control. A representative hierarchical encryption scheme was proposed in [18] in 2007 by Jajodia *et al.* In this scheme, two layers of encryption are imposed on data: the inner layer is imposed by the owner for providing initial protection; the outer layer is imposed by the server to reflect policy modifications. The combination of the two layers provides an efficient and robust access control solution. However, there is a fatal defects that its large computing cost caused by the re-encryption [19]. In 2010, Yingjie Xiao *et al.* proposed a novel access control scheme which is implemented based on a Hierarchical and Hybrid Elliptic Curve Cryptography (HHECC) to fulfill the efficiency and security requirements in cloud [20]. The scheme is achieved by a one-way hash function on the level key, merged by the hybrid feature which denotes the combination of one-way hash, Advanced

access control.

Attribute-Based Encryption (ABE) was developed from Identity-Based Encryption (IBE). The first implementation of identity-based signatures and an email-address based Public-Key Infrastructure (PKI) was developed by Adi Shamir in 1984 [21], which allowed users to verify digital signatures using only public information such as the user's identifier. Under Shamir's scheme, a trusted third party would deliver the private key to the user after verification of the user's identity, with verification essentially the same as that required for issuing a certificate in a typical PKI.

As time goes on, some improvement schemes of IBE such as [22]-[24] has been proposed. However, defects of IBE have been exposed at the same time. On one hand, for a decryption system, the computing overhead is too large to support. On the other hand, IBE cannot protect system from collision attack initiated by multiple users.

In 2005, Amit Sahai and Brent Waters proposed Fuzzy Identity-Based Encryption (FIBE) [8] built upon several ideas from Identity- Based Encryption (IBE). A Fuzzy IBE scheme can be applied to enable encryption using biometric inputs as identities; the error-tolerance property of a Fuzzy IBE scheme is precisely what allows for the use of biometric identities, which inherently will have some noise each time they are sampled. FIBE achieves error tolerance making it suitable for use with biometric identities. Additionally, FIBE can be used for a type of application of the term “attribute-based encryption”. Hereafter, Goyal, Amit Sahai and Brent Waters improved the prototype of ABE and proposed the concept of policy tree [9], which is similar to the tree in data structure and is used to describe the decryption process. In later researches, policy tree has been also mentioned. One can specify a tree access structure where the interior nodes consist of AND and OR gates and the leaves consist of different parties. Any set of parties that satisfy the tree can reconstruct the secret.

In an ABE system [9], a user's keys and ciphertexts are labeled with sets of descriptive attributes and a particular key can decrypt a particular ciphertext only if there is a match between the attributes of the ciphertext and the user's key. The cryptosystem of Sahai and Waters allowed for decryption when at least *k* attributes overlapped between a ciphertext and a private key. While this primitive was shown to be useful for error-tolerant encryption with biometrics, the lack of expressibility seems to limit its applicability to larger systems.

III. Preliminary

In this part, we list some preliminary about access control schemes in detail mainly from four parts. Related definitions introduce some necessary definitions about the current ABE-based access control schemes. The second part provides some fundamentals about the problem of access control for cloud storage. And then, the third part mainly proposes one access control model for cloud storage based on ABE. Finally, we present the fundamental structure of access control based on ABE algorithm – access tree, and provide its operational principle.

A. Related Definitions

Definition 1: Bilinear maps

Let $\mathbf{G_1}$, $\mathbf{G_2}$ and $\mathbf{G_T}$ be three cyclic groups of some large prime order *q*, we view $\mathbf{G_1}$ as an additive group and $\mathbf{G_2}$ as a multiplicative group. We call $e: \mathbf{G_1} \times \mathbf{G_2} \rightarrow \mathbf{G_T}$ a bilinear map if it is a map with the following properties:

- Computable: There is a polynomial time algorithm to compute $e(g, h) \in \mathbf{G_2}$, for any $g, h \in \mathbf{G_1}$.
- Bilinear: $e(g^x, h^y)=e(g, h)^{xy}$ for all $g, h \in \mathbf{G_1}$ and all $x, y \in \mathbf{Z_q}$.
- Non-degenerate: if *g* is a generator of $\mathbf{G_1}$, then *h* is a generator of $\mathbf{G_2}$.

