HILL PUBLISHING

Advances in Computer and Communications, 2023, 4(1), 65-69
https://www.hillpublisher.com/journals/acc/
ISSN Online: 2767-2875

Analysis of the Application of Computer Information Technology in Network Security under the Background of Big Data

Ying Lin

Aaron Clothing Store, Tianjin, China.

How to cite this paper: Ying Lin. (2023) Analysis of the Application of Computer Information Technology in Network Security under the Background of Big Data. *Advances in Computer and Communication*, 4(1), 65-69.
DOI: 10.26855/acc.2023.02.011

Received: February 15, 2023
Accepted: March 10, 2023
Published: April 7, 2023

***Corresponding author:** Ying Lin, Aaron Clothing Store, Tianjin, China.

Abstract

With the rapid development of network technology, network technology has gradually been integrated into people's daily life. In the process of network application, massive data and data will be generated, which will determine the governance of human society and the allocation of resources. Because computer technology is closely related to the security of Internet technology, it has introduced modern technology into the Internet, which has made great changes in its use and use on the Internet, and has had a great impact on people's life and work. With the rapid development of science and technology, the application of various high-tech means is becoming more and more extensive. It not only brings a huge impact on people's daily work, but also constantly changes people's ideas. However, it should be pointed out that in today's world, it is essential to strengthen the security of computer information technology. It is necessary to strengthen the application of information technology and strengthen the universality and stability of its application. Therefore, this paper focuses on the in-depth analysis of the network security application strategy under the big data environment, with a view to providing some reference value for relevant personnel.

Keywords

Big data, computer, Information technology, network security

Computer information technology has provided some convenient and fast conditions for people's daily work, and also provided opportunities for some lawbreakers. Under the current conditions of information technology, the security situation of the network is still very bad. When people use information technology to transmit and store information, it is often maliciously leaked, seriously affecting the normal use of users. However, with the rapid popularization of big data technology, people have thoroughly dealt with the network security issues. However, when many people use information technology, their understanding of network security is not strong enough, which gives hackers a better opportunity [1].

1. Big data technology

Big data technology is a new technology that can quickly search, analyze and process massive data. It can filter meaningful data from massive data to serve users. People's work and life are inseparable from the Internet. Using the Internet is likely to cause massive amounts of data and data. Use big data technology to analyze and process the data left by users. The information obtained by using big data technology is valuable information that can well solve people's daily needs. Big data technology is a kind of computer technology, which has its own advantages. In the vast amount of information, people can quickly obtain the most valuable and useful information, and the processing

method of these information is much better than traditional computer technology. The data collected by big data can not only acquire images, audio, video, etc., but also a large amount of data. In the context of big data, big data technology has been widely used in all aspects and has important significance.

2. Overview and application of computer network security technology

At present, with the rapid development of Internet technology, when technicians and users use computer network technology, they often cause computer system failures or security problems due to the use of computer technology or improper use. In addition, in recent years, there have been more and more problems of network intrusion. Many security vulnerabilities have led to the inability of technology to be effectively repaired, resulting in users' exposure of their identity when using network products. In this situation, we must pay more attention to network security, and conduct in-depth research and discussion on the application of computers and the Internet in its application process, which can not only ensure the safety of users, but also further clean the entire network environment. With the diversified development of Internet information technology, many modern computer network technologies have emerged one after another. Internet technology and computer network technology have the characteristics of usability, manageability, confidentiality, integrity and controllability. Especially, network security technology and firewall technology in computer devices can be specialized on computer devices and applied to computer programs, So as to ensure the user's safety in the user's application process [2].

3. Advantages of big data application

Although big data is likely to reveal personal identity, it also has many advantages. For example, big data is born from cloud computing, which uses Internet technology to provide better services for users of many applications. It can not only save data, but also analyze data of various applications. More importantly, it can use massive data for secure computing, to determine user preferences. In this process, people store a large amount of data and information in the network, which not only facilitates people's query, but also facilitates people's query. At the same time, through virtual computing, the network can also provide better services for people's work through virtual computing. However, compared with the previous computer network technology, the large data storage technology has higher security, can better protect the user's privacy, and the storage method will not be displayed on the terminal of the device, but stored in the network. Even if the computer or terminal fails, the stored data can be queried through the account.

4. Core factors affecting network security

4.1 Internet openness

With the rapid development of network technology, information technology has entered people's daily life. It has open characteristics and can be applied to all walks of life. However, with the rapid development of Internet technology, many problems have also followed. Some illegal acts have been lured into the orbit of crime by money and interests. Although the computer has some self-defense functions and can protect itself through IP, its role is more significant before it is infected. When it is attacked, its value will be greatly reduced. In addition, when using computers for data transmission, if the security of the transmission service is not high, it will cause serious security risks. In the face of numerous current network security incidents, relevant departments must conduct in-depth analysis and discussion on the technology of strengthening network security, and establish a network security protection technology with a certain high cost performance and high level [3].

