Hidden Dangers and Prevention Strategies of Network Security in Big Data Environment

Limin Liu

School of Computer Engineering, Guilin University of Electronic Technology, Beihai, 536000, Guangxi, China

Keywords: Big data; Network security; Hidden danger; Preventive strategies

Abstract: Computer has gradually become an indispensable auxiliary tool in public life. While computers provide convenience for public life, they also bring hidden dangers to public information security. The network can involve many aspects of content in the age of big data. If users do not have a deep understanding of the Internet, they are vulnerable to threats in information security in the process of applying the Internet. In the big data environment, as an important strategic tool in social enterprises and other real development fields, it aims to achieve objective analysis and classification of effective information in the database through rational analysis and decision judgment of service subjects. When someone inputs personal privacy information into the Internet, it is likely to be used by criminals. Therefore, users should be very careful when entering personal privacy on the Internet, to ensure the security of personal privacy and big data information, and to prevent personal privacy from being invaded by hackers, causing losses to individuals and society. Therefore, how to protect the public's computer network security in the big data environment has become a problem to be solved in this paper.

1. Introduction

Model construction and theoretical innovation in the era of big data have promoted the circulation and practical transformation of data streams. Under the background of the new era, new network technologies and data regulation technologies have influenced the market application and security protection functions of big data systems imperceptibly. Under any conditions, once the person who needs authorization activates the information in the right way, the required content can be obtained. Attackers such as network hackers can't refuse the use of the licensee because they invade the network, and the network system must be available without any influence [1]. Computers have gradually become an indispensable auxiliary tool in public life. While computers provide convenience for public life, they also remove hidden dangers for public information security. The network can involve many aspects in the era of big data. If users don't know enough about the Internet, they will easily be threatened by information security in the process of applying the Internet, such as online fraud and telecom fraud, all of which belong to network information security problems. The main reason is that criminals steal users' personal information. Organizations and individuals concerned should always help users to improve their awareness of data security [2]. When someone inputs personal privacy information into the Internet, it is likely to be used by criminals. Therefore, users should be extra careful when inputting personal privacy on the Internet to ensure the security of personal privacy and big data information, and prevent personal privacy from being hacked and causing losses to individuals and society [3]. The processing of computer data becomes extremely complicated, so it is necessary to constantly innovate the technology of computer data processing. In this era of big data, people pay special attention to the problem of network information security while enjoying the convenience it brings.

Under the big data environment, as an important strategic tool in the real development fields such as social enterprises, it aims to objectively analyze and classify the effective information in the database through rational analysis and decision-making of service subjects. This "centralized" information processing technology has effectively improved the practical income, business efficiency and comprehensive competitive strength of participating groups [4]. While the Internet

meets users' data requirements, the security pressure is increasing day by day. Therefore, only by solving the network security problems scientifically, effectively and quickly can users really enjoy the convenience brought by Internet technology in the era of big data. Therefore, how to protect the public's computer network security in the big data environment has become a problem to be solved, so it is of practical significance to analyze and study it.

2. Characteristics and main types of network security in big data environment

2.1. Characteristics of network security

With the arrival of the age of big data, the capacity of computer hard disk has made a qualitative leap. Today's network data is incomparable in terms of quantity and type, which also puts forward higher requirements for data processing speed and quality [5]. At the same time, the pressure of data security management is increasing day by day, and the network security situation is very serious. This paper analyzes the characteristics of network security, which can be divided into the following three characteristics:

① Strictness

Rigidity refers to the feature that network information cannot be changed without authorization, that is, network information is not affected by natural and human factors during storage, transmission or processing, and is not tampered with or lost. Therefore, before users use the data, they must first conduct security isolation on the privacy data, and clarify the use rights and access rights, so as to effectively protect personal privacy.

② Usability

Usability refers to the ability of individuals, teams and organizations to access and use network information when needed. In the network security environment, the denial of advocacy services, the destruction of network systems and other normal online behaviors are all attacks on usability. For big data and its carriers that are vulnerable to attacks, protection measures must be upgraded in time. Once data is lost or stolen, it will cause unpredictable economic losses.

③ Privacy

Privacy means that information cannot be transmitted to other users, entities or processes without authorization, and cannot be illegally used or planted with Trojan. That is to say, the content of network information cannot be understood and processed by unauthorized third parties. Therefore, whether from a technical or management perspective, it is urgent to strengthen data storage practices. In particular, it is increasingly difficult to detect potential threats to data, so we need to further deepen the construction of network carrier security.

Big data refers to the collection of massive information and materials with the help of computers, and then the processing and sorting of data with computer technology to form information conducive to the development of enterprises. Therefore, big data actually contains high value and can be widely used in politics, national defense, economy, society and other aspects. At present, it has played an important role in many industries and fields [6-7].

2.2. Hidden dangers of network security

With the continuous increase of data, it is particularly important to effectively collect, analyze, process and store all kinds of data in order to make it more valuable. When different people use computers, the operating system generally marks users with different permissions by establishing "accounts" for different authorized users [8]. Users who have passed the authentication of the administrator of the operating system during the login process will enjoy high access rights. The application of computer is more and more extensive, which not only brings great convenience to people's life, but also improves work efficiency. Most people can use computer technology, but on the whole, there are still many people who can't operate computers reasonably, don't realize the seriousness of network security problems, and don't form awareness of network security and security precautions. The main types of network security are shown in Figure 1.

