Computer Network Security under the Cloud Computing Technology Environment

Sun Bin¹*, Wang Yongjie²

¹Weifang Medical University, Weifang, China
²Shandong College of Information Technology, China

*Corresponding author: xxb@wfmc.edu.cn

Abstract. The development of network technology has changed the traditional network application mode to coordinate all kinds of data and resources effectively. It brings about the improvement of computer computing ability, data processing ability and storage ability, and offers users a new and optimized usage experience by improving the ability of computer network service. However, the construction of cloud computing technology environment also causes people to worry about the network security, and the problem of computer network security under cloud computing technology environment can not be underestimated. The top priority is to speed up the research and development of defense technology, improve the risk response system, consciously enhance the awareness of security protection, and be answerable for dealing with network risk with multi-pronged measures. This work mainly discussed the problems of computer network security under cloud computing technology environment from aspects of encryption technology, authorized accessing, network monitoring, and consciousness awakening, expecting to provide guidance and reference for computer network security response under the background of cloud computing.

Keywords: Computer technology; Cloud computing; Network security; Analysis

1. Introduction
The emergence of cloud computing is conducive to people's production and life, but it has also brought some negative effects, for example, a variety of network frauds are endangering the security of computer networks. Therefore, under the background of cloud computing, carrying out further analysis is the inevitable requirement to promote the development of computer network in order to ensure the smooth development of various social work.

2. Cloud Computing Environment
Cloud computing came into being in 2008 with bright market prospects since it has high data processing and recovery performance. At present, cloud computing is the trend of the times, but it also triggers network security concerns. In essence, cloud computing is the Internet computing mode that improves the efficiency of data processing and supports a high degree of resource sharing. With the rapid development of information technology, cloud computing technology is also developing. The
The application of cloud computing can effectively reduce the manpower input and cost input of traditional data processing, and simplifies the cumbersome procedures of traditional data processing. Cloud computing has a specific data storage center, which can effectively recover and process related data. It has the function of data sharing, which can provide a sharing platform for different devices and improve resource utilization. Cloud computing can serve users of different sizes and geographic locations, and reduce the risk of data theft, so as to protect the integrity of data. Cloud computing can make the extraction and use of network resources more convenient cooperated with virtualization technology, cloud storage, and distributed processing.

3. Cloud Computing Structure

Its structure is shown in Fig. 1. In Fig. 1, the user access layer is a series of supporting services provided by cloud computing to facilitate cloud computing users to use the services provided by cloud computing. The access to cloud computing requires a series of access interfaces. According to different requirements of cloud computing users for cloud computing services, cloud computing needs to allocate different access interfaces for different levels of services. There is a service directory in the user access layer, which lists the services that users can choose according to their needs. Subscription management enables users to query services that have been subscribed, and to re-subscribe to other services or terminate a service. Service access is an access interface for cloud computing services of different levels. The function of the application layer is to provide software services for users. The platform layer is the upper layer of the resource layer, which encapsulates the service of the resource layer and makes the interface more friendly when users use cloud computing services. The function of the middleware service layer is to provide users with extensible message middleware or middleware for processing a series of things. The resource layer is the most basic level of the whole cloud computing structure. The resource layer of cloud computing provides some virtualized resources, that is, the resources exist in a virtualized resource pool, which is equivalent to the encapsulation of physical resources.

![Cloud Computing Structure](image)

**Fig. 1. Cloud computing structure**

4. Hidden Dangers of the Computer Network Security under Cloud Computing Environment

4.1. Hidden dangers arising from inadequate security systems

The emergence of cloud computing is conducive to the further development of computer network. However, due to the limitations of current technology, the security system of computer network is not
perfect. Since cloud computing is open and globalized, the imperfection of computer network is easily attacked by some powerful viruses or network hackers, which will cause the loss of computer network to various degrees. It can be seen that the security system of the current computer network is not suitable for the open characteristics under the background of cloud computing. In order to improve the security of the computer network, it is necessary to optimize the security and secrecy system of the computer network, so that it can better resist the virus, block the attack of hackers, and ensure the security of the computer network.

4.2. Risks arising from weak information discrimination
At present, cloud computing is in the process of development and perfection, which means that neither system nor technology is very mature. However, in reality, with the popularity of computer network, cloud computing begins to change from simple to complex. In the face of complex computer network, people should have the ability to discern information. Investigating the development situation of computer in China, it can be seen that although it has been further popularized, most of the people only master the basic computer knowledge, which gives some criminals a chance to take advantage of, thus seriously endangering network security. Although cloud computing provides security for enterprises and related organizations, the effect is not obvious. During the operation of cloud computing, the information and data of enterprises and related organizations can be transmitted normally. However, some enterprises may be intercepted or lose information midway during the transmission of information, which makes enterprises face great credit risks and may cause certain losses. Therefore, it is necessary to explore how to improve the computer network security problem.

