Computer Network Security and Effective Measures for the Era of Big Data

Changliang Zheng(✉)

Beijing Polytechnic, Beijing 100176, China

Abstract. The era of big data has come. At present, the application of big data is more and more, which has a certain impact on people's life. With the use of big data, computer network security problems also appear. This problem is not conducive to development, so it is urgent to find out preventive measures to solve this problem. Therefore, this paper focuses on the analysis of computer network security problems, and studies the effective measures to prevent computer network security problems.

Keywords: Computer network · Research on preventive measures · Big data · Network security

1 Introduction

The advent of the era of big data has brought great convenience to mankind, and it is also the inevitable trend of the development of modern science and technology. In such a background, the computer network has developed rapidly, and there are still some problems to be solved in the process of development. If we can solve the problem of computer network security, the development of computer network will move forward.

Network security, usually refers to the security of computer network, in fact, it can also refer to the security of computer communication network. Computer communication network is a system that connects several computers with independent functions through communication equipment and transmission media, and realizes information transmission and exchange between computers with the support of communication software. Computer network is a system that uses communication means to connect several independent computer systems, terminal devices and data devices which are relatively scattered in the region for the purpose of sharing resources, and exchange data under the control of protocol. The fundamental purpose of computer network lies in resource sharing, and communication network is the way to realize network resource sharing. Therefore, computer network is safe, and corresponding computer communication network must also be safe. It should be able to realize information exchange and resource sharing for network users. Below, network security refers to both computer network security and computer communication network security.

The basic meaning of security: objectively there is no threat, subjectively there is no fear. That is, the object does not worry about its normal state being affected. Network

security can be defined as: a network system is free from any threat and infringement, and can normally realize the function of resource sharing. In order to make the network realize the function of resource sharing, the hardware and software of the network should run normally, and then the security of data and information exchange should be guaranteed. As can be seen from the previous two sections, the abuse of resource sharing leads to network security problems. Therefore, the technical way of network security is to implement limited sharing, its structure is shown in Fig. 1.
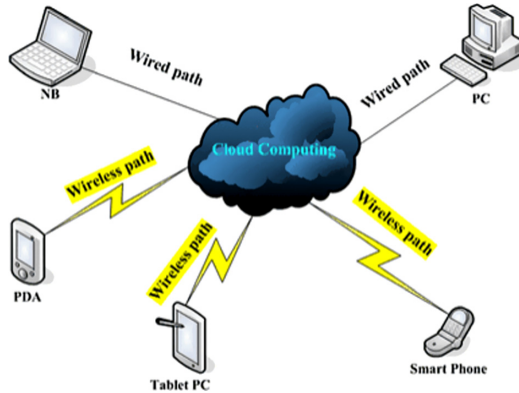

Fig. 1. Network security structure

2   Computer Network Security in the Era of Big Data

2.1   There Are Loopholes in Computer Network System

Most of the enterprise computers use Windows system, the utilization rate of windows system is very high, but there are some problems in the system. Whether it is the invention and update of windows system or the process of downloading windows system, there are some bugs, which will bring security risks to the computer network. In order to solve these bugs, the designers of windows system will constantly upgrade and maintain them, and timely launch new systems to solve these bugs. Nevertheless, there are still some loopholes in the new windows system that need to be solved [1–3]. Therefore, if we want to develop windows without any loopholes, it cannot be realized at present. We can only improve the windows system in the process of continuous attempt and development. In addition to Windows system vulnerabilities, there are many other system vulnerabilities. In the long run, these vulnerabilities will affect the user's information security, and may lead to user data theft and other problems.

Maximum weight matching can be defined as:

$$\max -value = \max \left\{ \sum_{c_i \in R f_j \in S} w_{ij} \right\} \tag{1}$$

The description of matching similarity between services can be defined as:

$$\sin RS = \frac{\max -value}{R}, 0 < sin\ RS \leq 1 \tag{2}$$

2.2 Safety Problems Caused by Improper Human Operation

Some improper actions of users in the process of using computer will cause safety accidents. First of all, there may be problems in the user's operation technology, some unintentional actions will bring security risks to the computer network, such as the user has no intention to close the firewall or computer information and data security protection function; secondly, there are many users deliberately attacking the computer network, enterprises should pay attention to this phenomenon, and allow such staff to be dismissed.

