HiLL PUBLISHING

Data Science and Big Data Technology, 2025, 1(1), 1-4
https://www.hillpublisher.com/Journals/dsbdt/
ISSN Online:

Research on Computer Network Security Prevention Measures Based on Big Data Era

Yuanchao Qi*, Shengzhi Zhu, Xiaoman Qiu

Wuhan Donghu College, Wuhan 430212, Hubei, China.

How to cite this paper: Yuanchao Qi, Shengzhi Zhu, Xiaoman Qiu. (2025). Research on Computer Network Security Prevention Measures Based on Big Data Era. *Data Science and Big Data Technology*, 1(1), 1-4.
DOI: 10.26855/dsbdt.2025.12.001

Received: September 22, 2025
Accepted: October 16, 2025
Published: November 14, 2025

***Corresponding author:** Yuanchao Qi, Wuhan Donghu College, Wuhan 430212, Hubei, China.

Abstract

Nowadays, with the remarkable improvement of computer technology in China, more and more enterprises use big data technology for daily management. However, due to the characteristics of computer network, related employees are easily threatened by network security in the process of data transmission management, which leads to data leakage and seriously affects enterprise operations. Therefore, under the background of big data era, relevant practitioners need to improve the overall security and reliability of computer networks. On this basis, the protection measures of computer network in the era of big data are discussed for reference.

Keywords

The era of big data; Computer network security; Precautions

Introduction

Computer network technology is a landmark technology of the 21st century. After a long period of rapid development, China's computer capabilities have gradually improved, greatly promoting the development and progress of domestic information technology. People's lives and production are increasingly integrated with various information technologies, providing great convenience and significantly improving industrial efficiency. The advent of computer network technology has further driven societal changes. However, in today's era of rapid development and progress, computer network security has also attracted much attention. Information security issues are very serious. More and more information is being transmitted into big data, making it relatively easy for anyone to access personal information, seriously impacting user privacy (Shi, 2020).

1. The Importance of Implementing Computer Network Security Measures

In the era of big data, strengthening computer network security management is of great practical significance. In this new era, enterprises and related organizations have implemented networked and information-based management models in their operations, applying high-quality and efficient information and intelligent management methods in areas such as financial management and record management. However, the information security issues arising from this process also require attention. Various industries have improved the convenience of their work by incorporating big data technology. In this process, strengthening information security management and maintaining network security plays a significant role in improving social productivity. Whether it's an individual or a business, a large amount of data is generated in daily operations and life. To maintain information security, it is essential to ensure the targeted and secure processing of relevant data. In the era of big data, data has become a core production factor within enterprises, involving trade secrets and strategic development plans (Zhang, 2020). Only by ensuring computer network security can enterprises ensure efficient and stable operation and development. In short, in today's digital economy

Note: The article was originally published in *Industry and Information Technology Development*, and this is an authorized translation of it.

environment, enterprises and related institutions need to strengthen network security control, innovate and optimize existing network security management workflows by incorporating new ideas and concepts, and utilize new technologies to improve the level of network security control (Zhou, 2020).

2. Computer Network Security Issues in the Era of Big Data

2.1 Malicious attacks by criminals

In the network environment, there are not only many ordinary users but also many unauthorized users. These unauthorized users exploit various network technologies to infiltrate the network environment and steal user data. Another security risk to information security is passive network attacks, which do not endanger the security of the user's network. However, installing various viruses can paralyze the network, and once these viruses are activated, large amounts of user data can be sent to malicious actors. In today's information age, illegal and malicious attacks pose a serious threat to network security, and many users have suffered huge economic losses.

2.2 User information is easily leaked

Today, we live in an era of massive amounts of data, with a variety of information resources available. Computer networks generate vast amounts of data that are more complex, and due to unique network characteristics such as openness, external intruders can more easily infect systems with viruses, and users can more easily collect data on computer networks (Sun, 2020).

2.3 Unauthorized user access

Because wireless network setups are often too simplistic, unauthorized users can easily gain access, disrupting the network's normal operation. Users who purchase and install wireless networks may not be aware of security issues, allowing others to share network bandwidth, thus impacting their own and reducing network speed. If unauthorized users download malware after connecting, it can lead to computer virus intrusion. Furthermore, unauthorized users may modify router settings to increase bandwidth, interfering with legitimate users' network access. Unauthorized users can also steal legitimate users' private information for illegal activities, posing a significant security threat to legitimate users (Zhou, 2019).

3. Computer Network Security Precautions in the Era of Big Data

3.1 Professional firewall technology

Firewall technology falls under the category of traditional information security technology. Through long-term research and development, this technology has become increasingly mature and is now one of the important technologies in computer big data information security processing. Professional firewall technology is typically applied within network environments. The most common firewalls are filtering firewalls and application-level firewalls. Application-level firewalls provide a secure and reliable environment for computer operation, implementing comprehensive monitoring of the entire operating system. They can promptly detect various adverse factors attempting to intrude into the computer system. Once a virus intrusion is detected, the application-level firewall can promptly cut off the virus's transmission path, thus isolating the virus outside the computer system. Filtering firewall technology integrates the characteristics and functions of the computer system itself. Through the combined efforts of the two, a comprehensive detection of the computer system can be achieved, thoroughly eliminating detected viruses at their source and maintaining a healthy computer system operating environment (Zeng, 2019). By applying professional firewall technology, viruses and important information can be isolated from each other, fully protecting the security of computer big data information, avoiding data loss, and ensuring the security of information data.

