Accounting Informationization Hierarchical Data Safety and Prevention Based on Cloud Computing Environment

Qin Hao, Zhang Shihong

Department of Forensic Technology, Hainan Vocational College of Political Science and Law

Haikou, China

e-mail: qinhao3806@163.com,e-mail: 251618193@qq.com

Keywords: cloud computing; accounting informationization; data security

Abstract. To solve the problem of accounting informationization hierarchical data security, this paper, starting from the basic architecture and data distribution of cloud computing environment , will analyze the accounting data security of the cloud, pipes, and the client, construct accounting informationization flow security environment with multi-level data security measures put forward. Researches have shown that the accounting information flow security environment made under the cloud computing has a strong safety performance and its data protection has good application value.

1 Introduction

With the multiple application of cloud computing technology and the constantly dropping cost of the hardware, many large-scaled ERP software providers like SAP, UFIDA and Kingdee choose accounting information services based on cloud computing , more and more business organizations have approved and used enriched cloud computing resources for business processing and information interaction. According to statistics, in 2013, the total cloud computing data volume is 1.8 ZB, and IDC has predicted that the total amount of data generated over the next eight years will be more than 40 ZB. With the high-speed development of cloud computing in the field of information technology, some key problems need to be solved, among which the security issues of cloud computing is the main problem. According to a report of IDC, at present 87.5% of the users regard "security issues" as the main obstacle to adopt cloud services. The settlement of the security problems is a key element related to whether cloud services can be recognized by the users, but the accounting data generating and processing ways under the cloud computing framework are different from the traditional computing mode which is based on the host, so if we want to explore the data security issues, we must firstly need to know about the basic structure of the cloud computing accounting information and the characteristics of its data distribution.

2 Cloud computing accounting information basic structure and data distribution

As for the physical level, the cloud computing accounting information basic structure as shown in figure 1, it can be divided into the cloud, pipe and the client according to the resource types. As the main body of accounting data computing and storage resources, the cloud is used for the deployment servers and storage devices; Pipe line is the main body of all kinds of resources to build accounting information transmission network, including switches, routers and other network communication equipments; The client is the entrance for the users to cloud computing accounting information system, including all kinds of terminal equipments: desktop computers, notebook computers, mobile phones, tablets, etc., which is the main body of the human-computer interaction interface. All levels have mutual cooperation relationship on accounting data processing [1]. All in all, the cloud is responsible for the storage, retrieval and analysis of accounting data, pipe is in charge of accounting data transmission, while the client is for the presence of the accounting data.

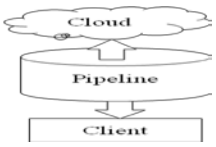

Figure 1. Cloud computing accounting informationization framework diagram

The generation and management way of the accounting data under the environment of the cloud computing is different from the traditional computing architecture based on the host. The latter is a kind of computing architecture like a lonely island and the body of computing and storage of accounting data is the client computer. There may be a network connection between different computings. If there are the share of the accounting data but the transmission channel of the accounting data for the request and response, pipeline maintenance data will not be produced. The three parts of the cloud computing architecture generate the accouting data and the client generates the user data; Pipeline is responsible for carrying the accounting data of the business request and response. At the same time, it can also generate the operational data; While the cloud can analyze and calculate according to the client and the pipe data so as to generate a new data which is more valuable. The main body of the calculation is concentrated in the cloud and the client is the main part of the data collection and display, which will weaken the function of calculation. Therefore, in order to ensure that the accounting information system under the cloud computing environment is safe and reliable, we need to protect the three parts at the same time; Moreover, there are many divisions among the three parts： the business division of labor， software deployment and hardware configuration, so the safeguard measures are different.

3 Cloud computing accounting information data security and prevention

A. Cloud accounting data security

The cloud often deploy server-side programs of big accounting information software, such as ERP, CRM, AIS system, etc. At present, enterprise software providers like Kingdee and UFIDA offer a SAAS software system which is based on cloud computing architectures. For example, the UAP platform of UFIDA deploy itself on the cloud virtual resource pool (operating system, database, hardware resource virtualization), quickly providing dynamic, flexible, elastic, virtual, sharing and efficient computing resources services for enterprise cloud application service. The characteristic of the cloud computing is to compute and store the cloud equipment, so the cloud equipment saves a large amount of accounting data information. In the cloud computing system, the cloud data is the final and effective data. Once lost or tampered with, it may lead to unrecoverable huge losses, so the cloud data security is the key of the whole system's safety and reliability [2].

