Advances in Network Security and Application of Information Processing and Retrieval for Large Multimedia Data Analysis

Yueying Li

Beijing Near Space Airship Technology Development Co., Ltd, Beijing, China

Keywords: big data; Network security; information processing

Abstract: This article first gives an overview of the big data background, then carefully analyses the importance of improving computer network information security under the big data background. Finally, according to the existing problems, corresponding protective measures are put forward to effectively guarantee the security of computer system, and make the computer play a greater role in the development of various fields of society.

1. Introduction

With the continuous development and innovation of social science and technology, the level of development of information technology continues to improve, and the comprehensive application of network communication technology also leads society to gradually enter the era of big data, which optimizes the development efficiency of society in all aspects and also plays a more positive role in social development. In the background of the era of big data, the transmission and acquisition of information has become more convenient. In this case, it has caused a certain impact on the security of computer networks, and even in serious cases it may lead to the leakage of computer network information and cause information security risks. Therefore, it is necessary to carry out adequate computer information security protection measures, so as to protect the security of information.

2. Overview of the big data era

As a term in the IT industry, big data refers to the collection of data that cannot be retrieved, searched and processed by conventional software within a certain time frame, and needs to be processed by new technical means to ensure that information retrieval is efficiently achieved by big data technology. On the premise of the current rapid development of society, the transmission and interaction of information has become more frequent. In various sectors of society, there are hundreds of millions of pieces of information generated and transmitted every day. The big data technology can be used to categorize and summarize such information, and the current situation and laws of industry development can be derived through analysis, which provides a data research basis for the development of various sectors of society and can improve the overall efficiency of social development. At the same time, if a particular industry needs to access relevant data, it can retrieve and analyze the data through big data to get effective data. In this process, not only the ease of data acquisition is improved, but also the quality of the data acquisition process is ensured, thus providing data infrastructure conditions for the development of social sectors.

3. The current situation of computer network information security in the context of big data

3.1 Vulnerabilities of computer network security prevention

In the process of computer operation, the risk of information leakage needs to be controlled through preventive measures to ensure the security of the computer in the process of use. However, in the current context of big data, the information data from the network is more complex and massive. If there are vulnerabilities in the computer prevention, it is impossible to effectively identify the security aspects of the information. Once the vulnerability of the computer system is accessed and exploited by unruly elements, it may lead to the security risk of information leakage.

  DOI: 10.25236/iemetc.2022.013

In serious cases, it may even be attacked by network hackers, resulting in the information of enterprises or individuals being illegally accessed and used for illegal activities, causing serious hazards to social development.

3.2 Attacks of computer network virus

During the computer usage phase, computer viruses can also cause great hazards to network information security, leading to the paralysis of computer systems, which in turn can lead to serious impacts on business development. Computer viruses are defined in the industry as malicious programs that are artificially programmed and destructive to computer systems, and can directly threaten the security of computer information. Computer viruses can be spread in various ways, and they can enter a computer not only through system vulnerabilities, but also through network programs and files. Once the computer antivirus software can not carry out effective identification and detection of computer viruses, there may be information risks, resulting in computer information leakage, threatening the security of computer systems.

3.3 Illegal invasion and malicious damage

Illegal invasion and malicious damage can also affect computing information security to a certain extent and jeopardize computer information security. Although computer technology continues to progress, hacking technology is also developing and innovating, and the types of network viruses are also continuing to increase. On this basis, it may lead to the destruction of computer systems and generate security vulnerabilities. And because hacking technology also continues to progress, these vulnerabilities can not be detected in time, thus resulting in the theft of confidential documents in the computer, and the normal operation of the computer may also be affected. In this case, it not only reduces the operational efficiency of social enterprises, but also may lead to the stagnation of the production and development of social enterprises, which seriously affects the economic efficiency.

4. Protection measures for computer network information security in the context of big data

4.1 Improving software and hardware configuration for computer security

In the big data environment, in order to ensure that the computer can better systematize the application of big data and achieve the purpose of improving the development efficiency of social enterprises, it is necessary to pay full attention to the information security protection of the computer network to prevent the leakage of computer network information and cause unnecessary economic losses to social enterprises. In this process, the first step is to improve the software and hardware configuration of computer security, so as to ensure the security of computer network information. Given that social science and technology continues to develop, hacking technology also continues to improve, and the increase in the number of network lawbreakers also has an impact on computer information security, so it is naturally impossible to effectively prevent the problem of information leakage by relying solely on the protection means of network information security in the traditional mode . Therefore, it is necessary to improve the supporting facilities for computer network security management, and at the same time to monitor computer network security in real time. Secondly, in the enterprise, the network security supervision website should also be used to monitor the use of the computer by the staff during work, to prevent the staff from browsing network information not related to work and bad network information, effectively prevent the network Trojan horse from invading the computer, so as to prevent the computer from being attacked by network hackers in the process of use. Finally, in terms of software, it is also necessary to protect the computer system security in a timely manner, regularly check for viruses on the computer system, and detect the presence of Trojan horses in the computer by specialized means. For the vulnerabilities that exist in the computer system, the corresponding vulnerability patch should also be installed in a timely manner, so as to effectively prevent the vulnerability from being exploited by lawbreakers.