4.2 User's non-standard operation

The core of computer network security technology is the user. That is, computer users must master technology to effectively use computers, and ensure that computers can make full use of computer performance in the user's life cycle. Otherwise, computers will have network security problems. The reason for the failure of the computer in the process of use is that the operator is not familiar with or does not understand the operation process of the computer, resulting in the user's operation error, thus causing the computer safety problem. In addition, in the process of computer use, it is very important to understand the safe operation of users. Without proper preventive measures, personal data may be leaked, such as identity documents, credit cards, etc. From this point of view, in order to ensure the recurrence of such accidents, users must learn how to use programs to ensure their own operating standards.

4.3 Network virus

Although big data technology provides great convenience for human life, it also creates a favorable environment for network intrusion, which leads to increasingly prominent network security issues. Because of the concealment and high infectivity of network virus, once infected, it will cause great harm. Most viruses are from external devices and external devices, which pose a great threat to the security of the network. In addition, because many users store their data on the computer network, hackers will attack users' computers to obtain better data, resulting in a significant decline in computer performance [4].

5. Common problems of information management technology in network security under big data

5.1 Incomplete information security management system

For many companies, CIO was established by many companies in the early stage of development, and this system was later recognized and applied by many companies. Through the investigation of the development of domestic enterprises, it can be seen that although most companies have established specialized management organizations, their internal business models still remain in the original management system and management methods, lack of flexibility, and the work division and coordination efficiency of each functional department is not high, which also leads to many security problems in the enterprise's network information management. In addition, due to the lack of clear regulations and regulatory support, domestic enterprises lack effective network security management, and lack effective constraints on them. At the same time, due to the low level of understanding of informatization and network, network security problems occur frequently.

5.2 Insufficient investment in information system security management construction

In the West, it attaches great importance to the security management of network information and has invested a lot in it. However, in China, people have not paid enough attention to the security of the network information system and the financial support. For large companies, the investment in IT systems accounts for only 2% of the company's total revenue, while the investment in small and medium-sized enterprises and private enterprises is less than 1%. Through analysis, we can see that at present, many domestic companies have focused on their own development and ignored the basic security of the network, while the internal network security management organization has no real role, some are just a cover, and there is no necessary software upgrade, resulting in frequent network security problems. Once problems occur, they cannot be effectively handled, this will seriously damage the company's development.

6. Main factors affecting network security in the context of "big data"

6.1 Public use of networking

The openness of the Internet and the whole big data environment make the Internet well used in social life and create huge benefits for enterprises, but there are also criminals who illegally use the Internet for private interests. Because the IP protocol adopted by the computer network itself is not strong enough to protect itself, the security of its transmission service is not high during data transmission, which poses a great threat to the security of the computer information network.

6.2 Improper operation of computer network operator

In the process of computer application, the operator is the central link of the whole system. Only by ensuring its correct operation can its function and function be fully realized. In use, due to the inconsistent and unskilled use methods and conditions of each operator, various hazards will be brought. In addition, the security of some operators is not high, and the leakage of key information such as user's security password when using the network poses a serious threat to computer security.

6.3 Invasive network virus

On the premise that it greatly facilitates people's daily life and work, it also creates a favorable environment for hackers to invade, making network problems more prominent. Computer network virus has the characteristics of high concealment and high transmission. When the virus invades the computer, it will cause huge damage to the user's

computer system, and even bring huge economic losses. Usually, the source of computer viruses is external devices and network data, so we must pay enough attention to these data.

6.4 Computer hackers

The reason why hackers come into being is, to a large extent, that many computer hackers can use flaws in the network to steal users' personal data or enterprise information. Hackers implant Trojan programs into computers in order to illegally steal confidential information and make profits. In particular, some secret data have been stolen, causing huge damage to computer users. It can be said that the harm of hackers exceeds that of computer viruses, which will not only threaten the security of computers, but also pose a great threat to the overall operation of computers [5].

7. Application of computer information technology in network security under the background of "big data"

7.1 Effectively improve national security protection awareness

On the security of computer network, strengthening the security of network is the most direct and effective way. Government officials should remain vigilant and continue to strengthen their prevention and attention. Through training or lecturing on the characteristics of relevant individuals, students can understand the importance of the network, gradually form the concept of security and prevention, and enhance the awareness of prevention.

