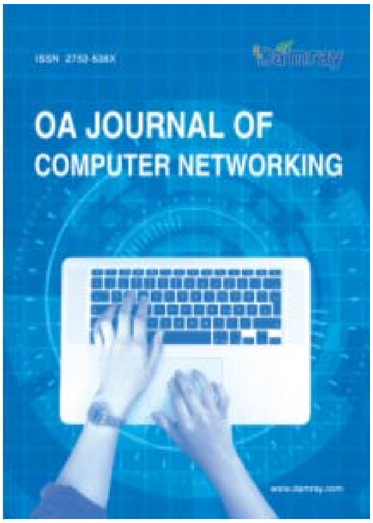
# Problems and Protection Measures of Computer Network Information Security in the Era of Big Data



https://oajcn.damray.com/

OPEN ACCESS

**DOI:** 10.26855/oajcn.2022.09.002
**Received:** July 28, 2022
**Accepted:** August 26, 2022
**Published:** September 22, 2022

**Yang Yuan**

Nanjing University of Science and Technology, Nanjing, China.

## Abstract

Computer network technology is changing the way people work and study. Computer network has penetrated into our lives and has had a profound impact on our lives. It not only promotes the development of social production in the direction of intelligence, but also the problem of network information security has gradually become a hot issue that people pay attention to. Computer network security is a long-term, arduous and very important system engineering. The network security technology mentioned in this paper is a relatively common and general technology in network security, which can guarantee a certain network security in combination. This paper expounds the definition, existing problems and protection measures of computer network information security, discusses the network information security protection and computer network information security loopholes in the big data environment, and proposes computer network information security countermeasures in the big data environment. With the wide application of computer network communication technology, information security plays an increasingly important role in maintaining social stability, promoting economic development, and safeguarding national security.

## Keywords

Computer Network, Information Security, Protective Measures

## 1. Introduction

Big data technology has powerful information data collection, storage, processing and analysis characteristics, which can greatly simplify the information data processing process, and it has become an important pillar of various social production and business activities. However, due to the openness of the network environment and other characteristics, network security risks emerge in an endless stream, so it is very important to strengthen the protection of computer network information security. Under the background of the rapid development of informatization, the information network has become the core resource to support the sustainable development of the national economy and ensure the national strategic security, while information security is related to the construction of the army and national defense, and its security issue has risen to a major national security issue. Strategic issues. Maintaining network security is not only a need for national security, but also a need for national stability and development.

## 2. Information Security

### 2.1. Concept

Network information security, in a narrow sense, refers to the security of services and information in the network, ensuring the security of software, hardware and system data in the network system. Broadly speaking, the theories and technologies related to the integrity, confidentiality, authenticity, availability and control of network information belong to the category of network information security. Network information security mainly refers to the control of human or material resources in a certain cyberspace to ensure the authenticity of information in the network to a certain extent. In essence, computer network information security mainly refers to the security and stability of hardware configuration in the computer system and the confidentiality and security of software data information, ensuring that the hardware and software are in a normal and safe operation state in the computer system, and will not be maliciously damaged and tampered by the outside world, so as to better reflect the reliability of the computer network.

### 2.2. Features

#### 2.2.1. Changes in the basic principles of information protection

With the continuous development and progress of big data, there will still be some security problems in computer network information security. Although users can directly obtain the information resources they need through traditional collection methods, the complexity of the dissemination of data resources is deepening at this stage, and more and more information resources are disseminated on the Internet platform [1]. Based on these changes, related Staff should improve their computer security technology. If the computer has certain technical limitations, the data information received by the user when using the computer is likely to be unreliable. In the context of the current big data era, the requirements for data information are different from previous network security technologies. Generally speaking, the subject rights of contemporary big data network data are weaker than traditional network data.

#### 2.2.2. The value contained in big data leads to the occurrence of computer security risks

Big data technology occupies a very important position in people's life and work. It can not only quickly obtain the required data resources, but also shorten the unnecessary collection time. In the process of development, enterprises need to recognize the value of big data technology, integrate this technology into enterprise work, and give full play to the value of this technology. Therefore, the relevant staff needs to continuously strengthen the computer security technology [2].