Definition 2: Access Structure [25]

Access structures are used in the study of security system where multiple parties need to work together to obtain a resource. Groups of parties that are granted access are called qualified. In set theoretic terms they are referred to as qualified sets. In turn, the set of all such qualified sets is called the access structure of the system. Less formally it is a description of who needs to cooperate with whom in order to access the resource. In its original use in cryptography, the resource was a secret shared among the participants. Only subgroups of participants contained in the access structure are able to join their shares to re-compute the secret. More generally, the resource can also be a task that a group of people can complete together, such as creating a digital signature, or decrypting an encrypted message.

Let $\{\mathbf{P_1}, \mathbf{P_2}, \cdots, \mathbf{P_n}\}$ be a set of parties. A collection $\mathbf{A} \subseteq 2^{\{\mathbf{P_1}, \mathbf{P_2}, \cdots, \mathbf{P_n}\}}$ is monotone if $\forall \mathbf{B}, \mathbf{C}$: if $\mathbf{B} \subseteq \mathbf{A}$ and $\mathbf{B} \subseteq \mathbf{C}$ then $\mathbf{C} \subseteq \mathbf{A}$. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) $\mathbf{A}$ of non-empty subsets of $\{\mathbf{P_1}, \mathbf{P_2}, \cdots, \mathbf{P_n}\}$, e.g., $\mathbf{A} \subseteq 2^{\{\mathbf{P_1}, \mathbf{P_2}, \cdots, \mathbf{P_n}\}} \setminus \{\varnothing\}$. The sets in $\mathbf{A}$ are called the authorized sets, and the sets not in $\mathbf{A}$ are called the unauthorized sets.

B. The Access Control for Cloud Storage

Cloud storage is a model of data storage where the digital data is stored in logical pools, the physical storage spans across multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store end user, organization, or application data.

The cloud storage makes data safety by dividing data into small pieces and save them to different places. It's an important method to promote the efficiency and effectiveness of the access control scheme. [3] In this field, Attribute-Based Encryption (ABE) is a commonly used encryption algorithm.

Cloud storage can be divided into three modes [26]: public cloud storage, private cloud storage, and hybrid cloud storage. Public cloud storage can provide each client with services of data isolation, access and security. Private cloud storage can fully satisfy clients' two concerning points: security and performance. In other respects, although private cloud storage has the same characteristic as the public one, its extensibility is not as well as the public one, and it costs slightly higher than the public one. Usually, hybrid cloud storage is dominated by traditional storage system or private cloud storage, public cloud storage is working as a supplement. The overall performance of ideal hybrid cloud storage must be equalized. For users, accessing to the data of private and public cloud storage should be transparent besides of a little network delay. Users having the hybrid could storage environment, can manage the internal and external resources.

Whatever cloud storage mode is adopted, security is the significant issue. The technology of access control is mainly aimed to ensure reasonable access of shared resources. It is based on identity authentication, and control access to specific resources by special authorization policy. Thus, invasion of unauthorized users or damage caused by illegal operation of authorized users can be prevented, and the resources in cloud storage can be controlled and Legitimate accessed.

C. Access Control Model

A basic access control model consists of the following three parts [27]: subject, object and action. Subject is the entity that has a number of action permissions over object. In cloud storage, a subject can be a user, a user group, an organization, a role, a process, a service and so on. Object is the entity as receptor of action and is need for protection. In cloud storage, the typical object can be data, document, services and other resources. There is no absolute boundary between subject and object. Action is the operation that a subject acts on an object, such as reading, writing, execution and so on.