4.2 Creating and deploying network security proxy servers

In order to fully ensure the security of the computer in the process of practical application, to avoid the risk of leakage of computer network information, and to comprehensively improve the efficiency of social development, network security proxy servers can also be created to ensure that the computers can be used more effectively in the actual applications. A proxy server is not a primary server, but a proxy server that serves the same purpose as the primary server in the application. A proxy server can be deployed to ensure the network security of the computer in the process of application. In the process of application, the proxy server can be interconnected with the external network, and accomplish the function of information acquisition and interaction. After that, the primary internal server and the proxy server can be interconnected to ensure the security of information in the process of computer use. In the above process, the proxy server can be an effective means of isolating viruses on the network, and the security of information can be guaranteed in the process of data exchange between the internal network and the external network to prevent computer information from being stolen by lawbreakers [3]. In order to ensure that the proxy server can fulfill the functional requirements of network protection in a better quality, the proxy server should also be set up in a scientific way to ensure that the proxy server can perform its functions in a better quality. For example, firewalls and alarm systems can be installed, which can fully reduce the risk of computer systems being infected with viruses.

4.3 Applying the virus protection system

For computer information security protection, one of the effective measures is to prevent computers from being infected with network viruses, which can not only upgrade the level of computer security protection, but also fully secure more stable and efficient operation of computers. Based on this, it is necessary to install an anti-virus system in the computer to effectively prevent the computer from being infected with network viruses. In the actual application process, if there is a virus-like suspicious file in the computer, the anti-virus system will automatically quarantine it to prevent other files in the computer from being infected, and then determine whether the file contains a network virus through comparison and analysis, so that the functional requirements of anti-virus network protection can be achieved [4]. In the process of installing an anti-virus system, it is necessary to ensure that the installed system is obtained from a regular source. For example, a genuine network anti-virus system should be purchased from a professional organization or enterprise, and then installed on a central server. Subsequently, the computer equipment should be mounted with PC-based virus detection software, which can achieve the purpose of improving the effectiveness of virus protection and efficiently prevent the destruction of computer systems by viruses. It should be noted that the computer needs to be regularly checked for viruses throughout the disk to prevent network viruses from hiding in the computer disk, and also the anti-virus system should be updated in a timely manner to ensure that the virus database contained in the system is up-to-date, effectively preventing the risk of information leaks in the computer network.

4.4 Enhancing the protection awareness of the staff

In the process of computer use, an important factor that generates the risk of information leakage is that the staff mistakenly click on the files with network viruses in the process of use, thus bringing the Trojan horse virus into the computer and affecting the security of computer data. Based on this, in order to prevent the risk of network information leakage during the use of computers, it is also necessary to enhance the protection awareness of the staff. In practice, the staff concerned can be regularly trained in the awareness of network security protection, and relevant knowledge can be imparted to the staff, and the staff can be made aware of the importance of network security and the actual practice to make sure that they will not mistakenly click on the bad messages and cause information leakage in the process of work.

5. Conclusion

In summary, in order to guarantee the security of computer information in an all-round way, it is necessary to analyze the risk factors existing in it and put forward the corresponding measures to prevent the risk of network information, so as to ensure the security of the computer during the use period. Through the above measures, we can also effectively avoid the situation of information leakage in the current era of big data, so that the computer can provide a full range of assistance to the development of society.

References

[1] Yang Xin. Research on Large Data Information Security Mechanism Based on Cloud Platform [J]. Information Science, 2017, 35 (1): 5.

[2] Chen Xingshu, Zeng Xuemei, Wang Wenxian, et al. Network security and intelligence analysis based on big data [J]. Engineering Science and Technology, 2017 (3).

[3] Zhou Liang. Large Data Oriented Network Security Analysis Method [D]. Nanjing University of Posts and Telecommunications, 2016.

[4] Zhuang Haiyan. Wireless communication network security risk prediction using large data analysis technology [J]. Microelectronics and Computers, 2019, 36 (8): 4.