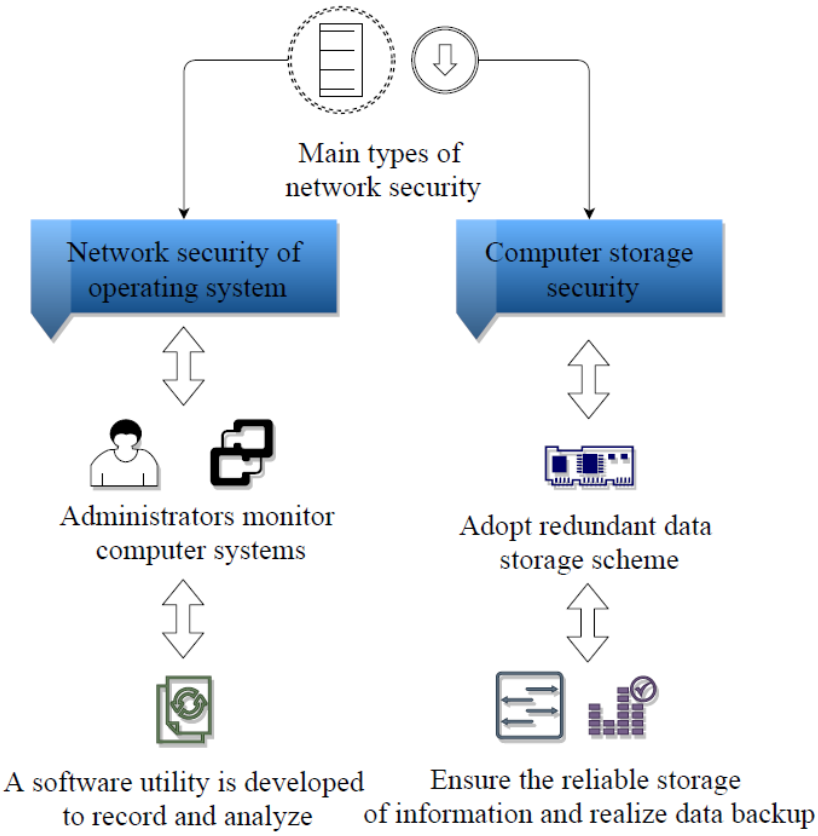

Figure 1 Main types of network security

It can be analyzed from the above figure that the main types of network security can be divided into two categories: network security of the operating system. Through this "advanced status", administrator users can monitor the behavior of the computer system and detect malicious or accidental damage. In order to consolidate this relationship, people have developed a large number of software utilities called audit software to record and analyze the behavior in computer systems. Computer storage is safe. Computers generally use magnetic storage devices to store data. Once the storage device fails, the loss caused by data loss or damage will be incalculable [9]. Application program security, computer viruses often use some loopholes or backdoors to infect or destroy applications, causing applications to fail to run; For some important databases, illegal users often invade them, copy, tamper with or steal useful data, so that the integrity of data in the network is damaged, and user data will be seriously leaked with unimaginable consequences. Therefore, users should take effective measures to protect computers from illegal intrusion.

Any important information is faced with the problem of data corruption caused by equipment failure. To solve this problem, redundant data storage can be used. Therefore, the protection of data storage security should be based on the encryption and confidentiality of the data itself, and targeted security measures should be selected according to different data types. In addition, it can also provide data storage separation protection, separate and store different data in big data, and track them in real time, so as to maximize the security in the data storage process [10].

3. Network security protection strategy in big data environment

In order to improve the safety factor of the computer system in actual use and reduce the occurrence of network injuries, while taking professional technical precautions, we should guide people to be more vigilant, pay attention to network security issues, strengthen security awareness and avoid various improper operations. Any type of operating system includes password authentication. The working mechanism of password authentication is that users submit their user names and passwords to the system, and the system recognizes the user's identity and allows users to access the required resources after checking them according to the user database [11]. In view of

various threats to data security in the age of big data, it is necessary to establish a sound data protection mechanism based on the characteristics and characteristics of big data, take active and practical security protection measures, and improve the security factor of data carriers. The specific treatment can be divided into five aspects, as shown in Figure 2.

