Research and Analysis on Cloud Computing Data Security

Yonghui Ma
Department of Electronic Science, School of Engineering and Technology, Xi'an FanYi University

Keywords: Cloud computing; Security; Network architecture

Abstract. With the rapid development of Internet technology, computer technology, network technology and database technology, the rapid development and wide application of cloud computing technology has been promoted. Cloud computing to provide us with more quality services at the same time, the transmission of data security issues are also more prominent. Cloud computing security has become more and more attention, and has become the focus of people's attention, and quickly become a new area of space.

1. Introduction

With the rapid development of Internet technology, computer technology, network technology and database technology, it has promoted the rapid development and wide application of cloud computing technology. The problem of cloud computing security has been paid more and more attention, and has become the focus of people's attention. The distributed denial of service attack against cloud computing is one of the security threats facing cloud computing.

In addition, the existing cloud computing network architecture is relatively complex. One of the data centers includes modules such as firewalls, Ethernet switches, server load balancers, service control engines, and intrusion detection. For each service, more equipment needs to be involved. The cloud computing network architecture needs to be redesigned and simplified in order to enhance the network integrity of cloud computing.

2.Current Stage Cloud Computing Data Security Analysis

While cloud computing provides us with better service, the issue of data transmission security is also more prominent. We must recognize the huge scale of cloud computing system and the complexity and openness of cloud computing system. Due to these characteristics of cloud computing data, it brings a very severe test to its overall security.

2.1 Existing cloud computing network architecture.

The existing cloud computing network architecture has many different elements at the service level, including routers, firewalls, Ethernet switches, fiber channel switches, and server load balancers. As shown in Figure 1:

Figure 1. Cloud computing network architecture

Through the cloud computing network architecture, we can understand that cloud computing networks use firewalls to protect servers and memory. The function of firewalls is to allow or refuse

  DOI: 10.25236/icess.2019.241

network transmission based on a set of rules. Load balancers enable load sharing between services.

In the cloud computing network architecture, data centers contain many service devices. This data center is connected to the Internet via a core router and the service layer device is aggregated through a convergence layer. Service layer devices include firewalls, load balancers, etc.. All service layer devices are connected to the convergence layer and exchanged or routed through the aggregation layer device. Users can flexibly submit business, and based on services, the network architecture can be different.

Some users can choose between load balancing services and firewall services; Other users can have more fixed business volume and choose flexible billing services.

The network architecture can vary depending on the service provided. The access layer includes virtual access devices, servers, and memory. The access layer provides interconnection between the server and the network. The structure and configuration of the network are very complex and difficult to operate.

2.2 Existing cloud computing cyber security threats

In the cloud computing environment, there are many network security threats, some of which are discussed and analyzed. Figure 2 cloud computing type diagram.