4.3. Prominent contradiction between open attribute and protection
Cloud computing has many characteristics, including globalization, complexity and openness. It can provide businesses and users with a large amount of information, but it can also provide opportunities for cybercriminals, thus endangering the property and information security of enterprises and users. Therefore, it is necessary to formulate corresponding protection measures. At present, the main protection measures are data encryption and identity authentication. These two technologies are the latest security protection technologies, which can better prevent viruses and hackers from attacking. However, these two technologies are not very mature, and there are still many hidden dangers in the specific implementation.

5. Construction of Computer Network Security under Cloud Computing Environment

5.1. Improving information encryption technology
Under the cloud computing environment, it is necessary to improve information encryption technology in order to improve the security of computer network. Information encryption technology includes symmetric encryption technology and asymmetric encryption technology, both of which should be continuously improved. Additionally, it should ensure that information is encrypted during transmission, that is, in cloud client, cloud storage and cloud management, so as to create a secure environment in which information can be transmitted in a timely, effective and secure manner, and to ensure the information security of enterprises and related organizations. At the same time, it is necessary to set up asymmetric information encryption technology to improve the security of information, realize data encryption through secure encryption technology, and ensure the information security under the background of cloud computing. Symmetric encryption technology is divided into substitution password and transposition password according to different encryption methods. In the process of encryption, the substitution password replaces a character that needs to be encrypted with other symbols that are not related to the encrypted character, and the transposition password is to recombine or sort a string of information that needs to be encrypted in the process of encryption and disrupt its original order. In practical applications, the two are generally used in combination, and the technical communication model is shown in Fig. 2. Asymmetric encryption technology is based on
asymmetric cryptography, also known as public key encryption technology. In the process of plaintext encryption and decryption, asymmetric encryption technology needs to use two keys, one is the public key that can be disclosed to the public, and the other is the private key kept by the decrypter that cannot be disclosed to the public. When data transmission is needed, the encrypter uses the public key of the decrypter to encrypt the original plaintext, and the decrypter acquires the ciphertext and decrypts the ciphertext with private key. The additive communication model of asymmetric cryptography is shown in Fig. 3.

![Communication model of asymmetric encryption technology](image)

**Fig. 2.** Communication model of symmetric encryption technology

**Fig. 3.** Communication model of asymmetric encryption technology

5.2. **Innovating data security protection technology**

Although the process of transmitting user information from computer network to cloud is very fast, it may be intercepted by hackers. In view of this kind of problem, network management scheme, such as VPN and SSL, can be adopted to ensure the security of information transmission between users and cloud. The gateway access scheme is to build a hidden network in the transmission path. The hidden network is only for a user, which can improve the security of the network information. Users need standard user identity when using data security protection technology, and different users can set different information access rights to achieve restricted access. After logging into the cloud, password is issued through security management, and the access identity is identified by integrating biological recognition and digital certificate technology. In this way, unauthorized users cannot access information, and the ideal role-based access control technology of the cloud platform can be applied.
The role-based access control model for the cloud platform is shown in Fig. 4. The model consists of five functional modules, including cloud platform, service directory, audit system, unified authorization platform, role-based access control module and interactive platform. The interactive platform mainly interacts directly with the user. The user can log in on the platform and customize the role with required permissions. This platform is the link between the cloud computing platform and the user. The unified authorization platform is mainly responsible for the distribution of roles and permissions of cloud computing users, and also undertakes the responsibility of cloud computing user information. The corresponding relationship between roles and permissions is also managed by the unified authorization platform. The role-based access control module is responsible for detecting the legitimacy of user access resources and judging the results. Cloud computing users can only access the corresponding resources according to the permissions of their own role group after passing the detection of role-based access control module, otherwise the access to the resources is denied. The service directory lists the size of various resources that cloud computing users can access within their own limits after being assigned roles and permissions, while cloud computing users can only access the resources allowed in the service directory. The cloud platform is the cloud computing platform, providing service for cloud computing users.

\[\text{Fig. 4. A role-based access control model for cloud platform}\]

