Academic Journal of Computing & Information Science
ISSN 2616-5775 Vol.2, Issue 3: 120-125, DOI: 10.25236/AJCIS.020314

Discussion on Computer Network Security in "Cloud Computing" Environment

Yan Li

Jingdezhen Ceramic Institute, Jingdezhen 333403,China

ABSTRACT: *With the continuous development of science and technology in China, the current society has shown an informatization and intelligent development trend. As an emerging technology, cloud computing has the characteristics of promoting the efficient and convenient resource sharing process and has an important impact on people's daily lives. Although cloud computing provides convenience to people, because it needs to collect and organize personal information of users, this will cause a series of security issues and affect the overall network environment. This article mainly starts from the basic overview of cloud computing, analyzes the problems of computer network security and specific protection measures in the cloud computing environment, and hopes to provide valuable reference for related computer network security staff.*

KEYWORDS: *"cloud computing"; computer; network security; solution*

1. Introduction

The rapid development of today's society, the continuous popularization of computer information technology, and its widespread use in all walks of life, the emergence of cloud computing, while providing convenience to people's lives, is also affecting people's thinking and production and lifestyle. Although it has undergone continuous development and achieved some results, in the process of cloud computing services, there are also a series of network security problems, such as viruses and hacking, which cause data leakage and serious losses. Realizing the security of information can effectively promote the sustainable development of computer network technology. Therefore, it is necessary to strengthen the security of computer network systems in the cloud computing environment. It can be seen that the research on computer network security in the "cloud computing" environment is of great significance.

ISSN 2616-5775 Vol.2, Issue 3: 120-125, DOI: 10.25236/AJCIS.020314

2. Basic overview of cloud computing

2.1 Basic Concepts of Cloud Computing

Cloud computing is essentially a new service model that relies mainly on the Internet to implement a shared service. As shown in (Figure 1), its prominent use function is to provide information and data storage in a large-scale distributed environment And corresponding network services. The more prominent feature of the use of cloud computing is that it can achieve secure storage, enable terminal information equipment to be effectively used, and enable sharing of different information equipment. Therefore, the security of the network is mainly an effective protective measure established against the information data system, thereby ensuring that the information is not infringed [1].

2.2 Basic Features of Cloud Computing

From a macro perspective, the characteristics of cloud computing can be summarized as having a certain scale. Powerful computing capabilities enable cloud computing to provide good support for the simultaneous operation of very large-scale servers. Furthermore, reliability is also a prominent feature of cloud computing. This reliability can well guarantee safe and stable operation in very complex network environments. In addition, cloud computing also highlights a certain degree of versatility, which can meet the different needs of different users, and can provide users with corresponding services in a timely and accurate manner. In terms of scalability, the application of cloud computing technology can make good use of its scalability and complete a series of services to provide users with a satisfactory experience. In essence, virtualization can be said to be a more prominent feature in cloud computing. After providing the corresponding IP address, users can browse in the network environment freely and obtain the required services. The main use of the cloud computing is an automated and centralized management mode, which can reduce maintenance costs. Users only need to pay a very low cost to get fast network services [2].

3. The computer network security issues in the "cloud computing" environment

3.1 Security certification issues

In the normal use of cloud computing, there is no clear limit to limit the contact between information and data. It means that when the demander obtains the required information and data, the obtained data can be reused indefinitely. In this case, the same calculation flow can be used for different areas and types of information data.

ISSN 2616-5775 Vol.2, Issue 3: 120-125, DOI: 10.25236/AJCIS.020314

In this way, the calculation efficiency can be effectively improved. However, in the context of this computing environment, there are still many problems in the method of obtaining data information, and these problems have not been effectively solved. The main reason for this is the transparency. When a user browses the Internet by using a valid IP address, during the browsing period, the user has a good understanding of the received information and data, channels, methods, and calculation methods used for the data. This information is not known. From the perspective of the user, the security of his personal information is not clear and clear. Even if it has been leaked or illegally used, the user cannot know the first time. Therefore, based on this situation, although the user's personal information needs to be authenticated and verified in the existing network system, in essence, there is still no effective security protection measures, and no effective external monitoring has been established. It is difficult to guarantee the security of personal information of users [3].

3.2 Tthe problem of illegal invasion

During the fair use of cloud computing technology, data computing and information analysis do not require user participation, and can be carried out independently. This kind of calculation method is convenient, but it is extremely dangerous. If there is a problem in the calculation of a certain step or the analysis process of a certain link, it will cause an uncertain degree of loss to the user. The most important users cannot find it in time. The problems that have arisen mean that corresponding measures cannot be taken in a timely manner. Many network users are aware of computer hackers. If computer network information does not have perfect security measures, it is easy to be attacked by hackers, causing information security problems and causing serious losses. By implanting network viruses, computer network information can be stolen. Such illegal acts will bring a lot of harm to human computer information activities. In the cloud computing environment, the probability of such problems will increase, and it will cause more damage to users. Although cloud computing has certain data protection capabilities, it does not work well, and it cannot be completely kept secret. There are huge amounts of information and data in cloud computing systems. Once illegally invaded by the outside world, it will have a serious impact on the data of the entire database system, and this impact is difficult to recover. The fundamental reason lies in the lack of security of the terminal equipment. The current information technology is constantly developing, and the accompanying virus technology will be constantly updated. The previous computer protection methods still do not protect these new viruses. Therefore, good protection measures need to be established, otherwise, when the system is infringed It may cause user information data to leak, tamper with, or even be used illegally. Therefore, both users and service providers need to pay more attention to the safety of terminal equipment [4].

