Research on Computer Network Security Policy in Cloud Computing Environment

Dawe Gui

School of Information and Intelligent Technology, Shaanxi radio and Television University, Xi'an, Shaanxi, 710119, China

guidw@163.com

Keywords: Cloud Computing, Computer, Network Security.

Abstract: With the continuous development of modern science and technology, our country has gradually entered the "cloud computing" era, in such an environment, computer network security has been widely concerned. Based on this, this paper briefly expounds the connotation and characteristics of cloud computing, analyzes the current situation of computer network security in "cloud computing" environment, and puts forward the computer network security strategy in "cloud computing" environment from the aspects of constantly strengthening the awareness of users' prevention, increasing the development and utilization of security technology and improving the security and confidentiality of information..

1. The Connotation of Cloud Computing

At present, people mainly use the computer to browse the network to obtain the required data information, in the information age, the rapid development of network technology and computer technology, a number of new technologies have emerged, providing great convenience for people's lives, cloud computing technology is one of them, the application of this technology is relatively simple and convenient, more and more scholars around the cloud computing environment network security issues.

Literally, cloud computing is a new method of computing based on computers, with a shared-based framework that can be used to store information while providing related network services, as shown in Figure 1. Cloud computing has many application advantages, such as ensuring the security of data storage and facilitating the application of data information by terminal devices. Therefore, in the information age, the network security of the computer is mainly to set up the corresponding preventive measures for the information data, and at the same time to formulate the protection measures of the data information, so as to avoid the leakage of the stored information because of objective factors, so as to ensure the security, confidentiality and reliability of the data stored by the computer.

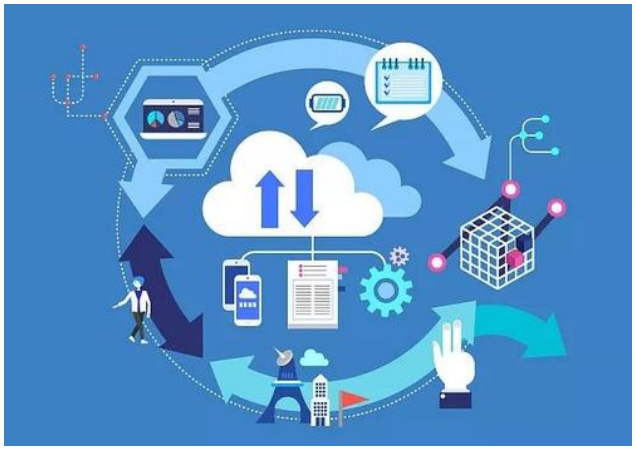

Figure 1 Functions and characteristics of cloud computing

  DOI: 10.25236/ictmic.2020.093

The main features of cloud computing include: the confidentiality and rigor of the data, in short, that the data stored in the computer is not arbitrarily disclosed to unauthorized users; cloud computing can also reflect the integrity of the data, that is, unauthorized users are unable to edit or modify the data in the computer at will; controllability refers to authorized user ownership. The right to edit and process information data; it also includes vetting, and if there is a security problem in the network, there is a need to use certain methods to effectively control the problem and strictly review the relevant data[1].

2. Problems in Computer Network Security

2.1. Safety Certification

In the process of applying cloud computing, the interaction between information and data does not produce obvious price limit, after the other party obtains the required data, the acquired data can be used repeatedly, in such a background, it is necessary to integrate multiple types and regions of data in the process of operation to improve the operation efficiency of the computer. However, in the operation of computer, there are still some problems in the means of obtaining information data, mainly reflected in the low transparency. When users browse the network system of computer, it is difficult for them to understand clearly the way of receiving information, the method and the calculation method of data application, and the user can not know whether their information is leaked or illegally used in the first time. Therefore, in the context of cloud computing, although users need to authenticate and review the information, there is a lack of corresponding security protection methods and monitoring means in this link, and the personal information of the knowledge computer users has security risks.

2.2. Illegal Invasion

With the application and promotion of cloud computing technology, data operation and data analysis can be carried out independently, and users do not have to participate in this link. Although this kind of form is very convenient, it also shows that if there is a problem in any part of the analysis or operation, it will bring some losses to the user, and the user can not find out the resulting questions in time. All along, hacking and cybervirus intrusion are the main influencing factors of Internet security, and it is possible to disclose the personal information of users, and the probability of occurrence in the past is relatively high. In the background of cloud computing, such problems will be further aggravated, and the resulting problems and losses will be higher than before, which will seriously damage the interests of users. Although cloud computing has the function of protecting data, its effect is limited and there is no way to achieve the effect of total secrecy. The data stored in cloud computing is not a simple single item or column information, but a large amount of data information base, if the database is illegally invaded by the outside world, it will cause the data in the database to suffer a certain degree of negative impact, and this impact is difficult to recover. The main reason for this kind of problems is that the security of the terminal equipment is insufficient, with the continuous development of information technology, the level of virus technology has gradually improved, the previous computer security protection methods have been unable to meet the requirements of the current stage of prevention, if not timely and effective protection strategy, there is a risk of virus intrusion into the computer, theft of personal information, tampering or illegal application of personal information, resulting in serious after. Therefore, both service providers and users need to pay special attention to the security of terminal devices[2].