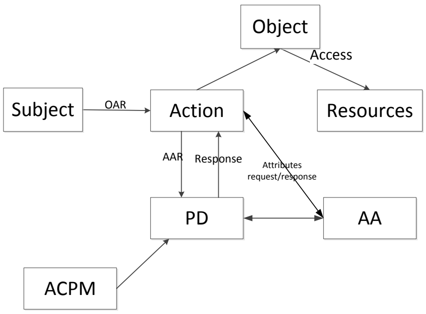


Fig. 1. Access control model based on ABE

As shown in Fig. 1, the access control model based on ABE can be described as follows. In this model, OAR represents the original access request, AAR presents the attributes access request, AA is the attribute authority, ACPM is the access control policy management, and PD presents access control policy judgment. The work process is roughly as follows:

Action accepts the OAR, according to the OAR, AAR is generated by AA. Then AAR is sent to PD, with the access policy from ACPM, PD judges whether the AAR is matchable to the access control policy, the judgment is responded to Action. Finally, according to the judgment, corresponding action is executed.

D. *Access Tree*

In the access tree construction, ciphertexts are labeled with a set of descriptive attributes. Private keys are described by a tree access structure, in which each interior node of the tree is a threshold gate and the leaf nodes are associated with attributes.

Let *T* be a tree representing an access structure. Each leaf node of the tree is associated with an attribute. Each non-leaf node of the tree represents a threshold gate, described by its children and a threshold value.

If *num(x)* is the number of children of a node *x*, and *k(x)* is its threshold value, then $0 < k(x) \leq num(x)$. When $k(x) = 1$, the threshold gate is an OR gate and when $k(x) = num(x)$, it is an AND gate. Each leaf node *x* of the tree presents a participant *part(x)*, it is described by an attribute and a threshold value $k(x) = 1$. The parent node of a node *x* is denoted by *parent(x)*. The access tree orders child nodes of each node by 1 to num. The function *att(x)* is defined only if *x* is a leaf node and denotes the attribute associated with the leaf node *x* in the tree. The access tree *T* also defines an ordering between the children of every node, that is, the children of a node are numbered from 1 to num. The function *index(x)* returns such a number associated with the node *x*, where the index values are uniquely assigned to nodes in the access structure for a given key in an arbitrary manner. [28]

A user will be able to decrypt a ciphertext with a given key if and only if there is an assignment of attributes from the ciphertexts to nodes of the tree such that the tree is satisfied. For example, the access structure that decided by Fig. 2 is $\mathbf{\{\{P_1,P_3,P_4\},\{P_2,P_3,P_4\},\{P_1,P_2,P_3,P_4\}\}}$. Only users who satisfy the structure can access corresponding data.

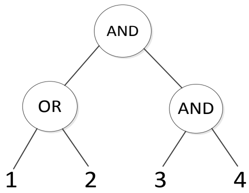


Fig. 2. Tree access structure

IV. The Analysis and Improvement of ABE-Based Access Control Schemes for Cloud Storage

A. *ABE-Based Access Control Schemes*

A data owner encrypts data, sends ciphertext to the service providers for storage, and distributes the corresponding key to authorized users. The constructed system allows a new type of encrypted access control where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt. In addition, the system allows policies to be expressed as any monotonic tree access structure and is resistant to collusion attacks in which an attacker might obtain multiple private keys.

ABE is a "one to many" encryption scheme, ciphertexts needn't encrypt only for certain specified user, so it is more applicable for cloud storage to realize data sharing and access control. A basic ABE scheme consists of four fundamental algorithms: Setup, KeyGen, Encrypt, and Decrypt. Before the algorithms are executed, the system generates $\mathbf{G_1}$ and $\mathbf{G_2}$, which are two cyclic groups of some large prime order *q*. $\mathbf{G_1}$ and $\mathbf{G_2}$ satisfy bilinear: $\mathbf{G_1} \times \mathbf{G_2} \rightarrow \mathbf{G_2}$. *d* is threshold parameter.

Setup (*d*): Setup is executed by authority. Select *y*, $t_1, t_2, \cdots, t_n \in \mathbf{Z_q}$, output the public key *PK* = $T_1 = g^{t_1}, T_2 = g^{t_2}, \cdots T_n = g^{t_n}, \mathrm{Y} = e(g,g)^y$ and a master key $MK = (y,\ t_1, t_2, \cdots, t_n)$.

KeyGen: KeyGen is executed by authority. Select a (d-1) polynomial *p* randomly, let *p (0)* = *y*, then output a private key *SK* for user *u*, $SK = \{D_i = g^{p(\mathrm{i})/\mathrm{t}_i}\}_{\forall i \in \mathbf{A_u}}$.