3.2 Strengthen hacker prevention measures

Given the increasing prevalence of big data technology and the growing number of hackers in China, this poses a significant threat to cybersecurity. Therefore, it is essential to protect relevant personnel from hacker attacks. Collecting relevant data while ensuring computer network security improves overall network security. This will create a model based on hacker attack characteristics to accelerate hacker detection. Furthermore, employees can leverage the

isolation between intranets and extranets and improve firewall configurations to better defend against hacker attacks. Additionally, relevant personnel can utilize digital authentication technology to effectively control access, preventing unauthorized inspections of the computer network and thus enhancing overall network security (Liu, 2019).

3.3 Enhance the implementation of cultural heritage protection

Internet users must be aware that online information is vulnerable to damage from various factors and must raise their security awareness to protect their online information. When using the internet, computer users must strengthen information security measures, regularly change their online banking passwords, avoid clicking on illegal websites and information, avoid using insecure links, and fully protect their online passwords to reduce the risk of user information theft. Since internet information providers are data providers and the processing of internet information is proactive, it is crucial that they assume a certain degree of responsibility for internet information protection. Information service providers must always remember their tasks and responsibilities, strictly abide by internet information security laws and regulations, and effectively protect the secure use of internet user data. Furthermore, the cybersecurity department must fulfill its responsibilities and recognize that when internet information security is threatened, it must take appropriate measures to improve the predictability of information security and strengthen information security protection. Simultaneously, it needs to fulfill its information supervision function, formulate more comprehensive information security supervision measures, and implement them to ensure internet information security through effective measures. Information security supervisors must also improve their technical processing capabilities to effectively perform their internet information security supervision and management work (Zhou, 2019).

3.4 Establish and improve laws and regulations for computer network security management

In recent years, computer technology has developed and innovated at a relatively rapid pace. However, the corresponding laws, regulations, and security management provisions have not been updated in a timely and efficient manner. Many cybercriminals exploit legal and information security loopholes to conduct illegal business activities, posing a significant threat to computer network security management. In the absence of legal basis and institutional safeguards, these criminals exploit information security and legal loopholes to damage public network security, seriously disrupting the security and stability of market operations. Currently, my country needs to strengthen legislative supervision to regulate and control current computer network behavior. At the same time, law enforcement agencies need to strengthen the control of information security crimes and severely punish those who illegally steal and sell personal information. Against the backdrop of each round of technological innovation and reform, my country needs to promulgate corresponding laws and regulations to meet the security management needs under the changing landscape of computer technology, establish an ecological network security legal protection system, and maintain the healthy, long-term, and stable development of the internet. Furthermore, both enterprises and individuals need to have a strong awareness of computer security when using computers and networks, strictly adhering to relevant regulations and requirements to avoid malicious attacks. At the same time, enterprises also need to clearly define security management incidents and security operation procedures in their computer security management work to provide comprehensive security protection for asset information data.

3.5 Security design of computer network security platform and big data center

(1) Big Data Center Design Concept. Based on the principle of phased implementation and multi-layered protection, the design task of the computer network security platform big data center is carried out. The main idea is to effectively surround the big data center server by designing three layers of external security protection. (2) Big Data Center Security Planning. Big data center security planning mainly consists of two methods: a. the implementation of defense functions based on IPS deployment; b. the implementation of access control based on firewall deployment. In order to truly realize the continuous and stable growth of enterprise business and reduce the occurrence rate of congestion problems that are prone to occur during the operation of computer security platform to the lowest level, it is necessary to accelerate the deployment pace in a targeted manner, and shorten the deployment time while ensuring the scientificity and effectiveness of the deployment. (3) Big Data Center Configuration. The security configuration of big data is achieved through the convergence access of related devices such as switches and routers. Here, the configuration of anti-virus data is used as an example to carry out a relatively detailed analysis. The implementation of other related configuration tasks can be completed based on the support of device login and gateway system.

Conclusion

Currently, in the work of preventing computer network security risks, enterprises and individuals need to cultivate good habits, build a security protection system, strictly abide by relevant laws, regulations and rules to use the Internet in a civilized and safe manner, and improve the level of computer security risk prevention.

References

Liu, Y. (2019). A Preliminary Discussion on Computer Network Security and Prevention Measures in the Big Data Era. *Digital Technology and Application*, *37*(12), 196+198.

Shi, X. (2020). Discussion on computer network security and prevention measures in the era of big data. *Computer Knowledge and Technology*, *16*(03), 43-44.

Sun, Z. (2020). Research on Computer Network Security and Effective Prevention Measures in the Big Data Era. *Digital World*, (01), 50-51.

Zeng, R. (2019). Computer network security prevention strategies in the era of big data. *Wireless Interconnection Technology*, *16*(24), 15-16.

Zhang, Y. (2020). Computer network security and preventive measures in the era of big data. *Electronic Technology and Software Engineering*, (02), 259-260.

Zhou, G. (2019). Preventive measures for computer network security in the era of big data. *Information and Computer (Theoretical Edition)*, *31*(24), 189-190+193.

Zhou, P., & Yu, Q. (2020). Discussion on computer network security prevention in the era of big data. *Information Recording Materials*, *21*(01), 50-52.

Zhou, Y. (2019). Research on computer network security and prevention measures in the era of big data. *Heilongjiang Science*, *10*(24), 112-113.