With the development of computer technology, most enterprises have installed computers, but the technical level of computer operators is still in the primary stage. These operators can only operate some simple operations, and they are not proficient in some basic software of the computer, so there are often phenomena such as improper human operation causing security problems [4]. In addition, some intentional people attack the computer network and steal the important data in the computer network.

2.3 Network Virus Infection

Users often watch the network virus when they operate the computer. The emergence of the network and work with convenience, many enterprises through the founder of the website to obtain profits, attracted a large number of users to register information. For example, the user base of Taobao Mall and other websites is large, and these users will pay for online shopping, so they must bind their own silver speed hackers to specially develop some kind of sick users' computers infected with these viruses. If they have been infected with network viruses, it is difficult to completely eliminate them [5–7]. In addition to the threat to the user's property security, the computer infected with network virus also affects the computer's protection system and hardware equipment, thus reducing the life of the computer.

3   Effective Preventive Measures for Computer Network Security Problems in the Era of Big Data

3.1 Application Firewall

With the advent of the era of big data, there are more and more kinds of viruses, and the number is also increasing. If we do not prevent and control viruses, it will affect the security of computer networks. At present, the best way to deal with viruses is to use firewalls. The function of firewall is to filter the data in the computer network, it will not affect the normal transmission of computer network information data, will leave safe information data, for the malicious virus processing, these viruses and some

junk information block out. So the installation of firewall in the computer can provide security for the computer network. In addition, the firewall function can also effectively distinguish the company and personal information, and process the relevant information separately, so both enterprises and individuals can use the technology safely. In addition, the firewall has been monitoring the data in the computer network to review the internal and external of the system. Firewall can block the virus invasion in time to ensure the security of computer network.

3.2 Application Safety Monitoring System

In order to ensure network security, users can set up security monitoring system in the computer. The system can detect the operation status of the computer system at all times, and ensure the user to use the computer safely [8–10]. At present, there are many security monitoring systems, including 360, computer security manager and so on. These safety monitoring systems are free of charge, and have many internal functions, including virus detection, comprehensive physical examination, garbage cleaning and other functions. In addition, there are some charging security monitoring systems with higher security performance. In order to avoid the internal important data being stolen, it is necessary to pay to use these security monitoring systems. After using the security monitoring system, the security of computer network will be greatly improved, providing users with a more healthy and safe network environment.

3.3 Using Antivirus Software

The emergence of virus directly threatens the security of computer network, and virus is also one of the biggest problems affecting the security of computer network. Now the network virus is more and more powerful, more and more kinds, such as Trojans, worms and other viruses seriously threaten the user's computer data security. In order to avoid computer being invaded by virus, enterprises and individuals can install anti-virus software in the computer. Anti virus software can help users find and remove viruses. Now there are many anti-virus software in the computer market, some anti-virus software specifically for a virus, some anti-virus software can kill common viruses. Now most of the anti-virus software functions are more and more complete, which can basically meet the needs of users [11]. At present, the more commonly used anti-virus software are computer security manager, Jinshan drug bully and so on. Enterprises and individuals can install some anti-virus software according to their own needs, and set relevant settings in the software, such as setting automatic detection of virus or killing virus, etc. All in all, the use of antivirus software can help users deal with the computer virus, so that users in a safe state of the Internet.

3.4 Ensure the Security of Information Storage and Transmission

After enterprises use big data, the network is transmitting data and information all the time. For enterprises, some data is very important and must not be lost. Therefore, in order to avoid data loss or theft, the security of information transmission and storage

should be guaranteed. There are many ways to deal with this problem. The most common way is to use encryption technology to encrypt the transmitted data, so that the data can be more safely transmitted to the other party's computer. After receiving the data, the other party needs to decrypt the data information, and only the two parties know the key. Taking this way to transport the data information improves the security of transmission [12]. The lawless person can't crack the key of data transmission in a short time. In addition to ensuring the security of information transmission, but also to protect the security of information storage, so the enterprise can also encrypt the important data inside the computer, to avoid intentional intrusion into the computer to steal data. In fact, enterprises can employ excellent computer talents to deal with the problems of computer network security.