#### 2.2.3. The security risks of big data are invisibly magnified

There are many areas that need to be adjusted in the process of using cloud computing technology to disseminate information. With the passage of time, these deficiencies have a great adverse impact on the development of computer security technology. Now users can use big data technology to collect the information of each customer, and countries or regions can establish cloud computing service platforms locally, but there are still security problems, customer data leakage, and personal privacy and security are gradually increasing. These phenomena will adversely affect the development of big data technology.

## 3. The importance of information security protection

With the rapid development of information technologies such as big data technology, cloud computing and Internet of Things technology, computer technology and the Internet have been integrated into all walks of life, becoming a necessary tool for data transmission, and a necessity for people's daily online shopping and online learning. Because of the wide application of the Internet, the network environment security of computer systems and the confidentiality of information and data are particularly important for the operation of business units and personal life. The security defense of computer network information helps the integrity and confidentiality of user information, reduces the possibility of illegal elements stealing information, and prevents information from being maliciously tampered with and stolen; it helps to meet the requirements of information technology development, while maintaining personal safety online s right. The development of network technology brings the advantage of convenient access and transmission of information and data, which can store a large amount of data in the intricate network space [3]. These data not only represent their own digital meaning, but also contain the survival and development space and future growth value of each enterprise. In today's era of rapid development of big data, more information can be received in time, which is more convenient for daily life and work needs. But at the same time, the mass dissemination of information will also lead to malicious disclosure of users' private information, making the user's own information in an unsafe state. Therefore, the computer network is also a double-edged sword. In any case, we must strengthen the emphasis on network information security.

## 4. Problems existing in computer network information security in the era of big data

### 4.1 Diversification of virus spread

Computer virus is written by program code, which has certain destructiveness, concealment and spreadability, and causes serious harm to network security. With the full popularity of the Internet, the spread of viruses has gradually shown a trend of diversification. The known transmission methods of viruses are network links, U disk transmission, access to dangerous websites, download of virus files, online chat, and mail delivery. With the rapid development of science and technology, the scope of network applications is getting wider and wider, and the network viruses that follow are also being updated, which leads to the gradual increase in the complexity and difficulty of people dealing with network virus problems, which affects people's daily work and study.

### 4.2. The risk of personal information leakage increases sharply

In the big data environment, the information security threats faced by network users are not only the leakage of personal privacy information, but also the key is that big data will predict the behavior and status of network users, and personal privacy information will be widely connected and analyzed. Sensitive information such as personal ID numbers, mobile phone numbers, account passwords and other sensitive information can be easily obtained illegally and used for criminal acts such as fraud and fund theft; various personal information trading platforms have emerged in large numbers, and the black information industry chain has developed rapidly, which has seriously violated The economic and spiritual interests of Internet users. At present, various information security problems occur frequently [4]. It can be seen that the popularization and application of big data creates a more convenient environment for the development of various industries and people's lives, but also makes the personal privacy of network users face huge security risks.

### 4.3. Hacking

Hackers are a very active group in the computer network, using the computer technology they master to destroy the security of the computer network system. Hackers use illegal means to attack computer systems, which are highly threatening and destructive. The main attack method is to find system loopholes to intrude on the computer, steal system confidential file data and personal account and other private information, and infringe on the user's personal privacy. Attacks that disrupt the normal operation of the system will cause the system to deny service to users and make the computer system paralyzed and unable to operate normally. In addition, hackers often use proxy servers to scan and attack the target computer, intercept important information, and achieve the illegal purpose of intrusion and stealing. Some hackers will clear the log files after the invasion, and use manual clearing and log clearing tools to achieve the purpose of leaving no trace of the invasion and hiding the intrusion attack behavior.

### 4.4. Weak awareness of personal safety protection

My country's network not only has security risks such as cybercriminal activities, but also has the problem of lack of Internet users' awareness of self-protection of privacy and security. The public and individuals in our country have insufficient awareness of network information security protection. This lack of awareness directly leads to the theft of personal network information by illegal intruders. In the process of using the Internet, most users perform improper operations after entering personal information, which leads to a series of information security problems such as information leakage. In recent years, even if Internet users install firewalls, their protection effect is not ideal, and they are more frequently attacked by hackers. Therefore, gradually cultivating a good awareness of network information security can better protect the security of cyberspace.

