Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 8, August 2017, pg.102 – 108

An Efficient Ciphertext Policy Attribute based Encryption Scheme for Hierarchical File Sharing in Cloud Computing

Paravasthu R Sugana Sagar[1], Lakshman Rao Battula[2]
[1]MTech Student (CSE), 14JQ1D5807, Kakinada Institute of Technology and Science, Divili, East Godavari, Andhra Pradesh, INDIA
[2]Asst Professor, MTech CSE Department, Kakinada Institute of Technology and Science, Divili, East Godavari, Andhra Pradesh, INDIA
[1] suganasagar@gmail.com; [2] lakshmanbattula@gmail.com

Abstract*— Cloud file sharing refers to a range of cloud services that allows people to store and synchronize documents, photos, videos and other files in the cloud—and share them with other people. These services also allow users to share and synchronize data among multiple devices for a single owner. These services are accessible through desktops, notebooks, smart phones and media tablets, and provide a simple mechanism for synchronizing data across multiple devices. In cloud computing, to protect data from leaking, users need to encrypt their data before being shared. In this paper we propose an efficient encryption scheme based on layered model of the access structure is proposed in cloud computing, which is named file hierarchy CP-ABE scheme (or FH-CP-ABE, for short). FH-CP-ABE extends typical CP-ABE with a hierarchical structure of access policy, so as to achieve simple, flexible and fine-grained access control.

***Keywords*— Cloud computing, File sharing, Cipher text, File hierarchy, Encryption.**

I. INTRODUCTION

In recent years, there has been a huge proliferation of the distributed computing systems use and advancement. This increase has produced a large amount of network distributed paradigms, infrastructures and architectures such as Grid, Pervasive, Autonomic, Cloud, etc. Cloud computing refers to a network of computers, usually connected through internet, sharing an amount of resources scalable to reach the user's needs and offered by a service provider [1]. Cloud computing allows users to access software applications and computing capabilities, while using different service models: Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) [2].

These three service models are described below:

- Infrastructure as a Service (IaaS) enables the consumer to provide fundamental computing resources (such as processing, storage, networks, etc.). The consumer can deploy and run different kinds of software including operating systems.
- Platform as a Service (PaaS): This model enables the consumer to deploy onto the cloud infrastructure applications created or acquired by the consumer.
- Software as a Service (SaaS): In this model, the user can benefit of the capability of using applications already deployed on the cloud environment by a provider.

There are currently several challenges facing cloud computing mainly related to scalability, interoperability and multi-tenancy. But, the most important issues are related to the security since cloud computing as a system using internet network (such as grid computing, embedded systems, etc.) is exposed to a number of attacks [3]. The cloud computing security issues can hold back its widespread adoption. In fact, sharing resources in cloud computing causes the problem of maintaining these resources secured and protected from malicious access or use.

Due to the novel architecture of cloud computing, many traditional security issues are countered effectively. Although, its infrastructure's singular characteristics have introduced a number of distinctive security challenges. Security in general is related to the AIC triad, namely, Availability, Integrity and Confidentiality. These three properties have become the key aspects used in designing secure systems, especially, in the case of cloud computing architecture. They are Confidentiality, Integrity and availability. Confidentiality refers only to authorized parties or systems having the ability to access protected data [4]. Outsourcing data, delegating its control to a cloud provider and making it accessible to different parties increase the risk of data breach. A number of concerns emerge regarding the issues of multi-tenancy, data remanence, application security and privacy [5]. Multi-tenancy refers to the cloud characteristic of resource sharing [4]. The cloud computing architecture consists of sharing different kinds of resources to enable multiple clients to use the same resource at the same time which presents a number of privacy and confidentiality threats. Integrity means that only authorized parties can modify assets in authorized ways and it refers to data, software and hardware. Availability refers to the property of a system being accessible and usable upon demand by an authorized entity.

In several distributed systems a user should only be able to access data if a user posses a certain set of credentials or attributes. Currently, the only method for enforcing such policies is to employ a trusted server to store the data and mediate access control. However, if any server storing the data is compromised, then the confidentiality of the data will be compromised. In this paper we present a system for realizing complex access control on encrypted data that we call Cipher text-Policy Attribute-Based Encryption for cloud computing. Most existing public key encryption methods allow a party to encrypt data to a particular user, but are unable to efficiently handle more expressive types of encrypted access control. Ciphertext-policy attribute-based encryption (CP-ABE) has been a preferred encryption technology to solve the challenging problem of secure data sharing in cloud computing. The shared data files generally have the characteristic of multilevel hierarchy, particularly in the area of healthcare and the military. However, the hierarchy structure of shared files has not been explored in CP-ABE.

