Research on Computer Network Security Prevention in the Era of Big Data

Bocheng Ouyang¹*, Yinsheng Cui¹
¹Guiyang University, China, 550005

*Corresponding author e-mail: Oybe999@163.com

Abstract. In view of the special status and influence of computer network in big data era, this paper points out and analyzes the traditional and new problems and loopholes faced by network security in the new era. Finally, from the consideration of many levels, the countermeasures of preventive measures are given.

Keywords: Big Data, Computer, Network Security

1. Introduction
With the development and popularization of computer technology in China, computer technology under big data can bring benefits to people to a great extent, but what cannot be ignored is that there is a lot of privacy in the massive data information. Therefore, we should take computer network security management as the key content, and put forward network security precautions in time. Because there are some loopholes in the management of big data era, it has a lot of influence on life and development [1]. If we don't pay attention to it, it will probably affect people's life and information, account security. Therefore, it is necessary to arouse attention and strengthen the research in this field, which is worthy of further discussion.

2. Characteristics of network data in big data age

2.1. Resource data
Enterprises need to use big data technology to formulate sustainable development plans, and the development of various fields of society also involves the use of data resources. Only by mastering accurate data resources can enterprises gain insight into the development direction of enterprises and improve their competitiveness in the market economy.

2.2. Big data blends with other computer technologies
In big data technology, other computer technology, as the platform of big data generation, is also very important, all of which need to play a greater role in the integration with big data. All the data
information can be shared on the platform, and the data information of the enterprise will be synchronized in the internal platform of the enterprise to provide data support for the development of various fields of society.

2.3. Network data is easily leaked
At present, the main factor affecting the development of big data technology is information leakage. In recent years, the data leakage incident has also appeared the phenomenon of expansion, which information data preservation means, how to improve the efficiency of supervision, people need to take timely action, starting from the root, at the beginning of the big data to formulate relevant management measures, evolution control, as far as possible to reduce the risk of data leakage.

2.4. Strong computing power
The computer network created by using big data technology has the characteristics of wide range, large scale and strong computing ability, which meets the data needs of different people. The relevant data information obtained by the computer network is stored in the cloud, and the cloud computing center is used to connect with all user terminals, so that people can connect with the cloud computing center to form a large number of terminal equipment systems when using big data services [2]. A large number of data calculations are carried out. Virtualization is a major feature of information technology. This design also reduces the running cost of computer network for cloud computing services. Customers only need to buy computer network hardware to get a lot of data information.

2.5. Data sharing
How to better realize data sharing, using big data center for cloud storage is very effective. After authorization, users can use all terminal devices connected to cloud data center and enjoy the corresponding data. If the original data loss, damage and other problems, storage cloud data can still provide services to users. Compared with the traditional storage mode, the information storage of big data is very different. The traditional data sharing depends on physical connection, needs to use physical equipment to transmit and share data information, and there are problems such as slow data transmission, easy leakage and even network virus invasion, which leads to low application efficiency and network security.

3. Hidden dangers of computer network security in big data era
New scientific and technological means emerge in endlessly for the benefit of society, but also used by some lawbreakers to create network security risks [3]. Figure 1 shows the distribution of social perception of network security in the new big data era.
3.1. Safety awareness of internet users
Illegal elements cannot take advantage of the theft of Internet users' personal information. When the network sets the website password, do not set too simple, should use the combination of numbers, letters, symbols to set the password, so as to improve the safety factor of the password [4]. In addition, internet users should not set the password of multiple websites to the same for the convenience of memory, so that illegal elements may steal many kinds of news, thus causing certain losses to internet users.

3.2. Vulnerabilities in network systems
There are loopholes in the network system itself, so the computer may pop up the dialog box of updating the system in the process of using, which is that the manufacturer has introduced the updated system to make up for some loopholes in the original system. Therefore, when internet users see this message, they should update the computer system in time. Some personal operational reasons will also cause loopholes in the system, such as downloading some pirated software, browsing pirated websites, resulting in virus intrusion, causing a huge impact on the system.

3.3. Threats from hacking into computers
Hacker attack is to steal information and tamper with information without any response from computer security system. Often, hackers will attack some computers with important information files [5]. He can use big data to cover up his behavior, making it invisible and unfounded. Generally speaking, if hackers invade computers, it will bring huge losses to enterprises.

3.4. Virus invasion of computer hazards
In the era of big data, computer network technology has been developed at a high speed, and virus programs have also been improved. Because the network is full of all kinds of information, some pirated websites may hide a large number of viruses, and the way computers infect the virus has become diversified, and the harm of the virus is increasing [6].

3.5. Computer software has its own flaws
Nowadays, computer software is endless, but some software has not been fully designed and mature to
be put into the market for use, which is very easy to give lawbreakers the opportunity to find loopholes and steal the basic information of users. In addition, some software designed to ask friends to help bargain for cash, these links are particularly easy to be found by lawbreakers to find loopholes, thereby stealing a large number of customers' names and mobile phone numbers, and then these illegal businesses will sell personal information, obtain high profits [7].