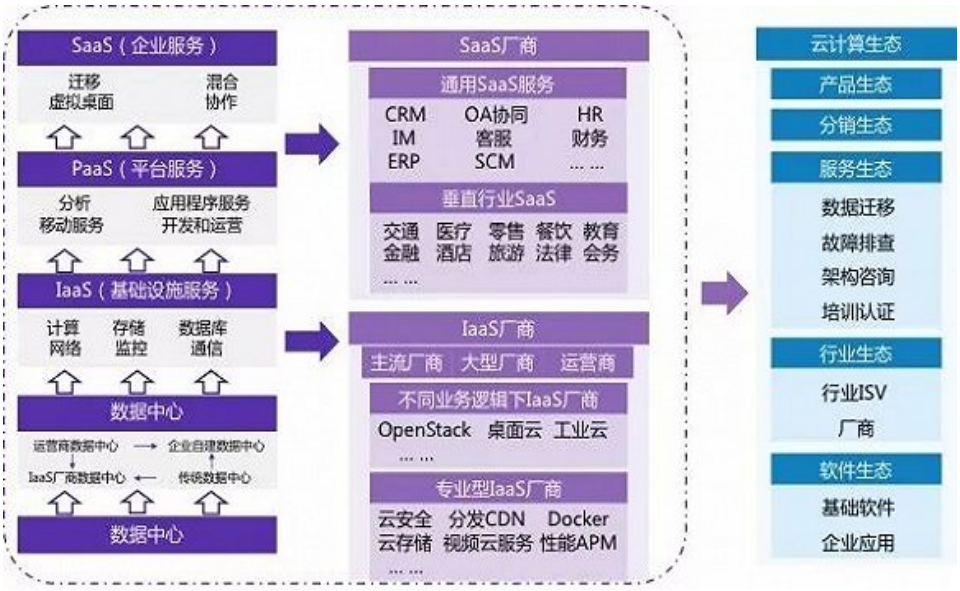

Figure 2. Cloud computing types

2.3 Denial of Service Attacks

Denial of service attacks means that the attacker finds a way to stop the target server from providing services or even the host crash. If the attacker frequently makes access requests to the server, causing network bandwidth consumption or application server buffer overflow: This attack makes it impossible for the server to receive new service requests, including access requests from legitimate clients. For example. A hacker hijacked the Web server and shut down its application service, causing the server to fail to provide Web services. In cloud computing, when a hacker makes a denial-of-service attack on a server, thousands of access requests are made to the server, causing the server to fail. Unable to respond to client's valid access request. The response to such attacks can be to reduce the permissions of users connected to the server, which will help reduce the impact of denial of service attacks.

2.4 Intermediary Attacks

Intermediary attacks are another means of cyber attack. The attacker intercepts normal network traffic data. The data was tampered with and sniffed, but the two sides of the communication did not know it. In network communications, this risk problem can occur if the condom socket layer(SSL) is not properly configured. For example, if the communication parties are interacting with information and the SSL is not installed correctly, then all data communications between the two parties may be hacked. The response to this attack is to install and configure the SSL correctly. And before using communications, third-party authorities should check and confirm the installation configuration of SSL.

2.5 Network sniffing

Network sniffing was originally a tool used by network administrators to find network vulnerabilities and detect network performance, but in the hands of hackers, it became a cyber attack method, causing a more serious network security problem. For example, in the course of communication, because the data password is set too simple or not set, resulting in hacking, the unencrypted data is obtained by hackers through cyber attacks. If the communication parties do not use encryption technology to protect data security. Then the attacker as the third convenience can steal data information during the transmission of data between the two sides of the communication. For this kind of attack method, the response strategy can be used by the communication parties to use encryption technology and methods to ensure the security of data during transmission.

2.6 Privacy of cloud computing data

The privacy of cloud computing data is one of the security of cloud data that people pay more attention to at this stage. The so-called privacy of cloud computing is that cloud computing can avoid illegal operations such as viewing and copying by unauthorized people. The security of cloud data plays an important role in cloud computing data. In the study, we found that the main reasons that affect the privacy of cloud computing data are: risk issues in data management interfaces, isolation risks, and incomplete data deletion issues. The problem of isolation risk is one of the hottest issues. The danger is mainly in the virtual machine in the process of cloud computing data, because the virtual machine that is prone to multiple users may run on the same physical storage device during use. On, If the user's virtual machine has a certain vulnerability, the result will pose a major threat to the privacy of the entire cloud computing data.

2.7 Data risk of cloud computing data

Unlike traditional IT companies operating internally on local networks, many existing IT companies provide cloud computing services on the public cloud through the Internet. Therefore, it brings certain risks to user data security. Coupled with the fact that cloud computing may serve multiple enterprise users at the same time, cloud customer data may be confused at the same time, resulting in increased risk.