4 Simulation Analysis of the Importance of Solving Computer Network Security Problems in the Era of Big Data

Let's first understand the meaning of big data. From the three words of big data, big data refers to a large amount of data. At present, big data is characterized by diversification and transmission through computer network technology. Compared with the previous local network transmission mode, this kind of transmission mode is faster and more convenient, and the data processing speed is faster. At present, the era of big data has arrived, and has promoted the development of computer network technology. According to understanding, most enterprises in China are currently applying big data, such as Jingdong tiktok, Taobao, jitter and so on, all of which have used big data [13–15]. The application of big data solves the core problems of enterprise development, changes the survival mode of enterprises, and promotes the development of enterprises.

There are many methods of data information transmission, and the media used are extremely complex. Therefore, there are some problems in the current network data dissemination. The biggest problem is the security problem. The security factors are mainly divided into: first, it may be caused by human activities; second, with the development of big data, the requirements for computer network technology are higher and higher, But the development speed of computer network can not keep up with the pace of the times. Finally, because of the openness of the network, many viruses invade the network, causing network security accidents (see Fig. 2 and Fig. 3).

In this case, we must take some measures to prevent and solve the problem of computer network security. Only when the problem of computer network security is solved, can it be more conducive to the development of national enterprises and promote the development of national economy [16]. So it is very important to solve the problem of network security.
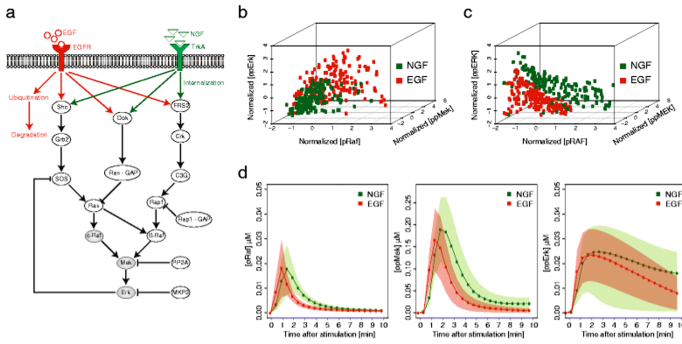
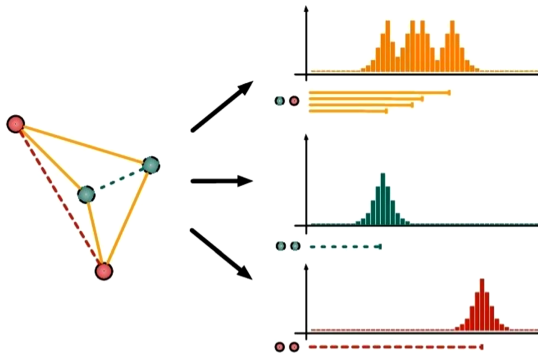**Fig. 2.** Network security with big data

Fig. 3. Attack frequency and effectiveness

5   Effective Response to Computer Network Security Problems Under the New Normal

Under the new normal, in order to effectively deal with the security threats of computer network, ensure the security of computer network, create convenience for users to better use computer network, and prevent unnecessary attacks, the following effective countermeasures can be taken.