3.6. The appearance of malicious websites
With the rapid development of random Internet, a large number of websites have emerged, including some pirated websites. These sites contain a variety of viruses, publishing deceptive messages. Once the internet users carries on the registration, will have the possibility to divulge the telephone number, the ID card number, more likely will divulge the user's bank card password, is very unfavorable to the user's property security.

4. The countermeasure of computer network security in big data age
To cope with the current problem of computer network security management, we must combine the development of network to formulate relevant network management countermeasures. As to do well in computer network security prevention countermeasures, we must guard against it from inside to outside, improve the network security management consciousness of computer managers, and strengthen the network supervision and management work. Figure 2 shows the classification of network security precautions.

![Classification of network security precautions](image)

**Figure 2.** Classification of network security precautions

4.1. Equipment control management should be strengthened
At present, people's way of Internet access has quietly changed a lot, no longer rely on broadband access to the Internet, but through the use of wireless networks. This also makes people online entertainment and offices become more convenient, enjoy the joy of wireless Internet. But wireless network brings people convenience, but also brings a lot of threats. For example, hackers can use
wireless networks to invade computer users’ computers, systems and information databases. So, we are supposed to strengthen the control and management of equipment and solve many problems existing in computer management, such as limiting wireless network matching, strengthening supervision, fully ensuring the security of equipment, and minimizing access to unfamiliar wireless networks.

4.2. Storage of data using encryption
For some very important files or contents, encryption technology can be used to save and transfer. If you discuss some trade secrets, you can use cipher-text, so that criminals do not steal useful information and ensure the safe transmission of data. The encryption technology of file transmission can be optimized from one-way encryption to two-way encryption, which makes the transmission file more secure and reliable. Bidirectional encryption is like the need to enter a password when transferring a file and the receiver also needs to enter a password when accepting a file, so as to prevent the disclosure of the file in the process of transmission. In addition, the record is hidden or deleted immediately after receiving the document, which fully guarantees the confidentiality of the document.

4.3. Enhanced data storage and transmission security
Now, network technology is leader of various fields of society. Technicians are strengthening the security of data transmission by means of data information encryption, and use information data transmission encryption to form cipher-text. Because cipher-text is the unique identity of each data, even if the lawbreakers obtain the document information, there is no way to identify the cipher-text, so there is no way to intercept the data information. Between the transmitting data information, it is also necessary to encrypt calligraphy and painting, control network access rights, and prohibit confusion of access rights. In addition, visitors need to conduct resource audits after entering the website. Only through identity authentication can access, which can also prevent lawbreakers from stealing data information.

4.4. System vulnerability repair capacity strengthened
Through the above analysis, we know that there will be some loopholes in computer program software. To some extent, these vulnerabilities will lead to hacker attacks, increase the probability of computer intrusion, and easily lead to human theft of information data. In general, hackers can use the relevant Trojan horse to infect computer users. For example, when a computer user visits a certain kind of website, it may be poisoned accidentally, resulting in the computer being infected with the virus, endangering the computer information security, and even constituting a very serious threat. We need to speed up the repair work of computer vulnerabilities, repair computer programs and software in time, so as to truly reduce the existence of vulnerabilities and prevent them from being exploited to the maximum extent.

4.5. Increased network access control
This measure is mainly to reduce or prevent illegal elements from invading the network and prevent them from doing some harmful things. In general, computer network control means mainly include access to network, network authority control and attribute control. In network access, relevant personnel should find more suitable methods and accurately identify the functions of computer network. In addition, the data information should be identified and managed to determine a single interface, so that the application system and permission engine on the computer can be combined
together.

5. Conclusion
The computer application under the background of big data era not only needs to adjust the working mode, but also industrial operation mechanism according to the practical needs of people at the present stage. At this time, the requirements for computer security increase, and it is necessary to make rational use of preventive measures to enhance the application value of computers. Therefore, the property and information security of enterprises or individuals can be guaranteed, and the later computer security construction can also achieve the goal requirements.

Acknowledgments
This work was supported by Natural Science Research Funded Project by the Education Department of Guizhou Province: Qianjiao He KY [2013] 110 and Guizhou Provincial Department of Education Innovation Group Major Research Project: Qianjiao He KY [2018]027.

References
[1] Mo Hongai. Analysis of Computer Network Security and Preventive Measures in the Age of Data [J].Digital technology and applications,2019.
[2] Liu Runxi. Analysis of Computer Network Security and Preventive Measures in the Age of Data [J].Reading and Writing (Teachers),2019(6):0297-0297.
[3] Yi Wenjing. A Study on Computer Network Security Prevention in the Big Data Age [J].Computer knowledge and Technology 13(012):19-20.
[4] Wan Huan. On Computer Network Security and Effective Preventive Measures in Big Data Age [J].Computer products and Circulation,2019.
[5] Tian Yanxiao, Shi Qingsong. Discussion on Computer Network Security and Preventive Measures in the Age of Data [J].Computer programming skills and maintenance 2016(10):90-92,3 pages.
[6] Zhang Sen. Analysis on Computer Network Security and Preventive Measures in the Age of Data [J].Network Security Technology and applications,2018(1).
[7] Zeng Shenggen. Discussion on Computer Network Security and Preventive Measures in the Age of Data [J].China New Communications 19(022):91-92.