7.2 Establish a sound security mechanism and system

From the perspective of network, security mechanism is a very effective means of protection, which is of great significance for promoting the development of computer technology. In order to achieve network security in daily work, we need to build a sound operation mechanism, scientific technology model, sound management technology model, sound talent management system, strengthen technology management, strengthen technology management, and improve the quality of employees. Managers needed by enterprises and society have laid a solid foundation for the efficient operation of network security. All units and units should actively promote the construction of safety management system, formulate long-term plans, strengthen safety education, effectively enhance the emergency response awareness of all units, and enhance the network security of enterprises [6].

7.3 Improve the security technology of computer information network firewall

Computer network security is a major guarantee of computer network security. Its purpose is to monitor the access of network data, so as to achieve the purpose of information security. On the premise of enhancing the security protection of the intranet and intranet, it can effectively prevent outsiders from using illegal methods to invade the LAN and ensure the security of the LAN. In addition, it is necessary to strengthen the preset of firewall technology, and use this technology to test the effectiveness of data transmission on the network, so as to effectively prevent illegal users from carrying out illegal data transmission. This technology can also prevent the setting of malicious plug-ins and the automatic screening of various harmful messages, so as to prevent various illegal acts. When necessary, it can also be used together with other network security software to ensure the security of the entire system.

7.4 Safety risk prediction

The potential safety hazards in engineering construction are analyzed, including technology and equipment. In the Internet environment of the Internet era, there are also great potential risks in the information security of the network. To ensure the security of information, we must be able to predict all kinds of security risks in the network, and be able to respond quickly and reduce their impact. Traditional computer information technology has a weak data processing capability, so it is possible to make risk estimation, but only limited to estimation. However, the use of big data technology to predict the security of the network can effectively play its advantages in massive information, and its most important protection purpose is to prevent network intrusion. With the development of science and technology, network intrusion has become increasingly complex and diverse, and has become an important issue for network security. At present, in the era of big data, it is very difficult to identify hackers only by personal strength, and it will greatly reduce efficiency. Therefore, it is necessary to apply big data technology to the level of computer information security to promote the development of information technology. The use of big data technology can better identify

network attacks, thus ensuring network security.

7.5 System error handling

There are both software protection and hardware problems in computer information security. Among the hardware failures, the most important is the system failure. In the normal system operation, some problems will occur in the hardware, such as aging, damage, etc. When a hardware failure occurs, the system will be forced to stop, and the data stored in the system will also be leaked. In traditional computer technology, problems can only be detected after they occur, and it takes a long time to repair. However, through big data technology, users can scan the hardware of the whole system in an all-round and detailed way, analyze the scan results in a timely manner, find faults in advance, find potential dangers in advance, and repair faults as quickly as possible. Improve the security of computer software and computer information.

7.6 Vulnerability recovery technology

In order to adapt to the rapid development of computer network technology in the era of large-scale information, people must be aware of the importance of security issues, and must increase the research and research on security issues in order to realize the scientization of security issues. The application can implement a security defect repair program to correct errors in time, thus preventing a large amount of data leakage. Using the security patch of the system, we can quickly repair the security risks of the computer network and the network. RD staff should improve the original security protection measures to ensure the normal operation of the computer network, enhance the anti-virus ability of the computer network, and reduce the security risks in the computer network. In order to make effective use of the network vulnerability repair technology, the staff should always pay attention to their working conditions, and take timely repair technology in case of abnormal conditions to ensure the normal operation of the system, which will also cause continuous security risks.

8. Conclusion

This paper believes that the current computer network technology has been quite developed, and many industries have adopted this technology. However, due to the openness, internet, sharing, freedom and other characteristics of the Internet, many lawbreakers will use these loopholes to steal information needed by others, thus posing a serious threat to their own privacy. Therefore, on this basis, it is necessary to take practical measures to strengthen the security of computer information systems, and to deeply understand the knowledge of information technology and information technology to ensure the security and stability of network information.

References

[1] Wang Wei, Zhao Yifang. Computer network information security and protection strategy in the era of big data [J]. China-Arab Science and Technology Forum (Chinese and English), 2022, (1): 72-75.

[2] Chen Wei. Research on computer network information security and protection strategy in the era of big data [J]. Electronic World, 2021, (9): 10-11.

[3] Lei Xueqiang. Research on computer network information security and protection strategy in the era of big data [J]. Information recording materials, 2020, 21 (9): 206-207.

[4] Zhang Ling. Research on computer network information security and protection strategy in the era of big data [J]. Computer Programming Skills and Maintenance, 2021, (2): 166-167+176.

[5] Yuan Zhendong, Li Teng. Computer network information security and protection strategy [J]. Computer and Network, 2020, 46 (18): 53.

[6] Xiang Lili. Discussion on computer network information security and protection strategy [J]. Digital Communication World, 2021, (2): 34-36.