II. RELATED WORK

Sahai and Waters [6] introduced attribute-based encryption (ABE) as a new means for encrypted access control. In an attribute-based encryption system ciphertexts are not necessarily encrypted to one particular user as in traditional public key cryptography. Instead both users' private keys and ciphertexts will be associated with a set of attributes or a policy over attributes. A user is able to decrypt a ciphertext if there is a "match" between his private key and the ciphertext. The primary drawback of the Sahai-Waters [6] threshold ABE system is that the threshold semantics are not very expressive and therefore are limiting for designing more general systems. Goyal et al. introduced the idea of a more general key-policy attributebased encryption system. In their construction a ciphertext is associated with a set of attributes and a user's key can be associated with any monotonic treeaccess structure. The construction of Goyal et al. can be viewed as an extension of the Sahai-Waters techniques where instead of embedding a Shamir [7] secret sharing scheme in the private key, the authority embeds a more general secret sharing scheme for monotonic access trees.

Pirretti et al. [8] gave an implementation of the threshold ABE encryption system, demonstrated different applications of attribute-based encryption schemes and addressed several practical notions such as key-revocation. In recent work, Chase [9] gave a construction for a multi-authority attribute-based encryption system, where each authority would administer a different domain of attributes. The primary challenge in creating multi-authority ABE is to prevent collusion attacks between users that obtain key components from different authorities.

In Mona [10], a user is able to share data with others in the group without revealing identity privacy to the cloud. Additionally, Mona supports efficient user revocation and new user joining. More specially, efficient user revocation can be achieved through a public revocation list without updating the private keys of the remaining users, and new users can directly decrypt files stored in the cloud before their participation. Moreover, the storage overhead and the encryption computation cost are constant. In FADE [11], a secure overlay cloud storage system that achieves fine-grained, policy-based access control and file assured deletion is proposed. It associates outsourced files with file access policies, and assuredly deletes files to make them unrecoverable to anyone upon revocations of file access policies. To achieve such security goals, FADE is built upon a set of cryptographic key operations that are self-maintained by a quorum of key managers that are independent of third-party clouds. In particular, FADE acts as an overlay system that works seamlessly atop today‘s cloud storage services.

In Secured sharing of Personal Health Records [12], to achieve fine-grained and scalable data access control, they suggest attribute based encryption techniques. In this approach they focus on the multiple data owner scenario and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE (MA-ABE). The proposed architecture uses some important security services including authentication, encryption and decryption. The same is discussed along with compression in [13]. Key Policy Attribute-Based Encryption (KP-ABE), Proxy Re-Encryption (PRE) and Lazy re-encryption [13] handles many of the security issues. A main issue in the proposed system is distributed auditing. A flexible distributed storage integrity auditing mechanism, utilizing the homomorphic token and distributed erasure-coded data is referred in [14]. The design in [15] allows users to audit the cloud storage with very lightweight communication and computation cost. The auditing result not only ensures strong cloud storage correctness guarantee, but also simultaneously achieves fast data error localization.

III.PROPOSED WORK

Basic Construction

The system model (Fig. 1) in cloud computing is given, which consists of four different entities: authority, CSP, data owner and user. In this work, we assume that data owner has *k* files with *k* access levels and *M* = *{m*1, ... *,mk}* is shared in cloud computing. Here, *m*1 is the highest hierarchy and *mk* is the lowest hierarchy. If a user can decrypt *m*1, the user can also decrypt *m*2, ... *,mk*.

