*2012 International Conference on Education Technology and Computer (ICETC2012)*
***IPCSIT vol.43 (2012) © (2012) IACSIT Press, Singapore***

# Analysis and Research on Security Defense Strategies of Cloud Security

Ming Li [1 2+], Liping Ding [1] and Shuo Tian [1]
[1] National Engineering Research Center for Fundamental Sof tware of Institute of Sof tware , Chinese Academy of Sciences ,Beijing, China
[2] Special EducationCollage,Beijing Union University,Beijing, China

**Abstract.** The information security problem in cloud computing circumstance is the primary problem facing by cloud computing, this article analyses the security problem of cloud computing and proposes the solution strategies through the principles and features of cloud computing and the differences between the security mode and traditional mode in cloud computing circumstance.

**Keywords:** cloud security; security mode; virtualization; trusted computing

## 1. Introduction

The definition of cloud computing is an IT system implementation technology using large-scale low-cost operation units through IP network connection to provide a variety of computing services. The cloud computing system should meet the following characteristics at the same time: (1) large scale: a cloud computing system is an IT system cluster consists of multiple nodes with certain sizes; (2) smooth expansion: the system cluster scale should be provided with flexible expansibility and elasticity; (3) resource sharing: provide one or more forms resource pools, including physical servers, virtual servers (virtual machines), transaction and document processing capabilities or task processes and storage resources, etc. These resource pools can be implemented by abstraction mode, and provide services for multiple applications simultaneously; (4) dynamic allocation: implement automatic allocation management of resources, including resource real-time monitoring and automatic scheduling, etc.; (5) cross-boundary: the cloud computing system need to be provided with integrating resources of different regions, providing management abilities of all levels. The basic classification of cloud computing can be classified by the providing service styles, such as IaaS,SaaS, PaaS, etc.; also can be classified by the characteristics of cloud service objects, such as share cloud, private cloud and mixed cloud, etc. As Figure 1shows.

The cloud computing brings a brand new business mode, provides resources with the “service mode” to the users through internet, while the users do not have to realize, know or control the technical infrastructure supporting these services. The cloud computing is the development of parallel computing, distributed computing and grid computing, or can be considered as the commercial implementation of these science concepts; the cloud computing is also mixed developing result of the virtualization, utility computing, IaaS (Infrastructure as a Service), PaaS (Platform as a service), SaaS (software as a service), HaaS (Hardware as a service) and other XaaS (anything as a service) concepts and techniques. When it comes to cloud computing and security, there are two aspects of meanings generally, one is the own security of cloud computing, mainly is how to establish security protection system, to guarantee the safety of the cloud computing platform itself, the other is cloud security, which means providing security as a resource and service with cloud computing technology.

[+] Corresponding author. *E-mail address*: *li.ming.buu@gmail.com*.

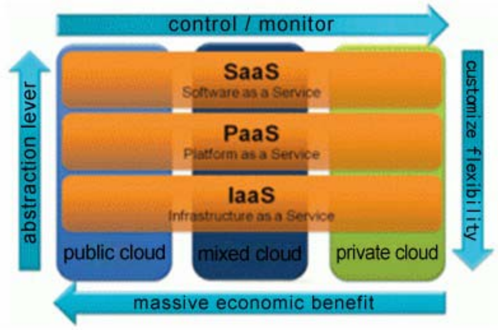

Figure1. Architecture model of cloud computing system

The cloud security includes two aspects. One is security cloud computing, which means the specific applications of cloud computing technology in the security field, is a branch of cloud computing applications, can improve the service performances of security system with cloud computing technology, such as the anti-virus technology and Trojan detection technology based on cloud computing, the other is the application security of cloud computing, which is using network security technology to improve the own security of the cloud computing applications, including how to guarantee the availability of cloud computing services, data confidentiality and integrity, the protection of privacy, etc. The security of cloud computing application is the foundation of the healthy and sustainable development of cloud computing [1].