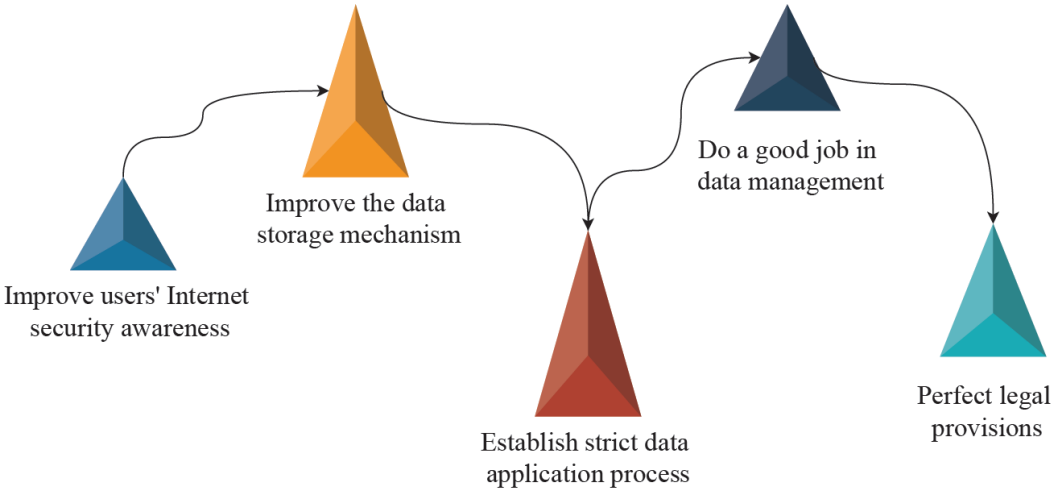

Figure 2 Protection strategy of network security in the era of big data

In order to effectively prevent the network security, we should start from the root, improve the security coefficient of the computer system, conduct research and exploration in programming, and practically improve the computer network security. According to the characteristics of big data in today's society, we should focus on deepening the awareness of responding to advanced persistent cyber attacks, and make targeted protection plans for this hidden security risk, so as to ensure that the early warning system will find malicious viruses at the first time. In the process of request and response, the encryption algorithm will be used to encrypt the information, providing the highest possible security protection at the lowest possible cost, and the authenticity of the identities of both parties communicating through the network. In the era of big data deepening, how to improve the security of computer network data and how to prevent network viruses has become an urgent task for IT workers.

Computer virus prevention is mainly to install security software. It is best to install professional anti-virus software for comprehensive monitoring and system security software. It judges whether it is a virus through dynamic rules, so users should update the installed antivirus software and system software in time to better prevent viruses. Save time for virus resistance, and minimize the economic losses caused by network security risks. From the perspective of citizens, citizens should be encouraged to abide by the Internet order and relevant laws and rules, and not to maliciously destroy the network environment and order. When bad phenomena are found, they should promptly report and stop them, supervise each other, contribute to the computer network security and jointly safeguard the network information security.

4. Conclusions

Based on the above research, we can draw a conclusion that under the background of big data development, people's production and lifestyle have undergone qualitative changes. The development of network information technology has broadened people's vision, but there are also many security risks. In today's society, big data is widely used. However, while people's data information is effectively used, there are also many illegal uses. Big data greatly simplifies the data processing process and improves the quality of data results. There are still many aspects to be improved in China's network security system. People from all walks of life need to work together to explore and find a scientific and reasonable system to maintain the security of the information network environment, so that people can get more valuable information and more convenience through the computer network. Big data is not only an object in the sense of computer research, but

also an important part of science and technology modernization, which is one of the four modernizations of the country. It plays a strong role in improving the national informatization ability, social progress, and the overall and lifelong development of individuals. In order to ensure the information security of the computer network, scientific and effective network security management measures should be actively adopted to improve the security protection level in the network system, so as to ensure the security of contemporary network information and effectively avoid security accidents.

References

[1] Liao B. Analysis of Computer Network Information Security and Protection Strategy in Big Data Era[J]. China Computer & Communication, 2018, 68(20):27-35.

[2] Xiao M, Guo M. Computer Network Security and Preventive Measures in the Age of Big Data[J]. Procedia Computer Science, 2020, 166(37):438-442.

[3] Jiang H. Discussion on Computer Network Security Under the Background of Big Data[J]. 2020, 56(35):44-55.

[4] Ouyang B, Cui Y. Research on Computer Network Security Prevention in the Era of Big Data[J]. Journal of Physics Conference Series, 2020, 1648(38):022011-022066.

[5] Zhu B, Chen Y, Cai Y. Three Kinds of Network Security Situation Awareness Model Based on Big Data[J]. International Journal of Network Security, 2019, 21(1):115-121.

[6] Gong W, Information D O, Hospital A C. Main Hidden Dangers and Preventive Measures of Computer Network Security[J]. China Computer & Communication, 2018, 38(10):21-42.

[7] Han C. Personal Electronic Information Security Hidden Danger and Preventive Measures under the Background of Big Data[J]. China Computer & Communication, 2018, 48(19):28-43.

[8] Wu Y. Hidden Dangers and Preventive Measures of Computer Network Information[J]. China Computer & Communication, 2018, 52(17):29-47.

[9] Luo D M, University J. Analysis of Network Security Preventive Measures Based on Big Data Era[J]. Digital Technology & Application, 2019, 31(11):36-44.

[10] Hui W, Amp X V. Exploration on the computer network security and preventive measures in the big data era[J]. Wireless Internet Technology, 2018, 34(10):15-22.

[11] Zheng C. Computer Network Security and Effective Measures for the Era of Big Data[J]. Springer, Cham, 2021, 25(7):21-38.