Research on the Security Strategy of Computer Network in Cloud Computing Environment

Zhuohua Liu, Caijuan Huang*

Guangdong Mechanical & Electrical Polytechnic, Guangzhou, China, 510515, China

*Corresponding author

Keywords: cloud computing, computer network, security strategy

Abstract: With the development and application of Internet, many information technologies have been recognized and applied to various industries, including cloud computing. However, in cloud computing environment, the security of computer network becomes more and more important. At present, lots of computer networks have been attacked, which makes people’s privacy security under certain threat. In order to solve this problem, this paper introduces the definition of cloud computing, describes frequent network attack methods, and puts forward a relatively stable and effective security strategy for computer network security in cloud computing environment.

1. Introduction

In the course of the development of Internet, computer network is covered by a lot of data information. With a strong computing ability, cloud computing can make rational use of data information and scientific analysis. With the development of Internet, cloud computing rises. The data of cloud computing will bring convenience to people’s life and promote the development of industry. However, in cloud computing environment, there are a series of security problems in computer network, which have caused serious impact on the security and service of computer network, or even have brought a lot of unnecessary losses to users.

2. Introduction of Cloud Computing

Cloud computing is a new type of computing mode, which will provide computer with corresponding assistance according to the actual needs. In addition, it can share resources with other devices, and its storage, processing functions and related technologies bring great convenience for people’s lives [1]. Cloud computing has many advantages. For example, as the center to storage network data information, cloud computing has a strong reliability and high-level security. Besides, cloud computing is very convenient to use, through which, people are able to get needed information resources more quickly and freely. It also can realize resource sharing, and provide a shared platform for information data of a wide range of devices. Cloud computing has the advantages of openness, by which, people are no longer limited by time and space to get needed information. In cloud computing environment, the security of related information of hardware and software will be ensured correspondingly, which can effectively prevent data information from being stolen and tampered with. However, with strong openness, the security of computer network is affected accordingly, including the weakening of security protection ability of information. Therefore, it is important to make a stable and effective computer network security policy [2].

In addition, cloud computing technology is also very economical and practical. The application programs of computer network are run based on the “cloud” platform. While cloud computing also helps to greatly reduce the cost, as well as strengthens the performance of computers, thereby reducing the cost of software maintenance. Moreover, cloud computing has great storage space and very strong computing power, which are conducive to share and take advantage of various resources among devices [3].

DOI: 10.25236/dpaic.2018.041

3. Common Attack Means of Computer Network

Due to problems of system itself and the carelessness of network administrator, there are frequent vulnerability in network system. Once a vulnerability is present, some network hackers will take a series of attacks against it, and enter into the system, or probe the associated password, resulting in the loss of computer network information data. In order to strengthen computer security and prevent computer network system from being vulnerable to malicious attack, network administrators need to pay extra attention to this problem, so that network vulnerability can be filled in time and effectively, and then vulnerability can be repaired.

Backdoor software is to steal users' information and control users' computers. There are user side and server side. If the user' computer has a server-side, the user will log in when the hacker attacks network. Besides, program of server side is very small, most of which are attached to other software for installation. Some users can easily download and install backdoor software in the process of downloading other software. Since backdoor software has a strong rebirth capability, they are not easily cleared by users [4].

The hacker always synchronizes some aggressive data packets to the network server by means of corresponding means and cause the server to be paralyzed, so that the other service requests cannot be processed correspondingly, and the user cannot log in on the website. To avoid a denial of service attack, users need to install appropriate firewall program in the network server.

E-mail attack, also known as a mail bomb attack, if a lawbreaker uses the mail bomb software, will send a large amount of mail to mailbox to cover mailbox, consume system resources, and then cause system to be paralyzed. To effectively protect this type of attack, the user needs to install and clear the garbage mailbox software in the computer network.

4. Analysis of the Security Strategy of Computer Network in Cloud Computing Environment

In cloud computing environment, computer network also suffers a series of security problems, which influences users' application of computer network, and seriously threats the safety of life and property of users. According to the characteristics of cloud computing, the environment of computer network becomes more complex, users of computer network are gradually increasing, and network information data also become complex and diverse. In the process of storing data information, conventional fixed communication devices are not used. In addition, the user does not have enough network information identification capability, which also has a certain influence on network security detection. Secondly, computer itself has the virtual characteristic. In the process of data acquisition by the user, connection interruption can be easily generated once the technical operation is in error, which can prevent further processing of the data. Meanwhile, the openness of computers makes computer network more vulnerable to virus intrusion, and further influence or threaten the network security.

The security protection is directly related to the use of computer network. If computer network lacks corresponding security protection, network information data will be easily lost. In cloud computing environment, there are still not enough security protection system in computer network, while the security system is not strict enough. Once the hacker attacks, it cannot reach effective protection effect, or even network does not work or easily leak or lost data.