## 2. The Security Mode Instances of Cloud Computing Providers

### 2.1. Cloud security mode based on service mode

From the perspective of service mode, CSA（cloud security alliance）proposed security reference modes based on levels and the dependency relationship of the three basic cloud services, and achieve the mapping from cloud service mode to security control mode, as Figure 2 shows. This mode shows that PaaS is located above IaaS, while SaaS is located above PaaS. SaaS: providing the services running application on cloud structure for the usesr. The users can access the application through client interface (e.g.: web browser) from various clients devices. PaaS：providing services deploying the application (which the users creates themselves or obtains from other places) in the cloud structure for users, while the program languages and tools which create these applications need to get the support of service providers; IaaS: providing process, storage, network and other basic computing resources services, the users can deploy and run any software including operation system and applications software on it.

### 2.2. Virtualization requirements

Based on the highly integrated of storage resources and server resources, when the cloud computing service providers providing the services to the clients, the distribution according to need of storage computing resources and the security isolation between the data are becoming basic requirements, and is the reason which the virtualization becoming the key techniques of cloud computing center. In this condition, how the security devices to adapt virtualization of cloud computing center basic network framework. To achieve the uniform virtualization delivery of and security, is the focus of security construction under the cloud computing circumstance[2]

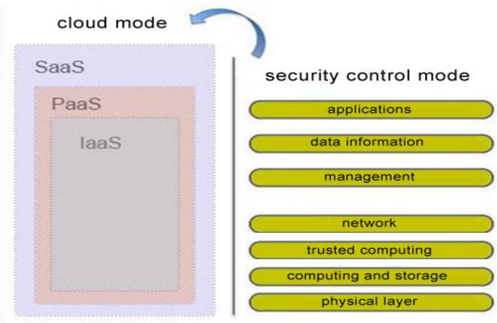

Figure2. Cloud security mode

### 2.3. Blurry security boundaries

The cloud computing introduces new potential threat problems for system security. The service mode of cloud computing, based on the virtualization and the bottom architecture feathers of distributed computing, make the security boundaries relatively blurry. The traditional security area division, network border defense and other security mechanisms can not guarantee the security requirements of the cloud computing applications.

## 3. The Main Strategies of Security Defense Under The Cloud Computing Environment

We can actualize the security defense of cloud computing through bottom architecture security, infrastructure security, user information security, operating and management security. Bottom architecture security mainly guarantees virtualization, distributed computing and other system securities. The infrastructure security mainly guarantees the stability and service continuity of the cloud computing infrastructure. The user information security is to protect the availability, and confidentiality of the information. The operating and management security mainly improves the security of operating and management, and completes security audit and traceability mechanism. Through the multiple mechanism combining the operating mode and bottom architecture features of cloud computing, adopting traditional security defense, adding security based on cloud security mode, construct deep security defense system facing to the application of cloud computing.

### 3.1. Cloud security defense based on service mode

From the definition of the three cloud service modes, we can get the conclusion that though the users entrust their computing and storage to the cloud, especially on the aspect of security strategies, definitely not hope the cloud providers to solve all the problems. The security defenses of three cloud service modes differ in the methods and responsibilities. The IaaS cloud service providers are mainly in charge of providing basic framework services for the users, like providing virtual data centers including servers, storages, networks and management tools. The reliability, physical security, network security, information storage security and system security of the cloud computing basic devices are its basic responsibilities, like the in-break detection of virtual machines, the integrity protection and so on. While the users of cloud computing need to take charge all security problems above basic device frameworks, like the security of self operating system and applications program. The PaaS cloud service providers mainly in charge of providing simplified develop, test and deploy circumstance of the distributive software. While the cloud computing user need to be responsible for the security problems above operating system and application circumstance. The SaaS cloud service provider need to ensure the providing SaaS services the whole security from basic devices to the application layer, the cloud computing user need to maintain the information security related to itself, like the identity authentication ID, password, terminal security, etc.