The reliability of the cloud accounting data can be divided into three levels.

1) Bottom ——Hardware Layer Security

It is mainly responsible for the reliable preservation of accounting data and the user's accounting data will de finally stored in the cloud storage medium, which usually contains the NAS or SAN storage. Generally speaking, the average annual failure rate of a server hard disk is about 0.5% ~ 1% and about 5~10 hard disks can be damaged every year among 1000 ones. For the cloud mass accounting data storage, it is normal to have some failed disks every year. The existing disk array have good protection measure for hard disk failures, such as RAID technology, hot spare, etc; The multiple disk can be arranged array when a single disk is fail but the data can still be read/write and can recover the data after the replacement of new dish. In addition to the hard disk, hardware (servers, storage equipments) itself have ignored faults. Generally speaking, the hardware adopts double power supply and UPS power supply, and the disk array adopts the double control mode to ensure that a single physical node damage accounting data will be not missing and that the operations will not be stopped. Today's cloud storage technology also provides a more reliable safeguard for the hardware layer security and the multiple cloud storage can support redundancy RAID array between nodes, so the whole array failures still can ensure that the data is not lost.

Further more, pre cope, fault migration and hard disk bad sectors repairment technology can also be used to prolong the life cycle of hard disk.

2) Middle Tier ——Virtualization Layer Security

For the security issues of the virtualization layer, the first consideration is the safety and reliability of the underlying software. For example, double machine HA software can ensure the real time backup of the accounting data. At the same time, the take over business and the accounting data should be started when the host is failed. The second consideration is the safety of the virtual machine. The safety of the virtual machine is a big subject of the accounting information system application under the environment of the cloud computing and the attackers can lease virtual machine service. Using a loophole in the virtual machine, we can visit them from a virtual machine to other virtual machine to gain the permissions. Once breaking through the barrier of virtual machine, the attackers can directly access to the private data of the server and even control the management system of the cloud computing, amending the important data including the billing, virtual machine operation permissions, service permissions. A new study made by the market analysis agency named Gartner has shown that 60% of the virtual server security is lower than the physical server it replaced. At present, a better preventive measure is still the manufacturer updates depending on the virtual machine and patches, the timing inspection of the maintenance personnel and the password modification on a regular basis. The safety of the virtual machine itself shows the tendency of steady increase. Gartner estimates that, by 2015, only 30% of the virtual server is lower than the physical server it replaced.

3) The Outermost layer ——Service Layer Security

The outermost layer is the security of the service layer. On the one hand, ERP software business can support multiple machine cluster switch, the software of multiply machines (or the multiply process of the same server) do the load balancing. Common Web server has such function, or achieved by a separate load balancer. Single server software failure (such as process exits or hang dead) can pull up the business by means of the software, or let the software of the other servers replace the failed software business, then cut back to the original server after failure. On the other hand, a large number of network services need to be employed on the server, such as HTTP, DNS or specific business services provided by the service providers, etc. These services are exposed within the Internet. In addition to complete the normal business, it will also bear a lot of network attacks and the loophole in the operating system itself may lead to the damages to the server software done by the illegal criminals, such as Oday attack. Therefore, the strengthening of security on a regular basis is required and this kind of reinforcement patches itself by ways of the operating system, including the Windows patches on a regular basis and the commercial software patches, such as Oracle database patches, etc.

B. Pipeline Accounting Data Security

1) Firewall

Firewall refuse to accept the access which is not permitted, whether it is from inside to outside or from outside to inside. Firewall can effectively control the data interaction between the inner and outer network and filter the illegal requests. At present, most professional firewall equipments have functions like switching, routing and VPN and some equipments of manufacturers can also support wireless Wifi, 3G and other access ways. The firewall can not only be deployed in the cloud accounting data center to prevent the unauthorized access, but also in the access side of the accounting application software to provide the function of authentication and security access [3].