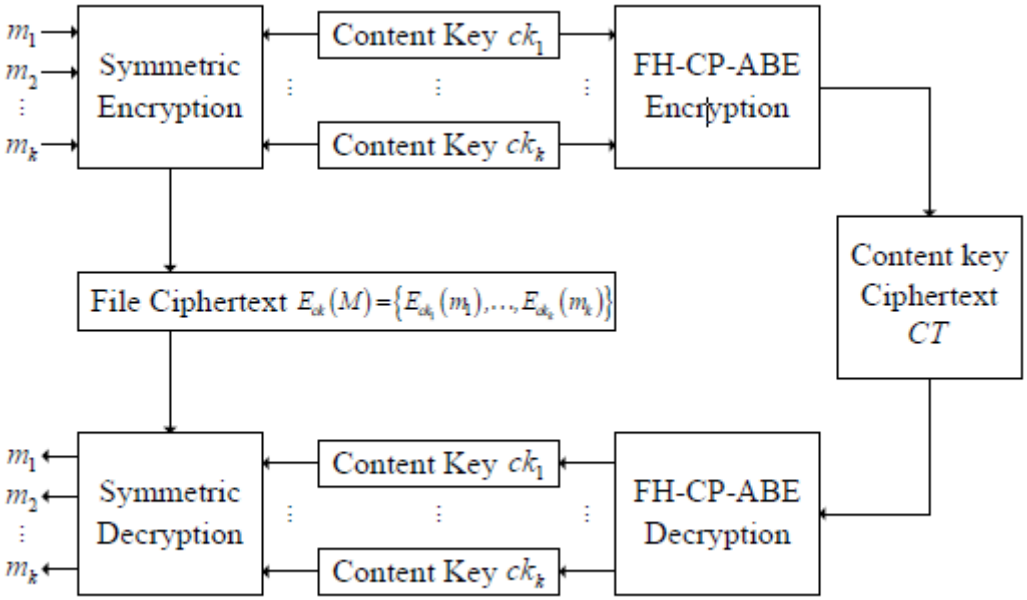

Figure 1. The system framework of FH-CP-ABE scheme

The components o our basic construction are as follows:

Authority: It is a completely trusted entity and accepts the user enrollment in cloud computing. And it can also execute Setup and KeyGen operations of the proposed scheme.

Cloud service provider (CSP): It is a semi-trusted entity in cloud system. It can honestly perform the assigned tasks and return correct results. However, it would like to find out as much sensitive contents as possible. In the proposed system, it provides ciphertext storage and transmission services.

Data owner: It has large data needed to be stored and shared in cloud system. In our scheme, the entity is in charge of defining access structure and executing Encrypt operation. And it uploads ciphertext to CSP.

User: It wants to access a large number of data in cloud system. The entity first downloads the corresponding ciphertext. Then it executes Decrypt operation of the proposed scheme.

In Fig. 1, a data owner processes the files as follows: Firstly, the data owner chooses *k* content keys *{ck*1,...., *ckk}*, and encrypts files *{m*1,...,*mk}* with the content keys by using symmetric encryption algorithm (i.e., DES, AES). The cipher texts are denoted as *Eck*(*M*) = *{Eck*1 (*m*1),...,*Eckk* (*mk*)*}*. Then, the data owner encrypts *{ck*1,..., *ckk}* using FH-CPABE

encryption algorithm and obtains an integrated cipher text of content keys *CT*. The procedures of decryption is described as below. Firstly, the user decrypts cipher text *CT* and obtains content key by using FH-CP-ABE decryption operation. Then, the user can obtain file by using symmetric decryption algorithm with content key. An example of FH-CP-ABE scheme in cloud computing is shown in Fig. 2.

