International Journal of Grid and Distributed Computing
Vol. 9, No. 7 (2016), pp.237-242
http://dx.doi.org/10.14257/ijgdc.2016.9.7.24

# Study on Data Privacy Monitoring of Cloud Computing and Access Control Strategy

Ke Lu

*Jiaozuo University.Henan .China*
*Corresponding E-mail:Kelu221@126.com*

***Abstract***

*With the development of information network, cloud computing has been widely spread, however the cloud security incidents are followed, which brought serious threat to the user data privacy security in cloud computing. In order to improve the reliability of cloud computing services, preventing malicious attacks, joint attacks, illegal access, tampering with data and other malicious acts of information and other malicious acts, we must use an effective method to solve these problems, so that the user's privacy data can be protected. In this paper, it takes rhe overview of cloud computing as the breakthrough point, describing the data security threats that the cloud computing has to face, discussing the privacy protection methods under the computer environment, demonstrating the data privacy protection technology, so as to enhance the user's safety index of using cloud computing.*

***Keywords****: Cloud computing; Data; Access control*

## Introduction

In recent years, with the development of computer and network technology, people began to seek a way to share the global range of computer resources, at present, the current popular technology in the field of IT such as cloud computing is born in such kind of demand. It is a new kind of network computing model which is proposed after distributed computing,parallel computing and grid computing. It can combine these together and make these modes commercialized by using a large number of computer resources, that is to say, it can combine the software and hardware resources and information together by the use of the network, so as to form "cloud" in a large scale. Therefore, the development and popularization of cloud computing is facing many key problems, the first of which is the security issues of cloud computing data. And the importance of cloud security issues will be accompanied by the growing popularity of cloud computing that has gradually increased and become an important factor to restrict the development of cloud computing.

### The Overview of Computer Clouding

Cloud computing is the intensive product of the network resources combined with grid computing, distributed computing, parallel computing, utility computing utility computing, network storage, network storage technologies, virtualization and load balance as well as computing resources and storage equipment, *etc*.. Cloud computing using the Internet to complex processing procedures by distributed processing technology division, to pay to the cloud computing center of search, calculation and analysis. Finally, the calculation results through the cloud feedback to hire service cloud users, so as to realize the software and hardware resources, open platform and application service sharing based on the Internet. The main feature of cloud computing is the use of centralized management of resources pool, through the virtual storage technology and

ISSN: 2005-4262 IJGDC

distributed deployment of cloud services, to provide users with a huge service center to facilitate the user's centralized storage, online office, shared resources and other applications. And with the help of network communication equipment, the user can according to the business needs of the selective service, and according to the use of the amount of pay, in order to save investment costs while enjoying high performance cloud services.

**Threat of Data Security that Cloud Computing Faced**

Due to the huge size of the cloud computing system, the application of a lot of users and privacy data is existed, at the same time, the cloud computing has unprecedented openness and complexity, its security is faced with more severe challenges than the traditional information systems, which can be shown in Figure 1.

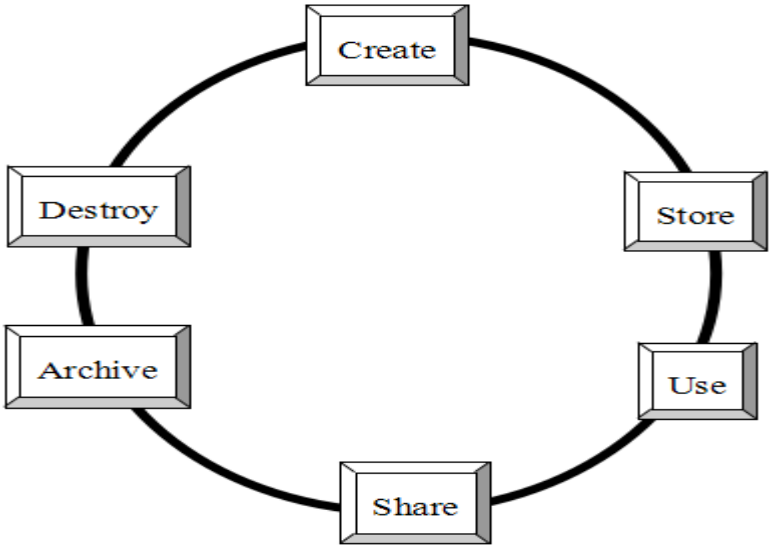


**Figure 1. The Security Life Cycle of Data**

At present, cloud computing security problems mainly manifested as the following seven aspects: (1) Data loss and leakage; (2) Shared technology vulnerabilities; (3) The reliability of suppliers is not easy to be assessed; (4) The identity authentication mechanism is weak; (5) Unsafe application program interface; (6) Incorrect operation of cloud computing; (7) Unknown risks. The transparency of the service can make the user to use the Web front interface without knowing what kind of platform or security mechanism is used by the supplier.