5.3. Power of cloud platform monitoring system

Hacker intrusion is also an important factor affecting network security. Using proxy server in actual prevention and control can obtain better defense effect. Filter is used in data transmission and reception. For all data monitoring, the data information with security risks can be intercepted directly to ensure the security, reliability and integrity of the data. In order to better fight hackers and viruses, it is necessary to establish a cloud platform monitoring system, which includes system function modules and data tables of important modules of the system, so as to deploy and test the data query function in the actual environment in advance. The content of the function module of the cloud platform monitoring system is shown in Fig. 5. After logging into the system, the monitoring manager can view the current virtual machine monitoring data and virtual machine related list, have the authority to manage the virtual machine, can add, delete, and edit the virtual machine, and at the same time add alarm rules and set the relevant threshold. In addition to the above permissions, the system administrator also has user management, role management, system configuration and other permissions. The monitoring of virtual machines is mainly divided into two parts: resource monitoring and application service monitoring. In the application layer of cloud platform, there are many virtual machines, and resource monitoring mainly includes monitoring the CPU, memory usage, system average load, disk utilization rate and load prediction of virtual machines. Application service monitoring mainly includes Mysql, Redis, Apache, and Nigix service monitoring alarm service, which is mainly divided into alarm configuration and alarm history view. The alarm configuration can support the customized alarm strategy, which will generate alarm when the condition is met according to the alarm strategy established by the system administrator. At the same time, when the alarm is triggered, the system manager will be notified in the form of messages. Previous alerts can be viewed
in the alert history, and the alert history can be migrated.

Fig. 5. Function module diagram of cloud platform monitoring system

5.4. *Raising awareness of client security protection*

Under the background of cloud computing, it is necessary to improve the security awareness of users. First, the personal identity authentication, real-name authentication and short message authentication of users can effectively avoid the intrusion of unidentified persons, criminals and hackers, which can realize the strict supervision of unauthorized users, and effectively realize the centralized control of negative effects. Second, users should learn to have basic network security knowledge and good computer operation habits, and avoid setting up data information and corresponding storage passwords on public computers. It is necessary to carry out security physical examination on the computer regularly, sweep and kill viruses, repair loopholes and install patches to prevent the illegal intrusion of the client. Enterprise users should make special security guarantee measures according to their own characteristics. For example, enterprises that provide services for cloud platforms can effectively improve the protection level of computer systems by means of filtering and prevention. Common used ways, such as using open source encryption software TrueCrypt to encrypt the disk, using RSA and DES to encrypt user information, adding Websense to intercept malicious code, using Vontu to protect confidential software, and using Vericept tool to monitor the data and information transfer in the individual user's computer, can discover security hidden danger in time, filter and intercept malicious information, and ensure the security of data information.
6. Summary
With the continuous progress of science and technology, people have officially entered the information age, and the use of cloud computing technology has also promoted the progress of China, which not only provides convenience for people's daily life, but also changes people's life styles. However, there are many security problems in the process of cloud computing. The computer network under cloud computing environment is more open, and it is more vulnerable to illegal attacks and data theft, which threatens the information security of computer network users. In view of this situation, it is necessary to actively adopt corresponding network security technologies, such as encryption technology, access control technology, and network monitoring technology, so as to effectively guard against computer network risks.

References
[1] Wu, H., Ding, Y., Winer, C., & Yao, L. (2010, November). Network security for virtual machine in cloud computing. In 5th International conference on computer sciences and convergence information technology (pp. 18-21). IEEE.
[2] Lee, B. H., Dewi, E. K., & Wajdi, M. F. (2018, April). Data security in cloud computing using AES under HEROKU cloud. In 2018 27th Wireless and Optical Communication Conference (WOCC) (pp. 1-5). IEEE.
[3] Chen, Z., Han, F., Cao, J., Jiang, X., & Chen, S. (2013). Cloud computing-based forensic analysis for collaborative network security management system. Tsinghua science and technology, 18(1), 40-50.
[4] Elzamly, A., Hussin, B., Abu-Naser, S. S., Shibutani, T., & Doheir, M. (2017). Predicting critical cloud computing security issues using Artificial Neural Network (ANNs) algorithms in banking organizations.
[5] Hu, Z., Gnatyuk, S., Koval, O., Gnatyuk, V., & Bondarovets, S. (2017). Anomaly detection system in secure cloud computing environment. International Journal of Computer Network and Information Security, 9(4), 10.
[6] Yang, C. (2019). Anomaly network traffic detection algorithm based on information entropy measurement under the cloud computing environment. Cluster Computing, 22(4), 8309-8317.
[7] Esposito, C., Castiglione, A., Pop, F., & Choo, K. K. R. (2017). Challenges of connecting edge and cloud computing: A security and forensic perspective. IEEE Cloud Computing, 4(2), 13-17.
[8] Yan, W., Wang, S., & Wang, C. (2019, November). The realization of network security technology based on cloud computing environment. In Journal of Physics: Conference Series (Vol. 1345, No. 5, p. 052022). IOP Publishing.
[9] Birje, M. N., Challagidad, P. S., Goudar, R. H., & Tapale, M. T. (2017). Cloud computing review: concepts, technology, challenges and security. International Journal of Cloud Computing, 6(1), 32-57.