2.8 Integrity of cloud computing data

The integrity of cloud computing data refers to the fact that cloud computing data has not been illegally deleted or tampered with. Therefore, it is necessary and important to fully realize the integrity of cloud computing data. It has a very significant impact on the security of information assets of various enterprises or private users and the reputation of vendors providing related cloud services. Based on the relevant data research, the main factors that affect the integrity of cloud computing data are: Hard disk driven capacity growth rate is lower than the speed of cloud data growth. In order to meet the user's demand for hard disk capacity, the cloud service provider adds the number of hard disks for the cloud service. In this process, it is very likely that the connection point failure will occur, causing the related cloud service disk crash and data loss. In addition, network hackers illegally realize attacks on cloud computing data, causing loss and deletion of cloud computing data, etc., which poses a greater threat to the integrity of cloud computing data.

3. Comparative Advantages of Cloud Computing Security

3.1 Problems with traditional security systems

While cloud computing faces security problems, it is also necessary to see that the security system of traditional IT model also has many defects and deficiencies. For example, most enterprises do not have professional development, operation and maintenance teams in terms of safety protection. Therefore, when the system is built at the beginning, it is extremely expensive to invest in the construction of the system. After normal operation, the maintenance investment will be less and less. The safety rules specified by many large companies are very complicated, such as supermarkets, hospitals, banks, etc.. In addition, there is a serious heterogeneity in the enterprise IT architecture, which makes the security problem more prominent. Some companies ignore the upgrade and replacement of the security system, as long as there is no problem and no investment. Even if there are problems, there are many problems where they occur, where they are solved, and they are not willing to invest in security systems on a large scale. Causes problems to squeeze into piles and trigger.

3.2Security Advantages Specific to Cloud Computing

Cloud computing has its unique advantages in security, which is unmatched by traditional IT models.

(1) Credit. The current cloud provider is a major cloud provider with large IT companies and traditional IDC(data center). However, with the continuous development of cloud computing, cloud suppliers will gradually be replaced by large state-owned enterprises. Taking our country as an example, there have been good mechanisms for government promotion, scientific research and enterprise participation. Among our operators, mobile's research into cloud computing technology started earlier, launching big cloud a few years ago. The goal of "Big Cloud" is to meet the high performance, low cost, extensible, and high-reliability IT computing and storage needs of mobile support systems. At present, Mobile has developed into the Dayun 2.0 platform. See Figure 3 Big Cloud 2.0 Product Overall Architecture.

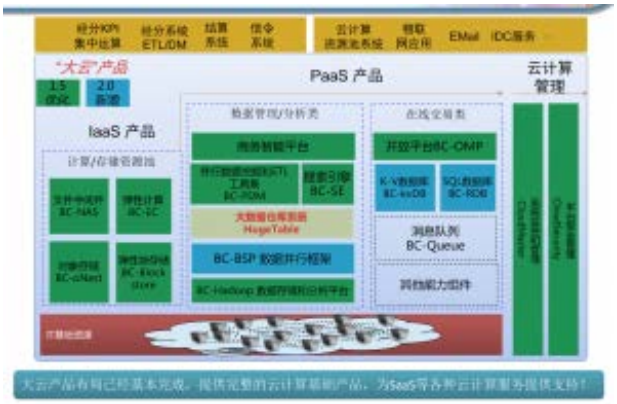

Figure 3. Big Cloud 2.0 Product Overall Architecture

China Telecom's "Sky Wing" cloud computing strategy is positioned as the leader of the intelligent pipeline, and the integrated platform provides participants in content applications. The "Sky Wing" cloud computing system consists of three levels: the resource cloud(Iaas), the capability cloud(PaaS), and the application cloud(SaaS). As shown in Figure 4, China Telecom's "Tianyi Cloud" architecture chart, with the development of e-commerce, cloud computing network platforms can also be further developed.