5.1   Application of Network Intrusion Detection Technology to Effectively Prevent Hacker Attacks

Using network intrusion detection technology, we can find and eliminate the hidden security in time, and the computer network is safe and reliable. Intrusion detection can also improve the foresight of security management, prevent and control security problems in advance, and take technical measures to intercept and block security risks in time for suspicious activities, which is conducive to the security operation of computer network [17]. The management personnel should find the security problems existing in the network in time, and take measures to calculate and manage the network. "Rukou"

attaches great importance to the daily tracing of computer tears leakage, and timely repair when double leakage occurs. As shown in Fig. 4. Add computer system management and daily push. To ensure the safety of software and hardware of jizhunge, we will ensure the safety and effectiveness of delivery limit setting, user setting and code setting, and timely access and recovery of safe delivery. Focus on the sweeping measures of the database, update and upgrade the pushed data laws, improve the security performance of the database, effectively ensure that the user's right of assistance, user settings, secret penalties and orders meet the requirements of the Taiwan security specification, and perform the patch according to the requirements to effectively ensure the network security of the gambling computing machine.
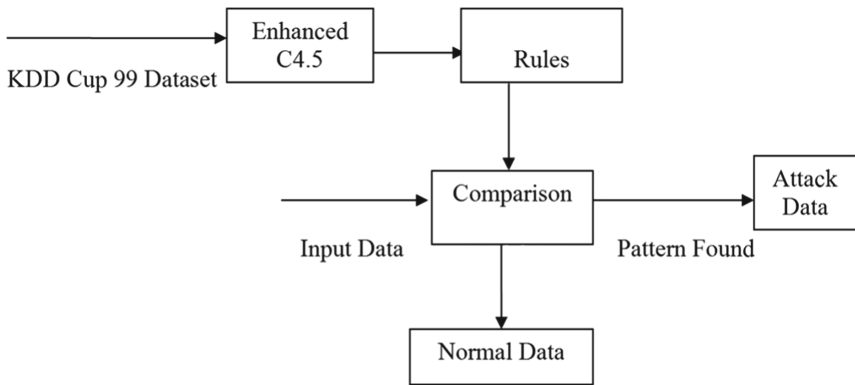

Fig. 4. Application of network intrusion

5.2 Strengthen the Network Security Management, Effectively Guarantee the Computer Network Security

Managers should understand the importance of computer network security management, and make comprehensive use of management rules and regulations, technical measures, etc. to do a good job of security. On the one hand, they should pay attention to computer network information encryption, avoid data loss or be improved. There are two methods of network security management: water code and public key code, which have different characteristics and should be reasonably selected according to the needs of security management. Conventional cipher means that both the sender and the receiver use the same key, which effectively guarantees the information security, has strong confidentiality, and can withstand the test of time [18]. When conveying information, it must be delivered in a secure way to avoid password leakage. Public key cryptography is quite different, and it is difficult to derive the decryption key in the application process. Simple management, meet the requirements of network development, can achieve digital visa and character verification, has strong confidentiality, can make the information transfer and delivery. But its algorithm is complex and not easy to use, which restricts its promotion and application. In order to improve the level of computer network security management,

we can combine the two, which is conducive to enhancing the level of computer network security management. On the other hand, improve the computer network security management rules and regulations 61. Establish a strict responsibility system, clear the responsibilities and authority of relevant personnel [19–24]. To effectively guarantee the computer network security, we should formulate the network security use system, formulate the access management system, and establish the network security maintenance and emergency response system.

5.3   Reasonable Application of Encryption Technology to Ensure the Security of Network Information Resources

There are many sources of computer network security risks, not only including websites, hacker attacks, Trojans and so on, but also from the internal database of the network [25]. For example, criminals illegally steal user accounts and passwords, use the database beyond their authority, arbitrarily and steal the information resources of the database. In order to make up for this deficiency, ensure database security, and create conditions for people to make rational use of computer network information resources, it is necessary to adopt encryption technology in management. The specific method is to set the password properly according to the needs of database and computer network resources. Users can access the corresponding database and obtain the required information only by virtue of the password and after passing the system kernel. In order to avoid unauthorized access, illegal intrusion, fundamentally prevent the occurrence of data change phenomenon, ensure the security of computer network [26]. Pay attention to the backup and recovery of teaching data to ensure the integrity of data. In order to prevent malicious invasion, data loss and other problems, computer network management should pay attention to the backup of data. Staff should fully understand the importance of data, make rational use of micro cloud, hard disk and other tools to backup and store important data, and take it as a habit, Protect important data [27]. Through data backup, even if there are security problems in the computer network, it can also restore the data in a short time, ensure the integrity of the data, and provide convenience for the use of information.