2.3. Internal Cloud Computing

In addition to external attacks, cloud computing also leaves some security risks inside, mainly reflected in system technology, system design and system management, in the process of cloud computing, some of the hidden dangers can not be avoided. In recent years, the rapid development of science and technology, the Internet can break through the regional and even national restrictions, but the excessive opening of the network environment, will reduce the security of use to a certain

extent, let the lawbreakers. Some lawbreakers will exploit the Internet to steal other people's information illegally, affecting other people's economic benefits. Although cloud computing technology has implemented many protective measures to protect information security, there will be malicious interception in the transmission of information data, which indicates that the cloud computing needs to be improved continuously.

3. Computer Network Security Policy in " Cloud Computing "Environment

3.1. To Continuously Strengthen the Awareness of Users on Prevention

To improve the protection of network security in cloud computing environment, it is necessary to enhance the user's awareness of prevention. In the new period, compared with the past, the problem of computer network security will obviously increase, and the form of the problem will also have a variety of characteristics, if the user's security awareness is insufficient, it is difficult to ensure the security of the network. This means that users should have some information security-related knowledge about how to effectively protect their information in a cloud computing environment. Common methods of protection include system updates or direct system changes, the use of professional antivirus software, or the maintenance of computer network security every certain time, as a way to organize hacking into computer systems, while avoiding system intrusion into viruses.

Identity authentication is one of the main effective methods to protect data security, and users can adopt this method to further ensure the security of information. The platform of cloud computing also needs to adopt the strategy of identity authentication, the system visitors must go through the authentication to successfully browse the required information, the person who does not pass the identity authentication is not allowed to browse or download the data, to avoid the security of the data is negatively affected by human factors, as shown in the figure. In addition, users should consciously protect their own information, it is best not to easily pass password, verification code or account information about authentication to other people[3].

Figure 2 Information can only be used after authentication

3.2. Increase the Development and Utilization of Safety Technologies

Cloud computing network security mainly depends on the update speed of security technology and the size of virus technology and hacker technology update speed difference, which means that the research of security technology needs to be strengthened continuously. In the case of data transmission, sharing and storage, there may be server disruption, resulting in data loss or damage. In this case, the R & D department of the technology needs to actively organize the research and development of the data recovery technology, and use this technology to restore the integrity of the data during the server interruption, while ensuring the efficient transmission of information during the normal operation of the server. In addition to the above mentioned content, it is necessary to

further enhance the recognition level of the network, limit the occurrence of illegal browsing, and avoid the question of information disclosure. Moreover, relevant departments also need to deal with the problem of hackers or viruses pertinently, update the user's system regularly, and improve the ability of the computer to resist the virus through the firewall.

3.3. Improving the Security and Confidentiality of Information

First of all, information encryption technology can be adopted to improve the security of data, so as not to disclose the user's personal letter. The reasonable use of encryption technology can ensure the security of information in the transmission process, and the encryption algorithm can also ensure the reliability of data use, such as figure. Second, you can use filtering technology, which can intercept abnormal data for the first time and ensure the security of the cloud environment. Finally, the authentication technology of data can be used, which can evaluate the needs of users, judge whether there is a risk, and also judge the degree of risk, and then help users to set the relevant permissions reasonably, ensure the information security, and reduce the cloud environment to the user's personal information. With the development and updating of security technology, the network security in cloud environment will be improved continuously[4].

Figure 3 Using encryption technology to ensure network security

4. Conclusion

To sum up, cloud computing has the characteristics of confidentiality, rigor, controllability and integrity, and has strong application advantages, but there are still some problems in the actual application process, and the network security of the computer is not. Therefore, we can fully refer to the above contents, ensure the security of information data, facilitate the daily work and life of people, and reduce unnecessary losses.

Acknowledgements

This research has been financed by The Vocational Education Research Project in 2019 of the Shaanxi Society of Vocational and Technical Education. Research and Practice on the training mode of school enterprise deep integration information technology talents based on 1 + X certificate. (SZJZD19-001)

References

[1] Xiao, Hong. Analysis of computer network security problems in the "cloud computing" environment. Information Technology and Informatization , no. 01, pp. 138-140, 2020.

[2] Guo. Computer network security analysis in cloud computing environment. Computer Products and Circulation, no. 01, pp. 66, 2020.

[3] Tan. Computer network security in cloud computing environments. Electronic Technology and

Software Engineering, no. 22, pp. 196-197, 2019.

[4] Zhou, Shi. Explore computer network security in the "cloud computing" environment. Popular Standardization, no. 12, pp. 20-21, 2019.