Analysis of Network Security Defense Technology Based on Cloud Computing Technology

Li Bin

North Sichuan Medical College, Nanchong, Sichuan, China

Keywords: Cloud computing technology; Network security; Defense Technology

Abstract: With the rapid development of network technology in recent years, cloud computing technology is more widely used. On the basis of bringing convenience to people's work and life, cloud computing technology also has security problems to a certain extent, which poses a great security threat to people's information property. Cloud computing is a new service mode of sharing resources on the network, which can make many computers and massive data organizations on the Internet a reality. From the perspective of users, this paper deeply analyzes the characteristics and application modes of cloud computing, and pays attention to the security problems faced in the development and practical application of cloud computing technology. Starting from these problems, combined with practical applications, this paper puts forward the main technical methods of network security system reinforcement and attack defense under cloud computing.

1. Introduction

Cloud computing is a distributed computing platform under network technology. In the process of implementing cloud computing technology, the platform shares resources and realizes quantitative and regular allocation based on the needs of different users. Cloud computing technology gives users the ability of data storage and distribution in the third-party data center, and the practical application can bring convenience to people. The rapid development and wide application of cloud computing technology is mainly due to its advantages of on-demand distribution and shared resource pool of cloud computing. The characteristics of on-demand service and self-service in the application process of cloud computing are relatively prominent. Users decide the resources they buy and the length of service, which do not need the intervention of service personnel [1]. The application of cloud computing is also prominent in the characteristics of resource sharing. The software and hardware form a resource pool, and users rent physical and virtual resources according to their needs. The multi terminal access feature of cloud computing is also prominent. The terminal can be selected according to the demand, and the characteristics of uniform deployment, scalability and elasticity, and measurable service are also prominent.

From the Internet era to the big data era, it has entered the third stage of the information age, which also means that data has become more important. Cloud computing data has penetrated into various industries and business functional areas, and has become an important production factor. People's mining and application of massive data indicates the arrival of a new wave of productivity growth and consumer surplus. Big data technology will be combined in physics, biology, environmental ecology and other fields, as well as military, finance, communication and other industries. So far, the emergence of the era of big data is inseparable from the emergence of cloud computing technology, which means that a large amount of data needs a large number of operations for processing, which makes us obtain more information in our life, and the information is growing in the form of explosion. At the same time, a new technology, artificial intelligence, has emerged. The emergence of this technology means that the data begins to become more logical, so there will be new challenges to network security. Whether cloud computing or artificial intelligence, they are inseparable from the carrier of the network, which makes big data more convenient to bring convenience to all fields in the carrier of the network. It was born in the network 5g era. It can be fully explained that entering a new stage, technology will also increase, and the corresponding relationship between various fields will be closer, so the scope of network security will also increase. In order to obtain all kinds of

DOI: 10.25236/icmmct.2022.011

information, today's society is inseparable from the Internet. In this era of big data, there are more and more platforms associated with personal information, which greatly facilitates the needs of daily life and work; At the same time, it becomes easy to understand a person's information. The more personal information is related, the simpler the way to obtain data, and the Internet naturally becomes a double-edged sword. In the Internet, personal information mainly includes basic information, equipment information, account information, privacy information, social relationship information and Internet behavior information. Personal information can represent our identity on the Internet and can be related to property information. With the popularity of Internet applications and people's dependence on the Internet, personal information can be the most valuable "material" in the era of big data. Therefore, there are certain security risks in personal information.

