ISSN 2616-5775 Vol. 5, Issue 4: 71-74, DOI: 10.25236/AJCIS.2022.050413

Network Security Technology Based on Cloud Computing

Lixin Liu

Intelligent Equipment Academy, Shandong University of Science and Technology, Tai'an, Shandong, 271001, China

Abstract: *With the rapid development of computers and the Internet, cloud computing network technology is widely used in all aspects of the world with its powerful data processing capabilities. While it promotes people's convenient life, it also faces many security issues. Aiming at the network security risks and threats under cloud computing, briefly describe cloud computing technology, analyze the types and characteristics of network security under cloud computing, and clarify the importance of network security under cloud computing. Research and analyze the implementation strategy and development direction of network security technology under cloud computing, in order to promote the development of cloud computing network security technology in the future.*

Keywords: *Cloud computing network; Network security technology; Implementation Strategy*

1. Introduction

With the popularization and application of the Internet, the progress of virtualization technology, distributed computing and other technologies, cloud computing technology came into being and has made great progress. However, the diversity of terminal access devices, the expansion of data computing, the application of virtualization technology and the change of data storage mode in cloud computing have all improved the security threat of network data to a certain extent. Malicious network attacks, network viruses and data theft are all important issues affecting network security. Therefore, new requirements and challenges are put forward for cloud computing network security. This paper studies and analyzes the network security in the cloud network environment.

Cloud computing services have five important basic characteristics: on-demand self-service, extensive network connection, resource pooling, fast elasticity and measurable. According to the service type, cloud computing service methods can be divided into SaaS (software as a service), PAAS (platform as a service) and IAAs (infrastructure as a service). At the same time, cloud computing technology also has the technical characteristics of autonomy, traversal and quickness. Therefore, in the development process of today's society, we attach great importance to the application of cloud computing technology. This requires that in the actual process of social development, we should ensure the correct use of cloud computing and make the design and application of cloud computing technology more reasonable. In the process of using cloud computing technology, we should also do a good job in network security detection and network security risk analysis to ensure that all aspects of its construction meet the requirements and better realize the application effect of cloud computing technology.

With the gradual development and maturity of cloud computing technology, cloud computing security problems also follow. Network security has become an important factor hindering its further development. It involves not only the privacy security of cloud users and the resource security of cloud services, but also the possible security problems in the network transmission between cloud users and cloud services. The cloud computing environment mainly includes nine security threats, such as data destruction, data loss, account hijacking or service traffic hijacking, unsafe interfaces, denial of service attacks, malicious insiders, abuse of cloud services, insufficient strict cloud computing review, shared security vulnerabilities and so on. The content of cloud computing security is closely related to the security of data, so protecting data and preventing data problems is very important for cloud computing security

ISSN 2616-5775 Vol. 5, Issue 4: 71-74, DOI: 10.25236/AJCIS.2022.050413

2. Network security risks and threats under cloud computing

2.1. Safety risk

2.1.1. Manage risk

According to the research and analysis of foreign professional institutions, cloud computing network security is not a network security technical problem. Most of the security time is caused by non-technical factors such as poor management or improper use. Cloud services depend on the cloud computing network provided to cloud users. In this case, the management risk faced by cloud computing network directly affects the security and performance of cloud services. Among them, the common management risks are security, convenience and ambiguity, identity management, internal staff management, service interruption, etc.

2.2.1. Technical risk

The flexibility, reliability and high scalability of cloud computing platform depend on the use of some new technologies, and the use of these new technologies also brings some new security risks. Different from the traditional model, cloud users cannot directly control their data and business by placing them on the cloud computing platform. Fixed infrastructure is the carrier of cloud user resources, and its security directly affects the security of cloud services and cloud users. Physical security is the foundation of fixed infrastructure security, and improper behavior will endanger the security of fixed infrastructure. For example, if the equipment is stolen or lost, it is easy to cause data loss and leakage, power failure and fire, temperature control system failure, etc., and it is easy to damage or even destroy the fixed infrastructure. In addition, environmental factors affect the safety of fixed infrastructure, which mainly refers to ensuring the safety of the surrounding environment where the fixed infrastructure is located. Environmental safety technology mainly refers to the protective measures against natural factors such as earthquake, landslide, fire, flood and temperature.

Virtualization technology will also bring a series of security risks to cloud computing network. For example, the vulnerabilities brought by the core technology and the security vulnerabilities brought by the inherent characteristics of the cloud computing network, as well as the migration risks caused by sending the content in the original virtual machine to another virtual machine through the cloud computing network.

2.2. Source of threat

Threats may come from inside or outside of cloud computing, or from people or applications. According to different sources, cloud computing network threats are divided into four aspects: anonymous attackers, malicious service providers, credit attackers and malicious internal employees.

2.3. Threat Technology

The threat technology of cloud computing network security is mainly composed of traffic eavesdropping, denial of service attack, tampering attack, forgery attack, insufficient authorization, virtualization attack, trust boundary overlap, sniffing attack and port scanning.

3. The importance of network security under cloud computing

First, network security technology protects information and data. In the cloud computing environment, a large number of personal and enterprise information and data are stored in the network. Once there are network security problems, it is easy to cause information and data leakage or loss, which will have a corresponding impact on individuals and a lot of economic losses. The application of network security technology can realize the security protection of user information and data, make the data more secure, reduce the possibility of data leakage, and prevent the personal interests of users from being threatened.