In cloud computing environment, there are some problems existing in users' authentication technology which may easily cause to lose users' information. If there is a malicious attack on users, the phenomenon of illegal theft of information will also occur. In addition, information data is very important for computer network. The database of computer network plays a key role in deciding whether the information data is safe or not. The network data information is scanned through security service terminal of network, thus constituting the security mode of computer network database. Once virus or abnormal situation appears in the network, the database will directly interrupt the connection with users, so as to achieve the protection of database. However, with the rapid development of cloud computing, the number of users is increasing gradually. If users do not attach importance to the use of cloud computing and network security, network databases are extremely vulnerable to attack, and the security of information and data will also be threatened.

5. Application of Security Protection Technology of Network in Cloud Computing Environment

Vulnerability scanning technology refers to detect the security of local computer system. In order to improve the security of computer network effectively, it is necessary to work closely with intrusion detection systems and firewalls. Vulnerability scanning technology is to scan network, so that network managers are able to discover hidden security danger in the network in time, and then repair the vulnerability of computer network.

The so-called firewall technology is a kind of network connection equipment which strictly monitors the access of Internet so as to prevent other users or even hackers from intruding into network and then to strengthen the protection of internal Internet. In order to ensure the security of network, all kinds of information in network need to be filtered and filtered, and Internet is carefully controlled through the firewall. In addition, firewall has a strong anti-attack ability, so the reasonable use of firewall technology can effectively prevent hackers from malicious intrusion into the network system, thus adding a layer of protection for the privacy of users and the security of information data.

Virus protection technology means that once virus invades computer network system, it is necessary to use the defense technology to judge invading virus in time and reasonably, and then to intercept virus effectively. At present, single machine anti-virus and internet anti-virus are effective computer virus protection measures. Single machine antivirus refers to the scanning and removing of a computer virus. Internet antivirus means the protection of a virus through network. If a virus is found in network, it will be accurately detected and cleared by network antivirus, so as to ensure the security of computer network.

Network access control technology is not allowed to control users' access, and also an authority to limit users' access. This technology is the most effective method to protect computer network security.

There are many methods to protect the security of computer network system, among which, authorization and encryption access technology are similar to firewall technology. They encrypt the information data of network and authorize users' access authority of computer network and so on. Authorization as well as encryption access technology are quite fast, simple, and relatively easy to control, which has an extremely effective role in open computer networks.

In the process of computer security protection, firewall is the most stable and effective method. However, with the rapid development of network technology, computer viruses and a series of malicious intrusion means are also increasing. In order to solve this problem, Firewall and other procedures should also be updated and improved in real time. Users can add firewall program in application, which is beneficial to the protection of network security. In addition, cloud computing is actually a virtual storage of network resources and abstract computing of network computing patterns. The following diagram shows the structure of computer network security prediction in cloud computing environment.