6   Conclusions

At present, the era of big data has come, people's lives have undergone tremendous changes, computer network technology has brought convenience to personal life and work, at the same time, computer network security issues threaten people's security. Therefore, enterprises and individuals should pay attention to the problem of computer network security. This paper is divided into three parts, respectively, for everyone to analyze the importance of computer network technology in the era of big data, computer network security problems and effective preventive measures.

References

1. Huang, G.: Analysis of computer network security risks and preventive measures. Popular Sci. Technol. **18**(12), 4-5+23 (2016)

2. Xinyue, H.: On computer network security technology. Heilongjiang Sci. **7**(22), 44–45 (2016)
3. Yuanbo, T.: Discussion on computer network information and network security and its protection strategy. Electron. Technol. Softw. Eng. **18**, 234 (2016)
4. Xiang, S.: Analysis of computer network application security. Mod. Econ. Inf. **21**, 360 (2015)
5. Huang, B.: Computer network information security and protection measures. Ind. Des. **09**, 179+185 (2015)
6. Juxi, X.: Research based on computer network security. Exam. Wkly **58**, 120 (2015)
7. Song, F.: Research on computer network security and firewall technology. Enterp. Guide **12**, 146+148 (2015)
8. Jun, Z.: discussion on internal computer network security maintenance. Inf. Comput. **10**, 84–85 (2015)
9. Li, Y.: Computer communication network security and protection countermeasures. Digit. Technol. Appl. **04**, 177 (2015)
10. Wei, W.: Research on computer network security problems and effective preventive measures. Comput. CD Softw. Appl. **18**(02), 164–165 (2015)
11. Xinyu, H.: Research on computer network security. Wireless Internet Technol. **12**, 62 (2014)
12. Wenjie, L.: Brief analysis of factors affecting computer network security and preventive measures. Comput. CD Softw. Appl. **17**(21), 194–195 (2014)
13. Xu, T.: Computer network information security analysis in civil aviation air traffic control. Silicon Valley **7**(20), 206+198 (2014)
14. Sun, M., Sun, P.: On the main hidden dangers and avoidance measures of computer network security. Inf. Technol. Inf. **09**, 189–190 (2014)
15. Guoyun, S., Wei, Z., Ping, D., Yuanlong, Z.: Effective improvement of computer network security and preventive measures. Comput. Knowl. Technol. **10**(04), 721–723 (2014)
16. Lin, L.: on preventive measures of computer network security. Electron. Technol. Softw. Eng. **23**, 243 (2013)
17. Xueqing, B.: Effective measures to improve the security of WLAN. Comput. Netw. **39**(22), 55–57 (2013)
18. Fengyan, S., Shimin, X.: Explore the threat and prevention of computer network security. Comput. Knowl. Technol. **9**(31), 6975–6977 (2013)
19. Meng, Z.: Analysis of computer information network security management construction. Wireless Internet Technol. **06**, 20 (2013)
20. Jianwu, N.: Effective measures of computer network security maintenance and management. China New Commun. **15**(08), 18 (2013)
21. Jun, H.: current situation of computer security prevention and control. Inf. Comput. **06**, 82–83 (2013)
22. Chuan, J.: On computer network security and prevention. Dig. Technol. Appl. **01**, 164 (2013)
23. Peng, L.: Discussion on computer network security and preventive measures. Silicon Valley **5**(01), 143+155 (2013)
24. Liu, Y.: Internet network database security management measures. Comput. CD Softw. Appl. **16**(01), 92+97 (2013)
25. Hailing, S.: Computer network security risks and effective maintenance measures analysis. Inf. Comput. **18**, 6–7 (2012)
26. Bokai, H., Ling, L.: On the harm and Countermeasures of computer network attack. Manag. Technol. Small Medium-Sized Enterp. **10**, 222 (2011)
27. Yongjian, D.: Analysis of preventive measures for computer network risks. Inf. Comput. **16**, 49–50 (2011)