Encrypt: The encryption algorithm is executed by sender. It encrypts plaintext M $\in \mathbf{G_2}$ and produces a ciphertext *CT* with attributes set $\mathbf{A_c}$. Select $s \in \mathbf{Z_q}$, then $CT = (\mathbf{A_C}, \mathrm{E} = \mathrm{Y}^s\mathrm{M} = e(g,g)^{ys}\,\mathrm{M}, \{\mathrm{E}_i = g^{t_i s}\}_{\forall i \in \mathbf{A_C}})$.

Decrypt: The decryption algorithm is executed by receiver. If $|\mathbf{A}_\mathbf{u} \cap \mathbf{A}_\mathbf{C}| > d$ is satisfied, then select d attributes $I \in \mathbf{A}_\mathbf{u} \cap \mathbf{A}_\mathbf{C}$, compute $e(\mathrm{E}_i, \mathrm{D}_i) = e(g,g)^{p(i)s}$, then according to Lagrange interpolation formula, we can get $\mathrm{Y}^s = e(g,g)^{p(0)s} = e(g,g)^{ys}$, further to get $\mathrm{M} = \mathrm{E}/\mathrm{Y}^s$.

In subsequent work, to provide better access control policy, researchers clarified two complementary forms of ABE, which are called Key-Policy ABE (KP-ABE) [29] and Ciphertext-Policy ABE (CP-ABE) [14]. In KP- ABE, as is shown in Fig. 3. [30], attributes are used to annotate the ciphertexts and formulas over these attributes are ascribed to users' secret keys. Different from basic ABE, KP-ABE adopts tree structure $\mathbf{A}_{\mathbf{u\text{-}KP}}$ to describe access policy, $\mathbf{A}_\mathbf{u}$ is the set of leaf nodes. Only when a user's attributes set satisfy $\mathbf{A}_{\mathbf{u\text{-}KP}}$, the user can decrypt the ciphertext and access corresponding data. As shown is Fig. 4. [30], CP-ABE is a complementary in that attributes are used to describe the users' credentials and the formulas over theses credentials are attached to the ciphertext by the encrypting party. The ciphertext adopts tree structure $\mathbf{A}_{\mathbf{C\text{-}CP}}$ to describe access policy, with which the data sender can decide the access policy. In CP-ABE, a user's key is related to his attributes set $\mathbf{A}_\mathbf{u}$, only users whose $\mathbf{A}_\mathbf{u}$ satisfy $\mathbf{A}_{\mathbf{C\text{-}CP}}$ can decrypt ciphertext and access corresponding data.