ISSN 2616-5775 Vol.2, Issue 3: 120-125, DOI: 10.25236/AJCIS.020314

3.3 Hidden security risks

In the application of cloud computing technology, it is not only vulnerable to external attacks, but also some security risks within itself, mainly in terms of system management, design, technology, etc., many of the issues mentioned above have caused a lot of security to cloud computing Hidden danger. Although technology is constantly developing, the development of the Internet will obviously not be limited to national, regional, time, and spatial restrictions, but the security of the open network environment has been greatly reduced, which has created favorable opportunities for illegal activities by some criminals. Many offenders use the defects of this network to illegally obtain personal information of others for illegal activities, resulting in damage to the economic interests of others. Although there are measures to protect data security in cloud computing, there are still many loopholes in the actual transmission process [5].

4. Computer network security protection measures in the cloud computing environment

4.1 Raising awareness of computer network security protection

In the cloud computing environment, more efforts are needed to improve network security protection. First of all, it is necessary to increase user awareness. In the cloud computing environment, different users will use a variety of network security issues. Therefore, it is necessary to increase the awareness of network security precautions of users to protect the overall network security. Users need to have certain knowledge of information and data network security, and fully understand the methods of protecting personal information and data security in a cloud computing environment. Common methods include: system changes, timely updates, regular maintenance of computer network security, and purchase of efficient antivirus software. These methods can effectively prevent the invasion of viruses and hackers, so that the network itself has a certain degree of reliability and security [6].

Authentication of identity is an effective way to ensure the security of user information and data. Users are authenticated to promote the security of personal information and data. In addition, in the cloud computing platform, it is also necessary to continuously improve the management of user identity authentication, and strictly formulate corresponding procedures, requiring all users to continue to store the required data information after identity verification. On the other hand, they have not passed user identity authentication. People cannot browse and download the information and data stored in cloud computing. In this way, user data security is effectively guaranteed. In addition, users should consciously protect personal information, and must keep confidential information such as account numbers, verification codes, and passwords, and do not tell others [7].

ISSN 2616-5775 Vol.2, Issue 3: 120-125, DOI: 10.25236/AJCIS.020314

4.2 Improve the effective development of safety technology

Regarding the cloud computing network security problem, it can be summarized that the security technology is not perfect. When providing computer network security, it is necessary to combine relevant laws and security technologies to ensure the computer network security under double guarantees. The law is still being improved. Therefore, China needs to pay more attention to computer network security technology. Strengthen the training of network information security professionals, proceed from the issue of computer network information security, implement practical security management, effectively implement security protection, avoid hackers and network viruses, and fundamentally ensure computer network information security.

For data storage, sharing, transmission, and server outages that cause data damage and loss, to solve this problem, relevant researchers can develop information and data recovery technology, and use this technology to effectively ensure that the server is interrupted. Time data integrity, and can be transmitted after normal operation. In addition, the ability of network identification should be strengthened to ensure that user information and data will not be leaked. For current hacking techniques, viruses, etc., it is necessary to take good solutions to continuously improve the anti-virus capabilities of the computer's own firewall [8].

4.3 Improve the security and confidentiality of data

1) The use of encryption technology for data can effectively improve the security of information and prevent the leakage of personal information of users. The use of encryption technology ensures that the security of the data during transmission can be guaranteed. In addition, encryption algorithms can be used to ensure data security performance.

2) It can make full use of filtering technology to block abnormal information data and improve the security of the cloud environment.

2) Then there is the data authentication technology, which can effectively evaluate the risk required by the user, and then assist the user to set permissions to ensure the security of the user's personal information, thereby effectively improving the security of user data in the cloud environment. With the continuous updating of science and technology, the security of computer network data in the cloud computing environment can be improved.

5. Conclusion

In summary, in the development of modern society, cloud computing has shown obvious advantages, which brings convenience to people's daily life, learning, and work, but it should also pay attention to its information security issues to avoid

ISSN 2616-5775 Vol.2, Issue 3: 120-125, DOI: 10.25236/AJCIS.020314

unnecessary unnecessary damage to users loss. Therefore, users should fully understand the problems of cloud computing network security, take precautions, and deal with the potential security risks of computers in a timely manner.

References

[1] Qi Xin, Jia Jiahua, Li Fangyu (2019). Cognition and Thinking of Computer Network Security in Cloud Computing Environment. World of Digital Communications, vol.45, no.28, pp.129-129.
[2] Wu Jian (2019). Thinking and Analysis of Computer Network Security in Cloud Computing Environment. Digital World, vol.45, no.41, pp.100-101.
[3] Lin Mingxin (2017). Computer Network Security in "Cloud Computing" Environment. Science and Information Technology, vol.23, no.34, pp.156 -157.
[4] Song Hengli (2018). Computer Network Security in Cloud Computing Environment. Digital World, vol.12, no.12, pp.234-235.
[5] Peng Yuanhui (2019). Analysis of Computer Network Security in Cloud Computing Environment. Science & Technology Innovation Review, vol.45, no.12, pp.236-237.
[6] Li Yinli (2018). Application of cloud computing technology in secure storage of computer network. Military-civilian dual-use technology and products, vol.45, no.12, pp.173-174.
[7] Liao Wei (2017). Talking about Network Security Threats and Countermeasures in Cloud Computing. Digital World, vol.45, no.18, pp.137-137.
[8] Zhang Hansen (2018). On Information Security Audit System in Cloud Computing Environment. Information Communications, vol.54, no.13, pp.178-179.