2. Security characteristics and problem analysis of cloud computing technology

2.1 Characteristics of cloud computing technology

Cloud computing network security characteristics in the application of cloud computing network, for cloud service providers, the traditional way of network security solutions is no longer suitable, and the network security characteristics of cloud computing environment are also changing. The encryption method has not changed in the cloud computing environment, but the network security boundary class and system security class are very different. The cloud service provider can not effectively master the system software like the traditional one, which leads to loopholes in the operation of the virtual system and may pose a great security threat to the network environment

According to the comparison between the previous mainstream security methods in the industry and the difficulties in the cloud environment, the traditional methods of system security are vulnerability scanning and penetration testing, virus killing, terminal security, configuration inspection, etc. In the cloud environment, the understanding of system objects is not enough, and there are corresponding differences in the access to the underlying permissions. From the perspective of the application of network boundary security methods, the traditional security methods mainly use security domain combing, boundary network management and boundary monitoring. In the cloud environment, the security domain is no longer a tree relationship, the boundary is dynamic and fuzzy, and the deployment mode of location is changing. The network security under cloud computing is more complex, the network accounting methods are more diversified, the characteristics of network dynamics and elasticity are also more prominent, service customization and the sharing of measurable services and virtual resources. In the past, the network topology was mostly tree shaped, and the external network entrance of the overall data center was single. The deployment of security equipment based on this architecture was relatively simple. Firewalls and audit equipment could be deployed at the external network entrance and each gathering point. When the technology of cloud computing is applied, a new structure is formed, which makes the network boundary fuzzy. Cloud users can rent internal virtual resources, customize them according to their needs, and share the resources with different users. In this way, system security problems will appear in the sharing. With the application of cloud computing, the increase of network elasticity makes the complex network topology more flexible, which increases the difficulty in network security protection.

Laptop
Network
Smartphone
Cloud Computing
Tablet computer
Server
Mobile
Database

Figure 1 Cloud computing technology

2.2 Analysis of security problems of cloud computing technology

When it comes to cloud computing, security issues cannot be avoided. In fact, this is also the biggest problem encountered in the popularization of cloud computing applications. Although cloud computing service providers are trying to play down or avoid this topic, as end users of cloud computing, this is precisely a major focus of their attention. At present, the commercial value of cloud computing has been confirmed T, and at the same time, these "clouds" have begun to become the targets of hackers or various malicious organizations. Taken together, with the development and success of cloud computing, the security problems of cloud computing are becoming more and more worrying, which are embodied in the following aspects.

The first is the problem of data storage security. The mode of cloud computing determines that a large amount of users' data should be stored in the cloud, which can not only reduce their investment in it equipment and resources, but also bring various conveniences. However, the more data stored in the "cloud", the greater the dependence on the cloud. Once the cloud data is damaged or lost, the loss to users will be very huge. Secondly, there is the problem of data transmission security. Enterprise DC keeps a large number of enterprise private data, which often represents the core competitiveness of enterprises, such as customer information, financial information, key business processes and so on. In the cloud computing mode, when enterprises transfer data to cloud computing service providers through the network for processing, they are faced with several problems: first, how to ensure that the enterprise's data is strictly encrypted and not stolen in the process of network transmission. The second is how to ensure that the cloud computing service provider will not disclose the top secret data of the enterprise when it obtains the data. The third is how to ensure that the access users have strict authority authentication and legitimate data access when they are stored at the cloud computing service provider, and ensure that the enterprise can safely access its own data at any time. Finally, the issue of data audit security. In the cloud computing environment, how can cloud computing providers not only ensure that they do not bring risks and interference to the data computing of other enterprises, but also provide necessary data support, so as to assist third-party institutions to audit the security and accuracy of data generation and realize the compliance requirements of enterprises? In addition, In the process of certification for the sustainable development of cloud computing service providers, how to ensure that cloud computing service providers can provide effective data without damaging the interests of other existing customers, so that enterprises can choose a cloud computing service provider with long-term existence and technical strength for business delivery, is also a potential risk in terms of security.

Table 1 Security issues of cloud computing technology

Security issues of cloud computing technology	type
	Data storage security issues
	Data transmission security issues
	Data audit security issues

3. Network security defense technology based on Cloud Computing Technology

The application of cloud computing network security defense technology should be fully considered from many aspects. The author puts forward the following defense technologies.