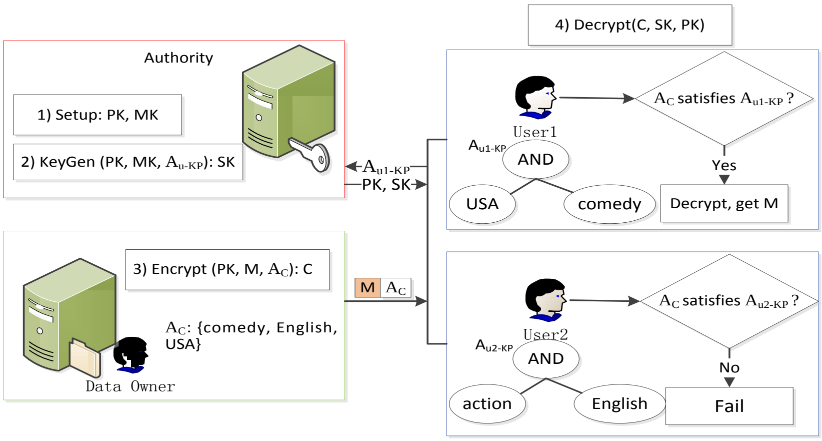


Fig. 3. KP-ABE illustration

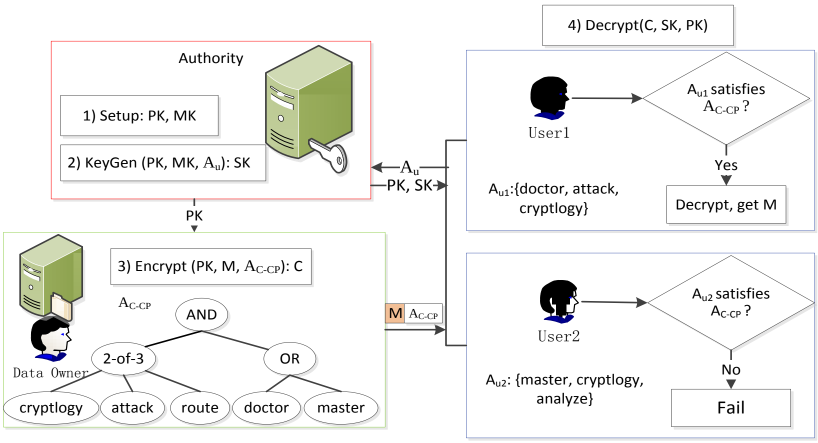


Fig. 4. CP-ABE illustration

TABLE I: COMPARISON OF KP-ABE AND CP-ABE

System	Basic ABE	KP-ABE	CP-ABE
Ciphertext	$\mathbf{\|A_C\|L_{G_1} + L_{G_2}}$	$\mathbf{\|A_C\|L_{G_1} + L_{G_2}}$	$\mathbf{(2\|A_C\|+1)L_{G_1} + L_{G_2}}$
User's secret key	$\mathbf{\|A_u\|L_{G_1}}$	$\mathbf{\|A_u\|L_{G_1}}$	$\mathbf{(2\|A_u\|+1)L_{G_1}}$
Encrypt	$\mathbf{\|A_C\|G_1 + 2G_2}$	$\mathbf{\|A_C\|G_1 + 2G_2}$	$\mathbf{(2\|A_C\|+1)G_1 + 2G_2}$
Decrypt	$\mathbf{dC_e + 2dG_2}$	$\mathbf{\|A_C\|C_e + 2\|S\|G_2}$	$\mathbf{2\|A_u\|C_e + (2\|S\|+2)G_2}$
Policy	Threshold	And, or, threshold	And, or, threshold

Table I presents the comparison of basic ABE, KP-ABE and CP-ABE, from which we can conclude that CP-ABE is more suitable for the implementation of access control. We can conclude that CP-ABE is more suitable for access control.

B. The Future Improvement

Even though the current existing schemes could satisfy the requirements of data access control for cloud storage, there are still problems to solve in the future.

- The computing consumption of encryption and decryption is large, which makes the existing schemes inapplicable for cloud environment. So the efficiency of this system is significant. To further improve the encryption scheme of access control is an effective method.
- For the privacy and security of data as well as the requirements of data owners, the revocation of authorized user is a question. So the efficient attributes revocation of ABE based data access scheme for cloud storage requires further study.
- In practical applications, cloud is accessed by users of various authorities, and the authorities are authorized by different authorized parties. The scheme in [31] adopts hierarchical tree structure to describe the hierarchical structure among attributes. However, the scheme didn't solve the hierarchical relationship among authorities. So the study of Hierarchical ABE (HABE) is necessary.

V. Conclusions

The current research of data sharing and access control is mainly focus on methods of public key encryption. As more sensitive data is shared and stored by third-party sites on the Internet, there will be a need to encrypt data stored at these sites. In which cloud storage is a typical application. With the development of cloud storage, data access control for cloud storage is significantly important.

The main goal of this paper is to study the current researches of data access control for cloud storage comprehensively. Firstly, we introduce the main representative existing schemes of data access control. We list some typical schemes as well as the realization principle of these schemes. From this part, we can draw a conclusion that the research on data access control has been going for years, and has achieved a lot of effective solutions. Secondly, we give some related concepts and their detailed description. Finally, we present a typical implement mechanism of CP-ABE based data access control. This scheme realizes the access control of encrypted data where user's private keys are specified by a set of attributes and a party encrypting data can specify a policy over these attributes specifying which users are able to decrypt. Due to the unsolved problems, further improvement of the proposed schemes is still urgent needed in future work.