### 4.5. There are loopholes in the operating system

Because a large number of applications are running in the computer operating system, there are inevitably certain defects in network management, resulting in the existence of different degrees of loopholes in the computer system. When a computer user chooses to upgrade the system, other system loopholes will also appear due to the increase of the functions of the operating system, which will reduce the security of the entire operating system and affect the normal use of other applications in the system. The vulnerability of computer operating system is a serious hidden danger that threatens network information security. The loopholes in the system will provide hackers with an intrusion window, so that they can successfully invade the user's computer operating system and damage the computer operating system, causing serious impact. The reason for the existence of loopholes in the operating system has a lot to do with the management ability and professional knowledge of computer network administrators. The technical level of computer administrators cannot meet the requirements of information security management, and the management methods do not fully regulate the operation of the operating system, which is not conducive to timely discovery of loopholes in computer software and hardware can easily lead to more information security problems in the computer operating system.

### 4.6. Lack of innovation in network information security technical means

In recent years, network information security technology management has been highly valued by the country. Not only my country has elevated network information security management to a national strategy, but other countries have also made important arrangements for the development of network information security. Judging from the current development status of network information security in my country, the actual effect of network information security management is still unable to achieve the goal of personal network information management. The main reasons for this status quo are the backward technology level of network information security and the lack of innovation in management methods. Most of the network information security management technologies have introduced foreign related technologies, the independent research and development technologies are backward, and the innovative ideas are insufficient. The society and organizations have not established a complete supporting supervision system, and it is difficult to fully implement the development and management of network information security.

### 4.7. Lack of perfect big data security protection system

With the industrial upgrading of various industries based on the development and application of big data, important data leakage problems frequently occur in many fields such as finance and government, and the contradiction between data information security and data sharing and opening has become increasingly prominent. Because there is no perfect big data security management guarantee system, some Internet and communication companies are tempted by various interests and begin to illegally obtain and use Internet users' online information and personal information to obtain economic benefits. At this stage, my country's network information security protection laws and regulations are still in the process of gradually establishing and improving, and the legal system related to information security still has relatively high limitations, many areas have not yet been covered, and the comprehensiveness and systematicness of information security laws are insufficient. This has led to criminals frequently exploiting legal loopholes, buying and selling credit data, and conducting false propaganda.

### 4.8. Information security protection is difficult

The most prominent feature of the big data environment is the huge amount of data, and with the passage of time, the massive data around the world will continue to increase [5]. At present, the unit of data storage has been upgraded to the PB and EB level. In the process of statistical analysis, processing and prediction of such huge data, the probability of information leakage is very high, which greatly increases the difficulty level of computer network information security protection. On the other hand, the specific types of structures in big data are also highly diverse, including social media usage, web browsing and shopping records of Internet users, etc., which are presented in various forms such as pictures, text, and videos. It also further increases the difficulty level of network information security protection.

## 5. Protection measures for network information security

### 5.1. Install antivirus software

Computers are often infested with viruses. Viruses hide inside computer systems without the user's awareness. In order to detect viruses in time and deal with the harm caused by viruses to the computer system, Internet users should install anti-virus and protection software, and constantly update the protection system in the computer, so as to better improve the performance of the computer system and protect the security of user information. At the same time, the national network supervision department should also monitor the viruses existing in the network in a timely manner, regularly release and update the virus database, and feed back to the specialized Internet management personnel for background program analysis. Relevant network security managers should improve the ability to identify and defend network viruses, and be able to provide effective protection systems for Internet users.

### 5.2. Encrypted storage and transmission of important files

The data file storage and transmission requirements of individual users and enterprise users in modern computer networks are very large, but in the process of data file storage and transmission, they are easily affected by adverse network factors, causing information security problems and becoming a major problem for network users in the era of big data. Safe question. On the one hand, when storing data files, they should be encrypted to avoid file theft and at the same time improve the overall security level of the information system. On the other hand, when transmitting data files, digital signature or file encryption technology can be adopted to improve the privacy and security of data files. Digital signatures can not only avoid the problems and risks caused by counterfeit signatures, but also play a significant positive role in reducing network transaction costs. In the actual application of file encryption technology, two encryption methods can be selected according to actual needs: one is end-to-end encryption, and the other is line encryption.