2) Intrusion Detection System

Intrusion detection system can provide the security protection of the network application layer. It can collect the traces left by the invaders' attack through a number of key points from the computer network or computer systems, such as abnormal network packets or the failed record caused by login, to analyze whether there are actions from the external or internal which are the violation of security policy or signs being attacked. For example, when the defense application layer refuse the service attacks (DOS/DDOS) and analyze the network packets which are attacking, it can make the

advanced warning, notify the administrators of targeted defense measures, shield the related user connections, control the numbers of connections or change the corresponding service port, etc.

3) Virtual Private Network (VPN)

Virtual private network (VPN) can ensure that the data transmission in the virtual network is a certified safety transmission and that the illegal user's data was not accepted through the IP tunnel technology, encryption technology, key management and authentication technology. VPN technology deployment is simple and effective and the vast majority of routers and firewalls support VPN deployment. VPN can not only protect the safety of accounting data but also monitor the network traffic and ensure the transmission quality without special equipments, so it has been widely used in the field of cloud computing, many have adopted the way of VPN whether it is the public cloud through a wide area network deployment or the private cloud through the enterprise local area network deployment.

C. Client Accounting Data Security

Cloud computing accounting information system contains a wide variety of access to the clients, including the form of the traditional fixed terminal like desktop computers and the form of mobile terminals like mobile phones and tablets. The accounting software running on the client have both the traditional and special client way and a way based on Web browser. For example, Kingdee' cloud management products can provide online accounting in the means of Web, EAS mobile application based on the IOS/Android mobile systems. If there are improper protection for the clients, the users' data may directly loss from the client into the hands of the criminals. The client's accounting data security needs the guarantee of the following several aspects:

1) Legality Identification

Legitimacy certification is one of the necessary security measures of the cloud computing accounting information system and the users can visit the services provided by the cloud through the client. The first step is to certificate the legitimacy. Legitimacy certification includes client and server authentication legality. Client legitimacy authentication can be made through the users' name, password and access address and the service provider can confirm that the client access is the lawful client; Service legitimacy authentication are mainly made through the digital certificate. Through the digital certificate, the client side is a certified and legal services to prevent bogus and illegal sites diddling users' data. All these belong to the network security control and protection measures based on the identity authentication. In recent years, some studies have also put forward the concept of the dynamic users' behavior authentication, which realized the key mechanisms based on behavior authentication. The certification process will not limited to the stage of the user login, it also extends to the process of business behavior for the users.

2) The Client's Virus and Trojan Protection

Although the client virus and Trojan protection is an old problem, it is still a major issue affecting the safety of the accounting data. The system access to cloud computing can avoid virus and Trojan attacks through the antivirus software. At present, there are measures in the industry to prevent the virus and Trojan through the cloud accounting. By the real-time cloud acquisition, it can constantly update virus signature files, eliminate the threat in time and ensure the safety of customer data [4].

3) New Client Formation and Cloud Terminal Protection

The cloud computing has evolved a new pattern of client and cloud terminals, the latter is in the form of the client terminal and the entire client desktop is provided by the cloud virtual machine. The client's hardware and software are greatly simplified, we can only run specified software and all software used in daily business are operated in the cloud desktop. In this regard, virus prevention and user authentication are all controlled by the cloud and the cloud desktop hardware and software have a similar environment. Unified management and control can avoid the differences caused by the client, which can effectively implement an integrated security strategy. Cloud terminal is suitable for the systems involving confidential data, because the users cannot modify the client's security policies and the center can control users' permissions for the whole client. It can effectively prevent the

internal users bypass security policies to steal confidential data through their own private cloud terminal equipment [5].

4 Cloud Computing Accounting Informationization Process Security Environment Construction

In the cloud computing environment, a typical accounting informationization business processing can be in accordance with the shown processing in figure 2 to ensure safe and reliable.