**Privacy Protection Method in Cloud Environment**

In cloud environment, the user data can be hosted in the cloud server management terminal, users can not check the operation of the system in the real-time, which also can not detect the operation condition of network, the cloud service can providers the users with managing and storing the user data. Thus the cloud environment of the data privacy should need users and the cloud service providers to complete together. Cloud computing can take a centralized approach to store, manage resources and data, while security should depend on the reliability of the cloud computing service center. Business data and information can be hosted in the cloud, the service provider has a higher priority than the user to deploy the service system. Service providers must provide a secure cloud platform, so as to ensure that users in the use of cloud services provided by the application which

 

van not be a failure, even if there is a sudden situation, it needs to do a good job with data recovery; secondly, it needs to provide a relatively secure network transmission, so as to prevent data privacy is stolen or illegal access during l the transmission stage.In short, cloud service providers need to consider the exception in the case of the technology, so as to provide security of cloud services.[1]

## Analysis on Data Privacy Protection Technology

### Analysis of Access Control Technology

In order to make reasonable access to the shared information, the resource manager puts forward the security level and security policy to regulate the user to read the shared information. At present, the problem of data security in the cloud computing environment is urgently to be solved. As one of the five security service problems, access control services will also be the key technology to solve the privacy of user data in cloud computing.[2] Since access control technology can limit the illegal access to the cloud data according to the reasonable security policy, which can ensure the security of cloud users in the cloud computing platform.[3] Meanwhile, the aim of access control technology is designed to prevent unauthorized access that the subject (users or process) can limit the access to the object (file or data), so as to ensure the system that can be properly used. Through clearing the users and process, some files and data can be operated with the resources, so as to ensure the subjects' access to the object is legal in the system.[4]

### Traditional Access Control

From the proposed research of access control technology to the present, a variety of excellent access control technology have been studied for protecting the system's security, they are able to prevent the illegal usage of the object in the system. Next we can analyze the following three kinds of classical access control.

### Discretion Access Control

Access Control Discretion can be shorted for (DAC), the owner of the object can restrict the possession of the object with the accessing rights, the feature of autonomy can be reflected in the object of the owner that can became the object of the management. This kind of access control mechanism is with high flexibility, the nature of the DAC model is worthy of the access control in cloud computing, so as to provide users with the ability to manage their own data.[5]

### Mandatory Access Control

Mandatory Access Control can be shorted for MAC, in each of the subject S and object O are being enforced on a specific security level (SC), MAC can be controlled by the security level of the subject and the object. The feature of mandatory lies in the subject S cannot realize its usurp power by enhancing its security level or reducing the security level of the object O, the security level of all entities can only be restricted by system administrator according to the provisions of the restrictive rules.[6]

The basic idea of mandatory access control is to mark the safety level of the subject and the object, so as to control information that can only be obtained from the entity with low security level to that with high security level.[7] The security level can generally be divided into four grades , namely: unclassified, confidential, secret and top secret, which can use ">" form of partial ordering relation to show the relationship, namely, $TS>S>C>U$. On one hand,the security level of the object can be called as security classification, on the other hand, the security level of the subject can be called as security

clearance. The grid that is formed by security label can be shown in Figure 2.