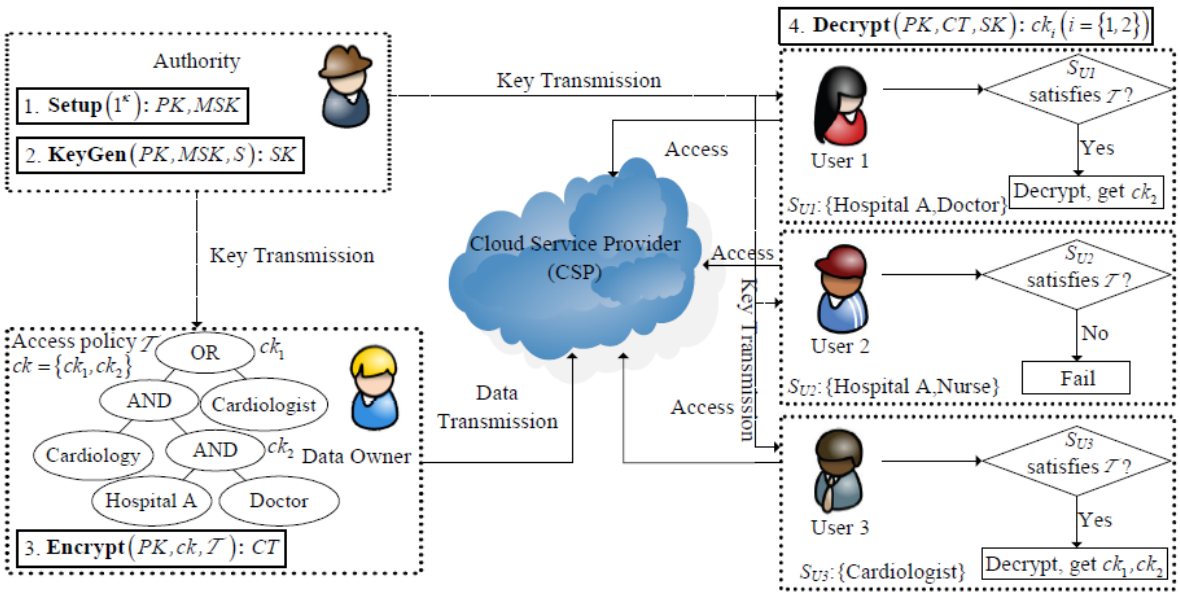

Figure 2. An example of FH-CP-ABE scheme used in cloud computing

Proposed FH-CP-ABE Scheme

In this section, the detailed construction of FH-CP-ABE scheme is first presented. The steps for construction of FH-CP-ABE scheme are as follows:

(1) **Setup**(1k). The authority runs the operation which inputs a security parameter *k* and chooses random numbers $\alpha, \beta \in Zp$. It outputs *PK* and *MSK* as the following formulas, respectively.

$$PK = \{\mathbb{G}_0, g, h = g^{\beta}, e(g,g)^{\alpha}\}$$
$$MSK = \{g^{\alpha}, \beta\}$$

(2) **KeyGen**(*PK;MSK; S*). The authority executes the algorithm which inputs a set of attributes $S(S \subseteq \tilde{A})$ and creates a secret key *SK* about the set as the formula, where $r \in Zp$ and $rj \in Zp$ are randomly chosen for each user and each attribute $j \in S$.

$$SK = \left\{ \begin{array}{l} D = g^{\alpha} \cdot h^{r}, \\ \forall j \in S : D_j = g^{r} \cdot H_1(j)^{r_j}, D_j' = h^{r_j} \end{array} \right\}$$

(3) Assume that a data owner shares *k* files, i.e., *M = {m*1,..,*mk}*, with *k* access levels. Then, the corresponding content keys *ck = {ck*1,.., *ckk}* are encrypted as the following **Encrypt** operation. **Encrypt**(*PK, c, T*). The public key *PK*, content keys *ck = {ck*1,.., *ckk}*, and a hierarchical access tree *T* are taken as input. The algorithm outputs an integrated ciphertext *CT*. Then, it computes ˜ *Ci* and *C 'i* for all *i* = 1, 2,... *k* as the formula

$$\tilde{C}_i = ck_i e(g,g)^{\alpha s_i}, C_i^{'} = g^{s_i}$$

Let *Y* be the set of leaf nodes in *T* . Then, data owner computes *C*(*x,y*) and *C'* (*x,y*) for all nodes (*x, y*) in the set of *Y* as the formulas:

$$C_{(x,y)} = h^{q_{(x,y)}(0)}$$

$$C_{(x,y)}^{'} = H_1(att(x,y))^{q_{(x,y)}(0)}$$

Then, data owner computes ˆ *C*(*x,y*)*;j* for each node (*x, y*) in the set of *X* and all *j* = 1, 2,..as the formula

$$\hat{C}_{(x,y),j} = \left\{ \begin{array}{l} e(g,g)^{\alpha \cdot (q_{(x,y)}(0) + q_{child_j}(0))} \\ \cdot H_2(e(g,g)^{\alpha q_{(x,y)}(0)}) \end{array} \right\}$$

Data owner outputs the integrated ciphertext *CT* as the formula:

$$CT = \{\mathcal{T}, \tilde{C}_i, C_i^{'}, C_{(x,y)}, C_{(x,y)}^{'}, \hat{C}_{(x,y),j}\}$$

(4) **Decrypt**(*PK,CT, SK*). A user needs the public key *PK* and *SK* described by *S* to decrypt *CT*. Similar to CP-ABE, a recursive operation *DecryptNode*(*CT, SK,* (*x, y*)) should be first defined. If (*x, y*) is a leaf node, we let *i* = *att*(*x, y*) and define *DecryptNode*(*CT, SK,* (*x, y*)) as below. If *i* =∈ *S*, *DecryptNode*(*C,SK,*(*x,y*)) = *null*. Otherwise, the operation *DecryptNode*(*CT,SK,*(*x,y*)) is obtained by the formula:

$$\begin{aligned} & DecryptNode(CT, SK, (x,y)) \\ &= \frac{e(D_i, C_{(x,y)})}{e(D_i^{'}, C_{(x,y)}^{'})} \\ &= \frac{e(g^r H_1(i)^{r_i}, h^{q_{(x,y)}(0)})}{e(h^{r_i}, H_1(att(x,y)^{q_{(x,y)}(0)}))} \\ &= e(g,g)^{r\beta q_{(x,y)}(0)} \end{aligned}$$