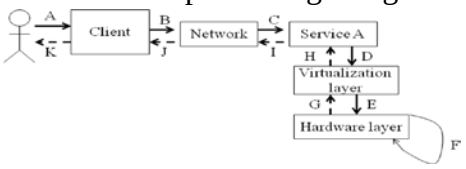

Figure 2. The basic business process accounting information

Specific accounting informationization business processing description is as follows:

A: When the user submits the accounting data. Users need a legitimate login to validate identities before submitting and there are also some certificating ways like digital certificates between the client and the server to confirm the legitimacy of both parties.

B: When the client sends the accounting data, the data may be encrypted and transferred by VPN channel to avoid intercepted in the network or data leakage.

C: Before sent to the cloud service, the accounting data should be permitted through the firewall confirmation. At the same time, it may be detected whether it is an attack message through IPS equipment. Through the checking of the firewall and intrusion detection system, data will be sent to Service A, performing the actual business, according to the load balancing strategies .

D: After decrypting the accounting data, Service A does specific business operation. If the persistence operation is needed(such as inputting to the database, etc.), the data must be submitted to the virtualization layer and then receives the request if the confirm is the authorized service.

E: Virtualization layer finds the actual physical devices according to the virtualization strategy and submits the accounting data to the physical device.

F: Physical device itself can perform the reliability protection mechanisms of the accounting data, such as data redundancy, data checking calculation, etc.

G: After the success of the execution, the hardware notify the virtualization layer the operating results.

H: Virtualization layer returns the results to business service.

I: Service A returned the result to the user and the encrypted result may be transferred through VPN channel.

J: The client receive data from the VPN channel and to decrypt, gaining the operating results.

K: The client will show the operate results to the users.

The safe cloud computing accounting informationization business process requires many different levels of security means, including the two-way legitimacy authentication between the client and server, the safe and encrypted network transmission, the legitimacy permission of the network packet, the legitimacy certification the services on the virtual machine as well as the high reliability of the service data storage and so on. It is important to note that the safety measures taken in business operation process can be graded and different types of user permissions and business operations will be affected by different security controls in order to distinguish and then ensure the control data is open to different users. Good cloud computing accounting information system is a business special for different clients, which can automatically identify whether the monitor user rights are abused. And the separation of duties control matrix of the SAP system is a good example. When establishing ERP system for Haier, SAP has built a set of separation of duties of control rules which is applicable to Haier. Through the automatic scanning of the SAP system, about 20% roles and the user account of the system are in the troubles of duties conflict separation and sensitive access authorization and this type of users can do fraud actions by the improper duty authorized.

With the continuous development of accounting informationization application scope and the increasing participation, there will be a lot of excessive authorization which is imperceptible in an artificial way and the hidden dangers caused by the role conflict. ERP service on the cloud manage all user rights and responsibilities information and it can take the initiative to avoid potential, artificial safety issues through the conflict scanner of the user privileges and responsibilities.

5 Conclusion

In short, cloud computing has brought the changes of data calculation and storage architecture, at the same time, it also brought the change of the data security. Compared to the traditional accounting software system, enterprises' accounting information software system based on cloud computing architecture deployment need to consider from different levels including the cloud, pipe and client, use a variety of means to solve the problems of data security. Security problem is more serious than ever in the past. If there are any security problems, it can bring significant influence on the data security of the whole accounting information system. Only there are professional, targeted norms and standards governing the security design at all levels can the data security of the cloud computing accounting information system be effectively guaranteed.

References

[1] Lou Jiayuan, Accounting Informationization Risk and Settlement Strategy Under Cloud Computing, Chinese Certified Public Accountants, vol. 12, 2013, pp. 110-111.

[2] Peng Chaoran, Accounting Informationization Risk Factors and Preventive Measures In the Era of Big Data, Fiscal Studies, vol. 4, 2014, pp. 73-75.

[3] Ma Guangqi, Cloud Computing Impact Analysis on Accounting Informationization, Accounting communication, vol. 3, 2014, pp. 92.

[4] Chen Jiali, On Financial Accounting Development Based on the Electronic Commerce Network, Enterprise Economy, vol. 6, 2012, pp. 129-130.

[5] Cheng Ping, AIS Module Relations Complexity Metrics Based on Cloud accounting, Accounting UFIDA, vol. 27, 2014, pp. 119.