3.1 Application of firewall Defense Technology

In the application of cloud computing network security defense technology, the application of firewall defense technology is the key. It is an internal network barrier to block the influence of external unsafe factors. It is mainly to prevent external network users from accessing without authorization. This is the combination of computer software and hardware to ensure the security of the internal network. Firewall is composed of service access policy, packet filtering and verification tools. It has the types of network firewall and computer firewall. From the technical application of network firewall, it is mainly to set firewall in internal and external networks, which can detect the entry information protocol, port and destination address, and filter the foreign information that does not meet the regulations. Firewall technology is developing rapidly at present. On the basis of two hole gateway, there are hidden host gateway and hidden intelligent gateway, which have a good effect on preventing illegal access of unauthorized external visitors. This is also an important application technology content of cloud computing network security defense technology.

3.2 Application of vulnerability scanning and Defense Technology

In the defense process of cloud computer network security, the application of vulnerability scanning technology can also play a good defense effect. The application of this defense technology is mainly to scan the computer system, find some vulnerabilities, and operate through the application of remote control technology. The query of computer TCP / IP service port is combined with the response record of computer host to analyze the data. The current application of vulnerability scanning technology is mainly to scan the program, which can find vulnerabilities and unsafe factors in a short time, and can effectively avoid the occurrence of security problems.

3.3 Application of server redundant backup Defense Technology

Ensure the security of cloud computing network, establish multiple backups of data through the application of backup technology to form a multi redundant data operating system, so that the computer can be combined with backup data recovery in case of threat, so as to ensure the normal operation of data and server. After the computer network security defense system poses a threat, the application of backup technology can also recover these lost data, so as to ensure the role of cloud computing technology and lay a foundation for improving the overall efficiency of technology application. At the same time, the security audit of data mining technology should also be done well. Through the application of neural network technology and genetic algorithm, the quality of data security audit should be controlled to avoid the elimination of illegal content. Pay attention to further improving the network access system to avoid the leakage of information and data caused by this factor. Fourth, the security management and defense of operators. In the application of cloud computing network security defense technology, the implementation of security measures of cloud service operators is also key. Network operators are also facing great challenges under the application of new technologies. To strengthen the protection of cloud computer network security, we should consider from many aspects, strengthen the operation of risk assessment, and establish two kinds of cloud organizations, Private and shared, which requires setting different security service levels to assist users in accurate risk assessment of data, so as to improve the level of security services. We should pay attention to the encryption processing of integrated data. In terms of cloud computing technology services, under the application of corresponding technologies of identity authentication and secure storage, we should ensure the security of cloud computing infrastructure and information transmission, and establish a perfect defense system to ensure information security. In addition, we should establish a trusted cloud and do a good job in security authentication to avoid the leakage of user information.

3.4 Identity authentication security

When the computer logs in, the terminal and server must rely on identity authentication. Only after authentication can they enter the operating system. Identity authentication under the application of cloud computing technology, after the failure of the third-party authentication server, as well as data operation and information theft through illegal means, will lead to the loss of information, and the consequences of hacker attacks are also relatively serious. In addition, the problem of residual security of data is prominent. Under the application of cloud computer technology, data is residual after being deleted by ordinary means, and illegal intruders will bring information security problems after recovery. In addition, the security problem of computer network communication is also prominent. The network security problem of information transmission in the environment of cloud computing is prominent, and the server network attack will cause data theft

4. Conclusion

The application of cloud computing network security defense technology needs to be combined with the occurrence of cloud computer network security problems and some current advanced security technologies. In the context of the development and changes of the times, the application of cloud computer network security defense technology is becoming more and more important. In the application of network security defense technology, it is necessary to expand the interface and comprehensively apply a variety of technologies to improve the security defense effect of computer network as a whole. It is hoped that under the theoretical research on cloud computer network security defense technology, it can provide corresponding theoretical reference for practical development.

References

[1] Yang Zhiyong Analysis of cloud computing network security defense technology [J] Network security technology and application, 2021 (11): 68-69.

[2] Sheng Jian Application of network security defense technology based on cloud computing technology [J] Electronic technology and software engineering, 2021 (14): 256-257.