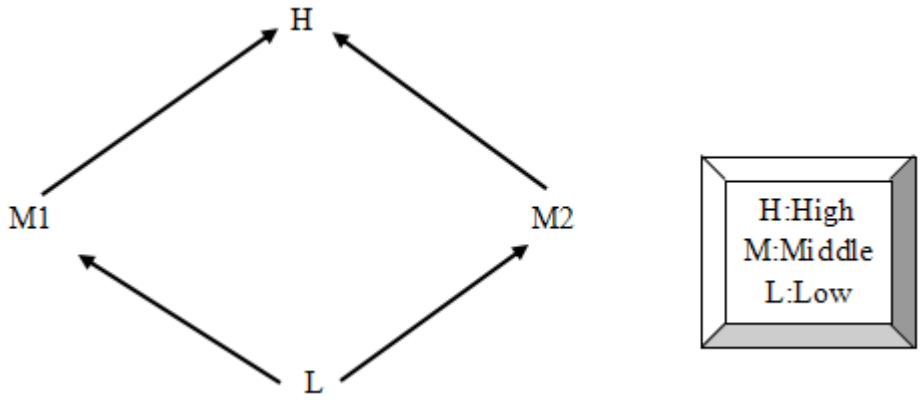


**Figure 2. Grid of Mandatory Access Control**

**Role-Based Access Control**

Role-Based Access Control can be shorted for RBAC, acting as a bridge between the subject and the object, assigning the authority to the roles, granting the user's authority to the users in the system. In the User Assignment, a user can be assigned with multiple roles, and a role can be granted to a role with multiple operating licenses. While in Permission Assignment, one role can can be granted with many operating permission. Therefore, it can combine the users and operating permission together through the associated roles. Through assigning the user's role or canceling the roles, it can complete the grant and recovery of user privileges. It can be shown in Figure 3, which can represent the relationship between the three entities in RBAC, the set of user (U), the set of role (R), and the set of permission (P). Among them: (1) The user is the subject of the access system; (2) The role is the carrier of the authority assignment, which can be used to represent a class of users; (3) The permission can represent the right of access to the system.

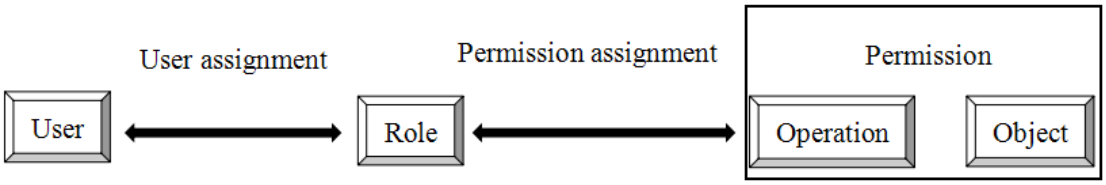


**Figure 3. The Permission Relationship between Users and Roles in RBAC**

**Confusion Algorithm of the Data Slices of Tenants Privacy Relationship**

In order to ensure the safety of the tenants' data privacy, when it goes on with the tenant's data slice, it can divide the data that may result in the leakage of tenants' data privacy to the different slices of tenants' data, the way of storing this kind of slice can ensure the safety of the tenants' data privacy by means of separating tenants' data privacy. For the feature of the separation of the tenants' data privacy, confusing the relationship between the slices of the tenants' privacy data,so as to keep the confusion strategy in the trusted third party, which can realize the confusion of the data slices and prevent the leakage of tenants' data privacy. The slices of tenant's data privacy can be marked as *DaPrild*, which can indict the slices of the tenants' privacy data, namely, *DaPrild* can be

 

represented as follows:

$$DaPrild=E_{key}(Id_{TTP} \oplus a^{DSld})$$

Among them, E can represent the dynamic multiplication function of the slicing strategy of the tenants' privacy data; while key is the corresponding key; $Id_{TTP}$ can be used to label each data record in accordance with the data privacy policy. *DSld* is the secondary serial number of data slices; while a is the generator of the slicing strategy of the tenants' privacy data.

**The Implementation of Access Control**

The reference monitor of DIFC-AC can adjust the data flow in the system by using arbitration and intercepting system calls in the kernel data. According to the label and authorization conditions and access control policies, it can control the process, so as to read and write data. At present, it can increase the visiting control strategy in the following four categories, when the process of data does not have the accessing right, it can directly return to error; when the process has access to the data, it can use the original system call to return to the original results, after having the process of data operation, the label of their own processes needs to be updated, therefore, the strategy of accessing control decision partly needs API that is provided by the management part of the label's to update the process. (1) File IO. It can mainly adjust sys_read and sys_write and other system to have interception. According to the tagging process and global authorization list of condition doesn't have, it can return to -EACCESS error, or it can revise the corresponding labels of process, which can represent that the process has read the data and return to the original read system to call; in the sys_write, it can determine whether the process has write permissions. If it does not have, then it returns to -EACCESS error, otherwise, it returns to the original write system. (2) Process control. It aims at intercepting the system such as sys_clone, sys_execve and other systems. In sys_clone, according to the label that is set for the sub process based on the current parent process. In sys_execve, set up the label for the sub process according to the label of program files of the sub process. (3) Process communication. It aims at intercepting sys_pipe, sys_mmap2 and other system calls. These pipelines belong to the controlled pipeline, in accordance with the process of label as well as the licensing condition to adjust for the communication of the process. (4) Network transmission. It aims at intercepting sys_socketcall, sys_sendfile system calls. In sys_sendfile, making determination to read and write according to the permission, so as to intercept the disallowed operation. In sys_socketcall, according to the specific function of the call, particularly connect and accept can have control over the data flow. If the connection of the host computer has not been authenticated, the data communication can be interrupted, if the other is the authenticated host computer by the DIFC-AC host computer, then the corresponding data that can be transmitted to the label and then data can be transmitted. Among them, the authentication of the host computer, as well as the transmission of data labels need to be completed by the help of transmitter that is deployed in the user mode.