Secondly, network security technology can also strengthen the security of network system. Network security technology can protect the application software installed through the network system and improve the security of users' network. Network system is the main area of network security risk. If the security protection of network system is insufficient, it will easily produce network security risk. The application of network security technology can comprehensively protect the network system and improve the security of user information. At the same time, network security technology can provide security

ISSN 2616-5775 Vol. 5, Issue 4: 71-74, DOI: 10.25236/AJCIS.2022.050413

protection corresponding to user equipment, prevent trojan virus intrusion and information security problems caused by insufficient equipment protection.

4. Network security technology strategy under cloud computing

4.1. Network security technology

4.1.1. Intelligent firewall

The intelligent firewall is improved on the basis of the original firewall. Compared with the original firewall, it will no longer ask users. Intelligent firewall mainly includes anti scanning technology to prevent data acquisition by scanning means; Anti spoofing technology for identifying and intercepting false addresses and intrusion prevention technology for protecting system data packets and preventing illegal intrusion from the outside world.

4.1.2. Cryptography

In the cloud computing environment, password technology is often used to ensure the data security in the cloud computing network. Information encryption technology in network security is to use encryption related algorithms to change the transmission content into a specific interpretation password before transmission. The receiver decrypts and translates the encrypted information in the same way to protect information security. Common cryptographic technologies in cloud computing environment include cryptographic model, replacement encryption technology, replacement encryption technology, symmetric encryption technology, public key encryption technology, etc. Among them, symmetric encryption technology is the same technology that encrypts the secret key and decrypts the key in the cryptosystem. The most representative symmetric encryption technology is des technology. In asymmetric encryption technology, the encryption key and decryption key are very different, and they can not be obtained by reasoning and calculation. PKI technology and RAS technology are typical technologies in asymmetric encryption technology.

4.1.3. Anti virus technology

Anti virus technology is mainly divided into static anti-virus technology and dynamic anti-virus technology [1]. Static anti-virus technology can update the virus database and check the security of the virus to judge the condition of the computer, so as to ensure the security of the computer. The purpose of anti-virus technology is to make a dynamic judgment according to the operation of the computer.

4.2. Physical security technology

Physical security is the first security in cloud computing. In cloud computing network security, the physical security of fixed infrastructure is the most easily ignored, but most network failures are caused by physical security problems. And the security threats faced by network physical devices are diverse. Therefore, physical security technology should ensure the confidentiality, integrity and availability of information system, and physical security protection should be carried out from the aspects of physical equipment security, environmental security and so on. For example, in order to improve the ability of physical security protection, managers can place devices with different functions in different locations in the space, reduce the pressure of security protection in an area [2], and ensure the security of data in the cloud computing service platform.

4.3. Network security protocol technology

Security protocols commonly used in cloud computing environment include security encryption protocol, data verification protocol, key management and security protection protocol. The level and scope of application of each protocol are different. A unified platform model needs to be established in the provision of cloud computing services. Relevant departments can also establish and improve scientific and reasonable network security rules and regulations according to the network security agreement and in combination with the current actual situation and future development, carry out corresponding network technology security management, and promote the formation of a safe and developable cloud computing network.

ISSN 2616-5775 Vol. 5, Issue 4: 71-74, DOI: 10.25236/AJCIS.2022.050413

5. Measures to strengthen network security under cloud computing

(1) Improve cloud security laws and regulations: We must provide legal provisions for all kinds of new network attacks and acts endangering network information security, and formulate relevant policies, laws and regulations to ensure and protect network security, so as to supervise the network. We should strengthen publicity and supplement cloud computing network security knowledge, strengthen the management of cloud computing network security, and create a stable, safe and harmonious network environment. At the same time, relevant departments should pay more attention to network security, provide various services in the cloud computing environment, and create a good green network environment.

(2) Improve users' awareness of network security: Establish and cultivate the excellent information security awareness and standardized security operation habits of computer network users, learn the common sense of network security, do not easily trust others, ensure the complexity of passwords, ensure that passwords meet the requirements, remember passwords and use multiple passwords

(3) Enhance the security of data storage: Password technology shall be used for the data center, and the detection and dynamic tracking of visitors shall be well done. In case of abnormal conditions or abnormal data, it shall be disconnected in time. At the same time, the stored data should be backed up regularly to avoid data loss and damage when cloud computing services are attacked and invaded.

(4) Focus on access security: Control the access of cloud computing and formulate special corresponding security strategies. In practice, the principle of minimum permission, the principle of disclosure, multi-level security policy and multi-level security isolation [3] are used to carry out special access control on ports and sockets, hide the IP address of the host, and properly deal with these sensitive parts to prevent attackers from using them to attack.

6. Conclusion

With the continuous progress and development of cloud computing technology and the creation of cloud computing environment, it not only meets people's needs, but also brings many threats and more and more security challenges. Therefore, both administrators and users should establish a good awareness of network security, cultivate standardized safe operation habits, strengthen network information security protection technology, pay more attention to network security, do not give criminals an opportunity to actively promote the progress and growth of China's cloud computing network industry.

References

[1] Liu Zhichao. Application status and countermeasures of network security technology based on cloud computing environment [J]. Overview and trend of Network Security, 2017 (12): 16743.
[2] Zhang Hao. Talking about computer network security in cloud computing environment [J]. Network Security Technology and Application, 2020 (10): 93-94.
[3] Wang ran. On Network Security and measures under Cloud Computing [J]. Electronic Technology and Software Engineering, 2018 (1): 224, 225.