IV. CONCLUSIONS

With the thriving growth of the cloud computing, the security and privacy concerns of outsourcing data have been increasing dramatically. However, because of delegating the management of data to an untrusted cloud server in data outsourcing process, the data access control has been recognized as a challenging issue in cloud storage systems. One of the

preeminent technologies to control data access in cloud computing is Attribute-based Encryption (ABE) as a cryptographic primitive, which establishes the decryption ability on the basis of a user's attributes. Cipher text-Policy Attribute-Based Encryption (CP-ABE) is a type of ABE cryptosystem in which cipher texts are associated with policies, whereas the user's private key is identified with a set of descriptive attributes as a string. An encryptor specifies a policy that private keys must satisfy to decrypt the message by using an access tree structure. A user is able to decrypt a ciphertext with a given key if and only if the data access structure is satisfied by the attributes associated with the private key to nodes of the tree. CP-ABE is more suitable to control data access in cloud storage systems than others because it gives data owners the ability to select an access structure based on attributes and to encrypt data under this structure regarding to the corresponding public attributes. In this paper, we propose the layered model of access structure to solve the problem of multiple hierarchical files sharing. The files are encrypted with one integrated access structure. It should be noticed that the proposed scheme differs from the subsequent CP-ABE schemes, which utilize the user layered model to distribute the work of key creation on multiple domain authorizations and lighten the burden of key authority center.

REFERENCES

[1] M. Koehler and S. Benkner, "VCE-A Versatile Cloud Environment for Scientific Applications." The Seventh International Conference on Autonomic and Autonomous Systems (ICAS'11) IARIA, 2011, pp. 81-87

[2] A. Tchana, L. Broto, and D. Hagimont, "Fault Tolerant Approaches in Cloud Computing Infrastructures", The Eighth International Conference on Autonomic and Autonomous Systems ICAS'12), 2012, pp. 42-48.

[3] A. Jemai, A. Mastouri, and H. Elleuch, "Study of key pre-distribution schemes in wireless sensor networks: case of BROSK (use of WSNet)", International Journal of Applied Mathematics & Information Sciences (AMIS'12). 2012, pp. 655-667.

[4] D. Zissis and D. Lekkas. "Addressing cloud computing security issues". Future Generation Computer Systems, 28(3), 2012, pp. 583-592

[5] Cloud Security Alliance. Top threats to cloud computing, Cloud Security Alliance, 2010.

[6] A. Sahai and B. Waters. Fuzzy Identity Based Encryption. In Advances in Cryptology – Eurocrypt, volume 3494 of LNCS, pages 457–473. Springer, 2005

[7] A. Shamir. How to share a secret. Commun. ACM, 22(11):612–613, 1979.

[8] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure Atrribute-Based Systems. In ACM conference on Computer and Communications Security (ACM CCS), 2006.

[9] M. Chase. Multi-authority attribute-based encryption. In (To Appear) The Fourth Theory of Cryptography Conference (TCC 2007), 2007.

[10] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan, "Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud‖, IEEE Transactions on Parallel and Distributed Systems. 2013.

[11] Yang Tang, Patrick P.C. Lee, John C.S. Lui and Radia Perlman, ―Secure Overlay Cloud Storage with Access Control and Assured Deletion‖, IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 6, November/December 2012.

[12] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou, ‖ Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption‖,IEEE Transactions on Parallel and Distributed Systems Vol. 24, Issue No. 1,2013.

[13] S Sajithabanu and Dr. E George Prakash Raj, ―Data Storage Security in Cloud‖, IJCST Vol. 2, Issue 4, Oct . - Dec. 2011

[14] Cong Wang, Qian Wang, Kui Ren, Ning Cao and Wenjing Lou,2012 ‖Toward Secure and Dependable Storage Services in Cloud Computing‖, IEEE Transaction on Services Computing, VOL 5, Issue 2, April-June.

[15] R.Uma Maheswari and M.Chinnadurai,2014 ― Secured Resource Sharing in Cloud Storage using Policy based Access Control‖, International Journal of Emerging Technology and Advanced Engineering.