References

[1] F. B. Shaikh and S. Haider, "Security threats in cloud computing," in *Proc. International Conference on Internet Technology and Secured Transactions*, Abu Dhabi, 2011, pp. 214-219.

[2] R. Buyya, C. S. Yeo, S. Venugopal, J. Broberg, and I. Brandic, "Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Computer Systems*, vol. 25, pp. 599-616, June 2009,.

[3] X. Zhang, H. T. Du, J. Q. Chen, Y. Lin, and L. J. Zeng, "Ensure data security in cloud storage," in *Proc. International Conference on Network Computing and Information Security*, Guilin, 2011, pp. 284-287.

[4] P. Samarati and S. C. de Vimercati, "Access control: Policies, models, and mechanisms," in *Foundations of Security Analysis and Design*, R. Focardi and R. Gorrieri, Eds., Berlin, Heidelberg: Springer-Verlag, 2001, pp. 137-196.

[5] G. Z. Sun, Y. Dong, and Y. Li, "CP-ABE based data access control for cloud storage," *Journal on Communications*, vol. 32, no.7, pp. 146-152, July 2011.

[6] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed NIST standard for role-based access control," *ACM Transactions on Information and System Security*, vol. 4, no. 3, pp. 224-274, August 2001.

[7] S. Jajodia, P. Samarati, M. L. Sapino, and V. S. Subrahmanian, "Flexible support for multiple access control policies," *ACM Transactions on Database Systems*, vol. 26, no. 2, pp. 214-260, June 2001.

[8] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Advances in Cryptology – EUROCRYPT 2005*, Ronald Cramer, Aarhus: Springer-Verlag, 2005, pp. 457−473.

[9] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based encryption for fine-grained access control of encrypted data," in *Proc. 13th ACM Conference on Computer and Communications Security*, lexandria, Virginia, 2006, pp. 89-98.

[10] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. on Security and Privacy*, Washington, 2007. pp. 321-334.

[11] V. Goyal, A. Jain, O. Pandey, and A. Sahai, "Bounded ciphertext policy attribute-based encryption," in *Automata, Languages and Programming*, L. Aceto *et al*., Eds., Reykjavik Iceland: Springer-Verlag, 2008, pp. 579-591.

[12] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Public Key Cryptography – PKC 2011*, D. Catalano, *et al.*, Eds., Taormina: Springer-Verlag, 2011, pp. 53-70.

[13] V. Daza, J. Herranz, P. Morillo, and C. Rafols, "Extentions of access structures and their cryptographic applications," *Applicable Algebra in Engineering, Communication and Computing*, vol. 21, no. 4, pp. 257-284, June 2010.

[14] N. Doshi and D. Jinwala, "Hidden access structure ciphertext policy attribute based encryption with constant length ciphertext," in *Advanced Computing, Networking and Security*, P. S. Thilagam, *et al.*, Eds., Surathkal: Springer-Verlag, 2012, pp. 515-523.

[15] D. Boneh and B. Waters, "Conjunctive, subset, and range queries on encrypted data," in *Theory of Cryptography*, S. P. Vadhan, Ed., Amsterdam: Springer-Verlag, 2007, pp. 535-554.

[16] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in *Advances in Cryptology-EUROCRYPT 2008*, N. Smart, Ed., Istanbul: Springer-Verlag, 2008, pp. 146-162.

[17] I. Ray, I. Ray, and N. Narasimhamurthi, "A cryptographic solution to implement access control in a hierarchy and more," in *Proc. 7th ACM Symposium on Access Control Models and Technologies*, Monterey, 2002, pp. 65-73.

[18] S. De Capitani di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: Management of access control evolution on outsourced data," in *Proc. 33rd International Conference on Very Large Data Bases*, Vienna, 2007, pp. 123-134.

[19] S. De Capitani di Vimercati, S. Foresti, S. Jajodia, *et al*., "Preserving confidentiality of security policies in data outsourcing," in *Proc. 7 ACM Workshop on Privacy in the Electronic Society*, New York, 2008, pp. 75-84.