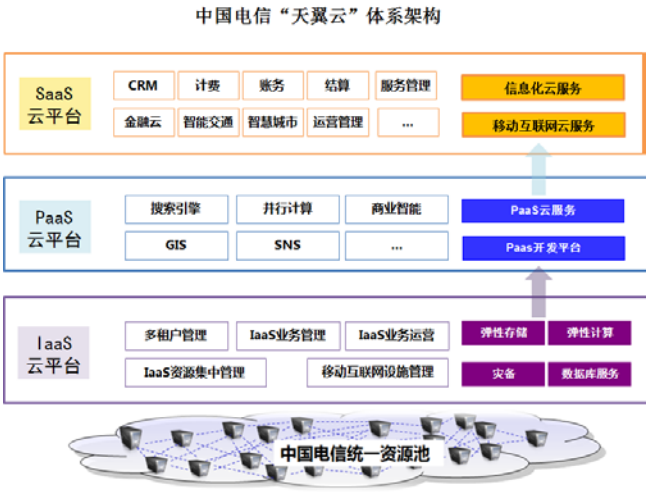

Figure 4. China Telecom's "Tianyi Cloud" system architecture

(2) Data isomorphism. The biggest problem of traditional IT data centers is data isomerism. Different formats, different libraries, and different storage methods make heterogeneous data very complex, data loss, intentional or unintentional changes and other security problems and hidden dangers have always existed. In addition, software, hardware, accessories, integration methods, etc. are varied and varied. Due to various conditions, the degree of automation is very low. The more complex the system, the more security risks, the higher the security cost. The advantage of cloud computing lies in the unified integration of various heterogeneous situations. All services are provided by cloud systems, which effectively reduces security risks, makes up for defects, and realizes unified security management.

(3) Operation management. Since the services provided by cloud computing are uniformly completed by cloud systems, the operation management is also uniformly deployed and unified in the cloud environment. Compared with the traditional service mode, the operating management program of the cloud system can be highly simplified, and unified services, standards, and supervision can be achieved. In particular, monitoring and recording systems at all levels of service operation is not comparable to traditional IT industry models.

4.Risk Response

From the analysis of the threats of data security in cloud computing, it can be seen that as a new information service model, cloud computing faces security problems that have surpassed traditional network applications. To guarantee the data security of cloud computing application, we should carry on the various means from many aspects.

4.1Integration of cloud computing networks

Adopt a new network integration device to simplify the network architecture. The design of this simplified cloud computing network architecture can increase the efficiency of network operation, management and maintenance and reduce the workload.

Use the "Clean gate" data and control plane separation design method to consolidate the original cloud computing network device. The traditional cloud computing data center aggregation layer is located at the boundary of the second and third floors. The data center contains functions such as firewalls and service equalizers. The newly proposed architecture uses a single "Clean gate" data and a device that controls plane separation design methods that can be converted through software and configuration functions.

4.2 Supply on demand

Cloud computing can flexibly supply virtualized resources on demand. when users book, cloud computing services, virtual machines, and network devices will immediately respond to these requests, and traditional network devices can not implement the services provided dynamically.

The on-demand cloud computing service network is completed through customers. First,

customers can access the portal via the Internet, which consists of a service platform and a network platform. Cloud services and web services must be provided by cloud providers. Cloud services include virtual machines and IP multimedia systems; Network services include network services such as stream billing and firewalls. Users submit cloud services and the subscription service will be provided immediately.

5.Concluding Remarks

Firstly, this paper analyzes the security of cloud computing data, and puts forward the comparative advantages of cloud computing security. Secondly, in order to consolidate cloud computing security, it provides a network architecture security solution for cloud computing network integration. Through the implementation of this scheme, the security of cloud computing network resources is solved.

References

[1] J.S.Li ,X.W.Zhang and J.Zheng. Application and trend of computer network technology in archives information management[J] .. Research on Urban Construction Theory(Electronic) 2013(36).

[2] Gold frost. Discussion on data security technology of power information system based on cloud computing[J] .. Computer Security, 2013(08)

[3] D.F.Zhang. Cloud computing practice[M] .. Beijing: Tsinghua University Press, 2012.

[4] Interactive Encyclopedia[EB/OL] .. H Ttp://www.hudong.com/wiki. Aliyun.