### 3.2. Construct security defense system with the support of virtualization

Currently, virtualization has become the key technique methods which the cloud computing providers providing “on – demand services”. Basic network architecture, storage resources, computing resources and application resources. They have all moved forward a big step to support virtualization. We can provide personalized storage computing and rational distribution of application resources according to the requirements of different users only based on this kind of virtualization technology, and actualize data security among different users by the logical isolation between virtualization examples. The security need to support virtualization no matter as the basic network architecture, or based on the Saas concept, to achieve virtualization computing from end to end. The typical schematic diagram as Figure 3 shows.

The corresponding security strategies of Virtualization:

Virtualization software security :

The virtualization software directly deploed on the physical machine, has the function of creating, operating and destroying virtual machines, can make the virtual machine isolated in multi-tenant environment. So, if the client wants to run multiple operating systems simultaneously and safely in the same computer, should strictly restrict any unauthorized users to access this virtualization software.

Virtual server security :

The virtual server is located above the virtualization software. We should distribute a separate hard disk partition to each virtual server, to logically isolate virtual servers logically when install virtual server. Every virtual server isolates from each other through VLAN and different IP network segments. In firework, we make relevant security settings to every virtual server and make further protection and isolation. Monitor the operating situation of virtual servers and the system logs and firework logs of the virtual machines, to discover the existence of security risks.

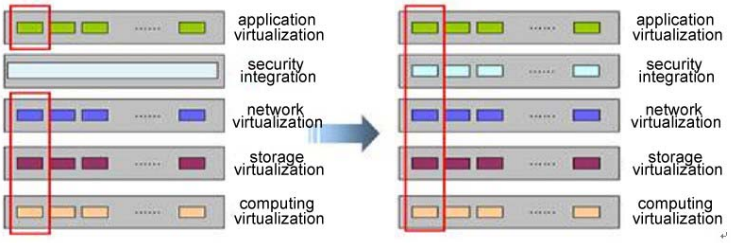

Figure3. The security defense system with the technical support of virtualization

Construct secure logical boundary

In the typical cloud computing application circumstance, the physical security boundary gradually disappears, and replaces by logical security boundary. We should actualize the transmission channel security from user terminals to the cloud computing data center through applying VPN and data encryption and other technologies, in the center of cloud computing data center, applying VLAN, distributed virtual switch and other technologies to actualize the security isolation of user system and user data.

### 3.3. Cloud security based on trusted computing

With the application of virtualization technology, the security of cloud and the evaluation and management of security risks become more and more prominent, common security measures hardly can meet the requirements. To establish trusted computing platform can effectively solve the security problems of cloud computing. Many cases show that the combination of trusted computing and virtualization technology is the most effective to cloud security. The main thought of trusted computing is introducing trusted platform module in the hardware platform to improve the security of terminal system. Construct trusting relationship from BIOS to the kernel layer of the operating system, to the application layer. Based on this, extent to the network, and establish relevant trusting chain, to enter into a computing "immunity" age. When the terminal gets attacks, can achieve self protection, self management and self recovery, to establish trusted cloud, it will be the fundamental path to solve the cloud computing security problem.

## 4. Acknowledgment

This research was supported by the National Science Foundation of China(NSFC) project(90818012)

## 5. References

[1] Bian Xin, *From theory to practice-depth analysis of cloud service providers and cloud security*, [DB/OL].http://www.cnw.com.cn/security-cloud/htm2010/20100910_207305.shtml

[2] Sun Songer, *The security construction idea based on cloud computing circumstance*, Information Security and Communications Privacy. Chengdu, pp.21-23.November 2010.

[3] Xie Sijiang, Feng Yan, *Analysis of Cloud Computing and Information Security*. Journal of Beijing Electronic Science and Technology Institute. Beijing, vol.16(4), pp.1-3, December 2008.