[20] Y. J. Xia, L. Kuang, and M. Z. Zhu, "A hierarchical access control scheme in cloud using HHECC," *Information Technology Journal*, vol. 9, no. 8, pp. 1598-1606, October 2010.

[21] A. Shamir, “Identity-based cryptosystems and signature schemes,” in *Advances in Cryptology*, G. R. Blakley and D. Chaum, Eds., Berlin Heidelberg: Springer- Verlag, 1985, pp. 47-53.

[22] B. Waters, “Efficient identity-based encryption without random oracles,” in *Proc. 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, Aarhus, 2005, pp. 114-127.

[23] D. Boneh and M. Franklin, “Identity-based encryption from the weil pairing,” in *Proc. 21th Annual International, Cryptology Conference*, Santa Barbara, 2001, pp. 586-615.

[24] C. Cocks, “An identity-based encryption scheme based on quadratic residues,” in *Proc. 8th IMA International Conference on Cryptography and Coding*, Cirencester, 2001, pp. 360-363.

[25] A. Beimel, “Secure schemes for secret sharing and key distribution,” PhD. dissertation, Dept. Israel Institute of Technology, Technion, Haifa, Israel, 1996.

[26] L. F. Yin, “The analysis of critical technology on cloud storage security,” in *Proc. International Conference on Computer Sciences and Applications*, Wuhan, 2013, pp. 26-28.

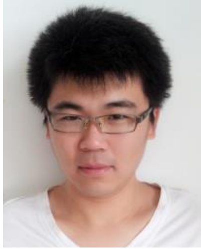
[27] M. G. Jaatun, G. Zhao, and C. Rong, “Towards an approach of semantic access control for cloud computing,” in *Proc. 1st International Conference on CloudCom*, Beijing, 2009, pp. 145-156.

[28] Z. J. Wang, “A multi-secrets sharing scheme based on access tree,” *Computer Knowledge and Technology*, vol. 8, no. 25, pp. 6002-6003, 6010, September 2012.

[29] J. G. Han, W. Susilo, Y. Mu, and J. Yan, “Privacy-preserving decentralized key-policy attribute-based encryption,” *IEEE Trans. Parallel and Distributed Systems*, vol. 23, no. 11, pp. 2150-2162, November 2012.

[30] J. S. Su, D. Cao, X. F. Wang, Y. P. Sun, and Q. L. Hu, “Attribute-based encryption schemes,” *Journal of Software*, vol. 22, no. 6, pp. 1299-1315, September 2011.

[31] J. Li, Q. Wang, C. Wang, and K. Ren, “Enhancing attribute-based encryption with attribute hierarchy,” in *Proc. 4th International Conference on Communications and Networking*, Xi’an, 2009, pp. 1-5.



Tengfei Li was born in 1990. He received the B.S. degree from the College of Software Engineering, Jilin University (JLU) and is currently pursuing the Ph.D. degree from the College of Computer Science and Technology, Jilin University. His research interests include Security of Cloud Storage, Cryptography and so on.

Liang Hu was born in 1968. He received the B.S. degree from the Harbin Institute of Technology (HIT), Ha’erbin, and the M.S. and Ph.D. degrees both from the College of Computer Science and Technology, Jilin University (JLU), Changchun. His research interests include Distributed Computing, Network Computing and Security, Data security and privacy and so on.

Yan Li was born in 1990. She received the B.S. degree from the College of Software Engineering, Jilin University (JLU) and is currently pursuing the Ph.D. degree from the College of Computer Science and Technology, Jilin University. Her research interests include Data Privacy Protection, Cryptography and so on.

Jianfeng Chu was born in 1978. He received the M.S. and Ph.D. degrees both from the College of Computer Science and Technology, Jilin University (JLU), Changchun. His research interests include Network Computing and Security, Data security and privacy and so on.

Hongtu Li was born in 1984. He received the Ph.D. degrees from the College of Computer Science and Technology, Jilin University (JLU), Changchun, China, in 2012. He has been a lecturer with the School of Jilin University since 2012. His current research interests include Network Security, Cryptography and so on.

Hongying Han was born in 1993. She is currently pursuing the B.S. degree from the College of Computer Science and Technology, Jilin University.