ORIGINALARTICLE

Universe Scientific Publishing

Research on Information Security in Cloud Computing Environment

Quanhui Ren [1], Hui Gao [2]

1,2. Zhengzhou Railway Vocational and Technical College, Zhengzhou 450052, China

ABSTRACT In order to adapt to rapid development of network information technology, the application of cloud computing technology is increasingly widespread. However, the security problem in the cloud computing environment has not been effectively resolved. Currently, the research on this problem is getting more attention from the industry. In order to further investigate the information security issues of Cloud computing environment, this article not only discusses the basic concept, characteristics and and cloud cube service model of cloud computing, but also focuses on the cloud computing security reference model model. In this paper, the information security problems and concrete solutions in the former cloud computing environment are discussed from different aspects.

KEYWORDS

Cloud computing

Information security

Model

INTRODUCTION

With rapid growth of network information technology, cloud computing technology has been rapidly developed. Meanwhile, related technology of cloud computing, distributed processing, parallel processing and grid computing have been widely used up, a large number of computer processing programs are split into numerous smaller sub-programs according to the procedures the network. After that, complex analysis can then be calculated by the server and the final results of the analysis are sent back to the client [1]. Cloud computing technology can achieve in a very short period to deal with millions or even billions of information to achieve the so-called “supercomputer” capability. The ultimate target of computing system is transferring of an individual and personal computing quickly and securely to a large number of cloud servers. In other word, users do not need to process the computing using own computer but can process by using cloud computing system. Presence of issues in information security information transmission and information processing users was discussed in this paper through the border security, data security and application security. In addition, simulation model was built in this study [2].

doi: 10.18686/esta.v3i1.8

1. Cloud computing

1.1 Basic concept of cloud computing

Currently, there is still no unified concept of cloud computing but a more recognition of the concept of cloud computing is proposed by the US National Institute of Standards and Technology (NIST). Cloud computing is defined as a model that the user can access a computing resource through this model, consists mainly of the networks, servers, storage devices, applications and other resources, and also able to provide a good and fast pathway [3].

1.2 Basic Specifications

(1) Characteristics of cloud computing

Characteristics of cloud computing are mainly self-service, public network access, rich resources, fast-responsive and providing measurable services.

(2) Cloud computing service model

Software as a Service (SaaS). A service provider offers individual enjoying service through the cloud infrastructure. Various clients can access a large number of applications through the network provided by the service providers. Users do not need to manage the cloud infrastructures, such as networks, servers, operating systems, storage devices and other program functions. If an abnormal situation occurs, the system will automatically limit the user-configurable application settings and achieve self-repair [4].

Platform as a Service (PaaS). Users can develop a wide variety of applications through cloud platform. At the same time, users can also use these applications to publish on cloud infrastructure and enable sharing of resources. Users do not need to manage the cloud infrastructure, such as network, servers, operating systems and storage devices. However, customers can manage the applications developed.

Infrastructure as a Service (IaaS). The service provider can provide services like processing, storage, network and some other basic computing resources. Users can follow the protocol to run a variety of software, especially the operating system and applications. Cloud infrastructure does not require user management. A user can achieve operating systems, storage, management of release of applications, and management of network components.

(3) Cloud computing release model

Private cloud. The cloud infrastructure is managed by a separate department operation. Besides, a third party of management may exist under certain conditions or unconditionally, i.e., the presence of uncertainty [5].

Community cloud. Infrastructures are managed by multiple departments operate, but also must support each other to share the concept of a particular community. There is the possibility of third-party management, and it may exist in certain conditions or unconditional presence, i.e., the presence of uncertainty.

Public cloud. The general user of the infrastructure is the public but can also be an organization that can provide a lot of paid cloud services.

Hybrid cloud. Cloud infrastructure is relatively complex, which is a mixture of two or more clouds. These cloud entities are unique, but can be combined using standard or proprietary technology. Transferring of data or the application can be achieved by this cloud infrastructure and ultimately, resources can be shared.

2 .Cloud security reference model

In real application, this cloud computing model will be a lot different from the status and consumption patterns. Therefore, the risk security characteristics and safety control functions are also very different. For effective security, a scientific cloud computing reference model must be established. This is the only way to achieve security communication structure for cloud services, and to identify risks, control security and to provide scientifically valid data to support through decision-making program [6].

2.1 Cloud security alliance model

Figure 1 shows the model of Cloud Security Alliance (CSA). This model is mainly based on service model. This model has an important feature, i.e., when the supplier has higher level, the users have less responsibility for security, the relationship between the two is in contrary.