### 5.3. Build a network security firewall

In the era of big data, various types of malware and viruses emerge in an endless stream, which will pose a huge threat to the security of the computer network in the process of using it. Through the application of security protection system technologies such as firewalls, most malware can be interfered or shielded, and its impact on computing can be blocked. Adverse effects on the system. The development of firewall technology is based on topology structure. With the continuous breakthrough and development, it has more extensive and in-depth applications, which greatly improves the security and reliability of computer network systems. Firewall technology mainly protects the internal network of the computer network by building an artificial isolation layer to prevent illegal and unknown intrusions. At present, the most widely used computer network security control method in my country is still data information restriction, which isolates and shields information with security risks, thereby fundamentally restricting the intrusion of security risk information. Through the function of the firewall, the data information exchange operation during the operation of the computer network can be effectively controlled, various types of information data can be sorted and separated, and finally the effective protection of the internal network security of the computer can be realized and the problem of information leakage can be avoided. Computer users should regularly update the firewall, and do a good job in relevant information security protection, such as backing up important data files, adding screen protection, setting keyboard locks, etc.

### 5.4. Building a Defense System for Network Security

In order to better protect the information security of Internet users, relevant computer enterprise users should establish a network security defense system. At the same time, it is necessary to comprehensively investigate the current status of computer network information security protection management, discover and analyze loopholes in computer operation, establish a strict network management system, do a good job in security management and control, improve the effectiveness of computer network information security defense, and better ensure The computer system runs safely and stably. In addition, the relevant departments should correctly guide netizens to strengthen their own computer system management, control the way they surf the Internet, clear access records in a timely manner, close unnecessary network ports, avoid personal network information leakage due to improper operation, and better improve computer network security and stability, performance, etc.

### 5.5. Effective management of computer network personal platform accounts

The factors that affect computer network security are usually viruses and Trojans. Hackers and criminals steal personal information or business secrets by implanting viruses, which seriously affects users' personal security and computer network security. This requires people to start from the computer management platform, further strengthen the management and filtering of the computer network, and include the computer system as a key part of computer network security. Through the protection and control of the computer, the ability to resist viruses can be strengthened, the degree of computer danger can be reduced, and the user's personal privacy can be protected. As people's demand for computers continues to expand, improving computer network security has become imminent. However, users themselves also need to strengthen their computer security awareness, set complex passwords to protect account security, and reduce security risks to a certain extent.

## 6. Conclusions

Now, with the rapid development of social economy, network technology has been applied to daily life. It has brought a lot of convenience to the development of society, and people are increasingly inseparable from the Internet.

The use of computer network technology can make data more private and more comprehensive. In order to achieve data and information security, it is necessary to take flexible and diverse measures based on a systematic and complete scientific information security system, enhance network users' awareness of security protection and related skills, and rationally use advanced network information technology to build solid and stable information. The data security barrier enables big data technology to further exert its application advantages in social operation and production and people's daily life.

## References

[1] He Yunlong. (2022). Research on computer network information security risks and countermeasures [J]. Wireless Internet Technology, 2022, 19(06): 27-28.

[2] Wei Chaoying, Su Zhen, Li Haiqiang. (2022). Research on computer network information security countermeasures in big data environment [J]. Information Recording Materials, 2022, 23(06): 75-77. DOI: 10.16009/j.cnki.cn13- 1295/tq.2022.06.035.

[3] Xie Luying, Wu Jiaoshu. (2022). Analysis of Computer Network Information Security Problems and Discussion on Solving Strategies [J]. Wireless Internet Technology, 2022, 19(12): 26-28.

[4] Su Feng. (2022). Computer network information security risks and solutions [J]. Network Security Technology and Application, 2022(07): 159-161.

[5] Zheng Xiuyi. (2022). Computer network information security issues and protective measures under the background of big data [J]. Network Security Technology and Application, 2022(08): 161-162.