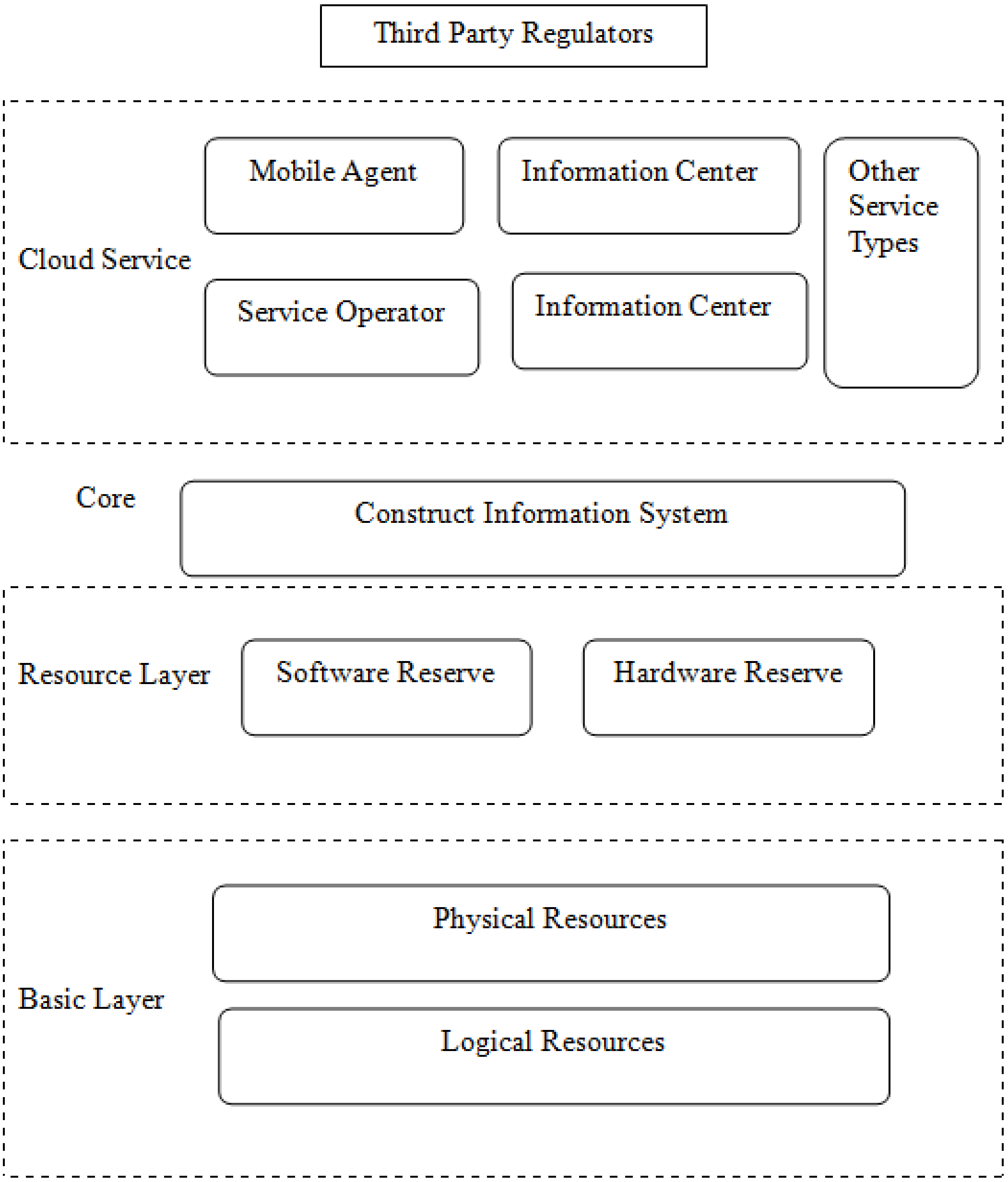

Fig.1 Structure of computer network security prediction in cloud computing environment.

It can be found that network information resources can exchange and process information data through switchboard. In cloud computing environment, the virus data of m terminals are:

$$x(k)=\left[x_1(k),x_2(k),\ldots x_m(k)\right],m=1,2,\ldots,n.$$

K in the formula represents the infection channel of virus. If the infected virus data in the computer network is a random variable, then information can be combined to form a function:

$$\Phi\left(w_1,w_1,\cdots,w_n\right)=E\left[\exp(x_1w_1,x_2w_2,\ldots x_nw_n)\right]$$

W in the function represents the feature of information. E represents information energy. In addition, the frequency and amplitude of computer network security prediction mode in cloud computing environment are as follows:

$$\mu_k=E\left[\left(x-\eta\right)^k\right]=\left(x-\eta\right)^k f\left(x\right)dx$$

$$m_k=E\left[x^k\right]=x^k f\left(x\right)dx$$

According to the Fourier transform correlation operation, the vector of virus data is obtained as follows:

$$\theta_1(k+1) = \theta_1(k) - \mu_k E\left[y\left(k\right) \Phi\left(w_1, w_1, \cdots, w_k\right)\right]$$

If there are m virus data in cloud computing environment, it will bring a certain threat to the security of computer network, and it is necessary to predict the network security in real time.

6. Conclusion

In cloud computing environment, it is very important to maintain the security of computer network. With the development of social economy and science and technology, computer network has been widely promoted and applied in our country. Nowadays, computer network plays a key role in all kinds of industries, and it also brings great challenges to computer network security protection. Therefore, for those factors that pose a threat to the internal computer network. we need to detect them in a timely manner and systematically analyze the security risks that exist in computer network. Furthermore, security protection methods of computer network are optimized and adjusted. Moreover, it is necessary to combine scientific and reasonable protection technology of network security to further create a healthier cloud computing environment for people.

References

[1] Zhe Mingwei. Research on Computer Network Security Strategy in Cloud Computing Environment [J]. *Modern Information Technology*, 2018 2 (4): 146-148. [2] Na Yong. Research on Computer Network Security Strategy in Cloud Computing Environment [J]. *Electronic Production*, 2014, (10): 149-150.

[3] Wang Jialan. Research on Computer Network Security Strategy in Cloud Computing Environment [J]. *Journal of Heihe University*, 2017 (12): 219-220.

[4] Rong Chunyang. Analysis of Computer Network Security Strategy in Cloud Computing Environment [J]. *Technology Wind*, 2017, (14): 86.