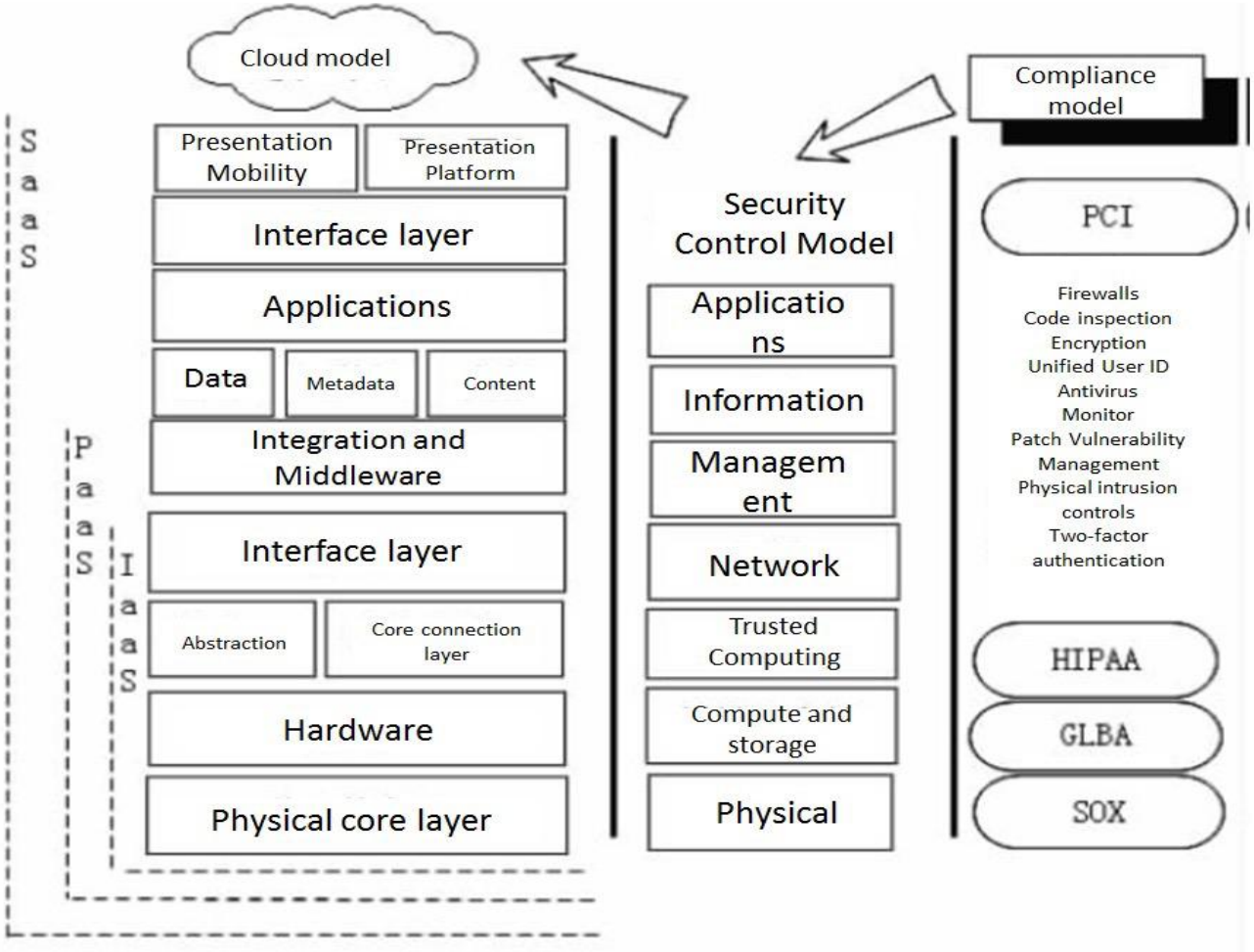

Figure 1 Cloud services security reference model

2.2 Cloud cube model of Jericho forum

This model is built mainly from the angle of security. This model mainly refers to the former relationship between the physical location of data, cloud-related technologies and services (Figure 2).

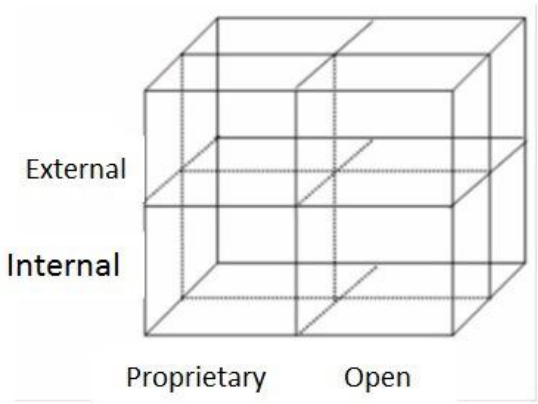

Figure 2 Cloud cube model

A significant difference in the form of cloud computing has resulted in great difference in collaborative, flexibility and security risks. It is also an important feature of cloud computing. A specific user can select different cloud computing models according to their needs, and ultimately achieve the “cloud” secure communications.

3. Security issues of cloud computing information

In actual application, the issues of information security in the cloud computing environment are mainly in the following three aspects, specifically as shown in Figure.