When the cloud joint node A needs to transmit data to the joint node B, it will experience the process that can be shown in Figure 4: (1) Host computer A and host computer B to establish a TCP connection I for the transmission of D with the labeled data, host computer A can call connect, while host computer B can return from the accept function; (2) The reference monitor of host computer A can send the label Ld to the transmitter; (3) The transmitter of host computer A and the transmitter of host computer B can establish safe connection, which can transfer the label information to the transmitter of host computer B; (4) The transmitter of host computer B can send the label to the reference monitor, noticing it establish the connection of the socket descriptor label to modify it into Ld. After that, the data from the host computer A to the host computer B can be controlled and protected in the host computer B.

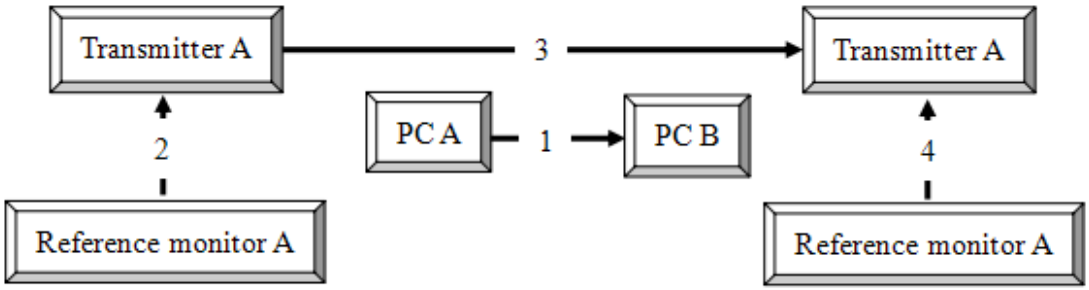


**Figure 4. DIFC-AC The Transferring Data between Host Computer**

## Conclusion

Cloud computing can combine hardware, software as well as a large number of IT resources in the form of services, which can provide them to the user through the network. In cloud computing service mode, the user can put data and application hosting to the cloud, the transparent feature of cloud services can make user lose the control over the data, due to the cloud service provider's credibility is not easy to be assessed, so the problem of data security has become the primary concern for users in cloud computing environment. The essence of data security in cloud computing is the trust management between the data owner and the service provider.The user and cloud service providers need to form a certain data usage constraints. Through the means of the credit and technical constraints, the data can be used to promote the legitimate usage of data that can not be abused and destroyed. As for the users, who can choose the trust of the service side, so as to get the security mechanism that two sides are satisfied with and achieve the maximum protection.

## References

[1] Chang YC, Mitzenmacher M. 2005. Privacy preserving keyword searches on remote encrypted data. In: Ioannidis J, Keromytis AD, Yung M, eds. vol.3531, pp: 442-455.
[2] Ostrovsky R, Sahai A, Waters B. 2007. Attribute-Based Encryption with Non-monotonic Access Structures Proceedings of the 14th ACM Conference on Computer and Communications Security, Alexandria. vol.14, pp:195-203.
[3] Bethencourt J, Sahai A, Waters B. 2007. Ciphertext-Policy Attribute-based Encryption. vol.26, pp:321-334.
[4] Crampton J, Martin K, Wild P. 2006. On Key Assignment For Hierarchical Access Control. vol.19, pp:98-111.
[5] Damiani E, Vimercati S D, Foresti S, *et al*. 2007. An Experimental Evaluation of Multi-key Strategies for Data Outsourcing. vol.36, pp:385-396
[6] Goyal V, Pandey O, Sahai A, *et al*. 2006. Attribute-Based Encryption for Fine-grained Access Control of Encrypted Data. vol.13, pp:89-98.
[7] [7] Gong L, Qian X. 1996. Computational Issues in Secure Interoperation. IEEE Transactions on Software Engineering, vol.22, pp: 43-52.

## Author

**Ke Lu**, male, department of international education,Jiaozuo University. Master Engineering. Research Field: computer network

 