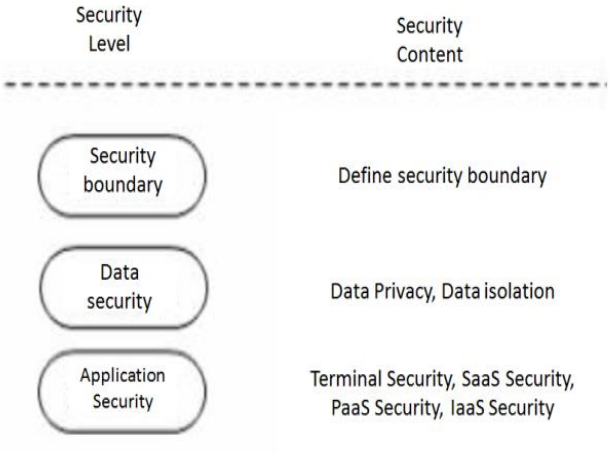

Figure 3 Cloud security content

3.1 Difficulties in definition of security boundary

A security boundary is hard to define as there are a large pool of users in cloud computing. At the same time, the storage of data is not centralized. Therefore, it is difficult to ensure information security of the users [7].

3.2 Data Security

Cloud computing services are open type, so users do not know where their data are stored and the location of management server. Therefore, they cannot effectively protect their data, which requires cloud service providers to effectively protect the user’s data, mainly through two aspects of effective protection.

(1) Data privacy. Only software vendors have permission to manage data privacy process. As large amounts of data are shared, the existence of risks for these data is inevitable. The biggest feature in cloud computing data is entirely managed by a third party. Because of the cloud computing architecture of their characteristics, these data cannot be stored centrally, while still stored in a clear text form. Traditional firewalls do not fully protect the security of these data, and some critical data leakage is inevitable. Now the best protection program is building a private cloud or hybrid cloud to achieve computing elasticity [8].

(2) Data isolation. The most widely shared data is to use encryption methods, because data storage in cloud computing environment is very complex, only data security can only be assured by isolation of data. To achieve data isolation, it is necessary to develop an appropriate framework. The most widely distributed now is a shared table schema, database schema separation and isolation table schema. These architectures have their shortcomings, and must be further improved to ensure better security of user data.

3.3 Application Security

(1) Terminal security

In real application, the security of the user terminal is under a cloud environment of the data security first line of defense. Cloud computing environment also ensures the most important part of the information security.

(2) SaaS application security

SaaS application security refers to software as a service application security. Service providers must provide complete services, including maintenance of infrastructure, meanwhile must be good to provide users with applications and components security. Therefore, users only need to ensure security of the data in operating stage [9].

(3) PaaS application security

PaaS providers must develop related anti-attack software to ensure the safety of the software package platform. In the process of using, there will be an extremely dangerous situation if PaaS is improperly configured, which means that the default configuration of the safety factor can be negligible. Therefore, the client must be familiar with the security configuration process.

(4) IaaS application security

In real application, IaaS cloud providers know nothing about the user’s information. The providers are not concerned about specific operations of the user within the cloud. Therefore, users must ensure that their data are safe in the cloud.

4. Conclusion

Currently, information security and cloud computing environments are getting more attention from the industry. This article discussed in detail on the concepts and features of calculation, introduced cloud security reference model and cloud computing information security, and the issues of information security in cloud environments that requires further solution. The US NIST pointed out that the security risks of cloud computing can be controlled and reduced through the management approach. Widely used of Cloud Computing Service Level Agreement (SLA) is imperative [10].

REFERENCES

1. Zhao L, Qiu X. Cloud computing environment security threats and protection. China Computer Federation Newsletter, 2010，6 (5): 47－50.
2. Liu W, Meng X, Ling Y. A graph-based approach for web database sampling. Journal of Software, 2008, 16(2):179-193.
3. Gao M, Jin C, Wang X, Tian X, Zhou A. A survey on management of data provenance. Chinese Journal of Computers, 2010, 33(3):373-389.
4. Zhang Y, Chen C, Bo P, et al. Cloud computing security critical technical analysis. Telecommunications Science, 2010(9): 64-69.
5. Nathuji R, Schwan K. VirtualPower: coordinated power management in virtualized enterprise systems. SOSP '07. New York, NY, USA: ACM, 2007.265-278.
6. Pallipadi V, Starikovskiy A. The ondemand governor: past, present and future. Proceedings of Linux Symposium. 2006.223-238.
7. Rao L, Liu X, Le X, et al. Minimizing electricity cost: optimization of distributed internet data centers in a multi-electricity-market environment. INFOCOM'10. San Diego, California, USA: IEEE Press, 2010.1145-1153.
8. Samadiani E, Joshi Y, Mistree F. The thermal design of a next generation data center: a conceptual exposition. 2007.93-102.
9. Cheng X, Guo J, Jin X. A retrospective of web information retrieval and mining. Journal of Chinese Information Processing, 2011， 26 (6) ： 111-117.
10. Shen H, Jin X, Ren F, Cheng X. Public opinion analysis for social media. China Computer Federation Newsletter, 2012, 8(4):32-36.