

Network Information Security Analysis under the Background of Big Data

Quan Liu

China University of Geosciences Beijing, 100083

Abstract: With the increasing degree of information technology in China, the Internet information technology is becoming more and more advanced. Network information technology is ubiquitous and brings great convenience to our life. However, with the development of network information technology, security can not be ignored, so network technology workers should strengthen the security of network information, in order to prevent users' privacy from being leaked. Therefore, this paper combines big data analysis with network information security technology to improve the level of network information security.

Keywords: Big data; Network information; Safety analysis

1. Network information security in the era of big data

1.1. Impact of natural disasters on network information security

Although computer network technology has strong virtuality, it can not completely break away from the objective environment and become an information island. To make the external conditions stable, computer network technology becomes the basic condition for information transmission. To achieve global dynamic interconnection, it is necessary to note that the external devices of computer network technology are vulnerable. At present, relevant personnel have carried out a lot of research and put forward a variety of protective measures to enhance its safety, but such measures can only play a key role in the limited environment.

1.2. Impact of network information itself

With the development of big data, the scale of information on the Internet is becoming larger and larger, and more and more applications are involved, which makes the problem of Internet information security increasingly prominent. Secondly, while bringing many conveniences to people, it also brings difficulties to people's daily work, making it difficult for people to find and make targeted corrections in a short time. Finally, because the back-end program of the computer system is relatively complex, some users may obtain information through indirect channels when using the computer network. As far as front-end storage devices are concerned, opening access rights to multiple devices may bring difficulties to network intruders. This allows hackers to attack computers through the defects of these systems. Under the framework of MapReduce, Hadoop distributed effectively manages big data in the distributed system architecture in a reliable, efficient and scalable way. However, many users only use the program at the initialization stage of the application, and only use the program for simple tasks, such as recording, while ignoring information security. Although Internet information technology has been widely used in all aspects of social life and has many advantages, because of the characteristics of the open and sharing network, it will inevitably bring great hidden dangers to people's information security, making it difficult to ensure the reliability of the information it provides .

1.3. Impact of human operation factors on network information security

In China, the user is the leading network operator and also the main body providing network information services. However, because the computer network is an open system, its scope is very wide, and many users have not strong security awareness, and computer technology is not mature. Therefore, when using the computer network, improper operation often brings risks to the network information security. For example, the user password is set, but the user does not know how to set the password, but simply sets a simple number or text combination. Therefore, when performing file removal and login removal, the importance of file removal is often ignored, resulting in insecurity of network information. In addition, because the computer administrator's management of network information is not perfect, its security is difficult to be guaranteed.

2. Network information security technology in the context of big data

2.1. Data encryption method

Data encryption is a special method to encrypt data based on password to ensure data security. In this process, the cryptosystems used mainly include symmetric cryptosystems and asymmetric cryptosystems. Based on the specific needs of users, the existing network technology and virtual network form are gathered, encrypted, transmitted, processed and used in the network transmission layer, which can make the network information more convenient. In practical applications, most enterprises adopt simple password technology to ensure data security.

2.2. Access control technology

Access control technology refers to the main method to ensure user information security by restricting access to users based on the existing network security protection. Access control technology refers to the effective control of network resources through access to network users, ensuring the security of network information, and preventing illegal access to network resources. The user's privacy can be effectively guaranteed through access control. Network users should use their own access rights to ensure the efficiency and reality of access technology. At present, network information access control technology mainly includes: network login right, network access right, attribute security, and server control security.

2.3. Intrusion detection technology

Intrusion detection technology is a kind of security defense technology, which can quickly respond to the intrusion in the network and intercept it. In the traditional network information security technology, it is an important technical means to provide real-time protection for the network system. The intrusion detection technology collects and compares the generated intrusion information in real time according to the preset attack mode and characteristics of the system. If the system preset the attack mode to meet the attack characteristics, it will be considered as an attack. However, this method can only protect known intrusions and attack features, while for unknown and new intrusions, it cannot effectively protect them, thus threatening the network information security. The existing detection technology mainly analyzes the system file in all directions to determine whether there is an attack, and uses genetic algorithms, data mining, fusion and other methods to detect the network, so as to improve the security of the network .

3. Protection measures for network information security in the era of big data

3.1. Establish awareness of account security protection

In the context of big data, human beings are increasingly connected with the Internet. At present, there are more and more registered accounts in online banking, computer systems and social network platforms. In addition, driven by big data technology, the role of platform accounts is increasingly obvious, and its role is closely related to individual privacy, property and other interests. Therefore, once the user account is harmed, it will not only harm the social security, Therefore every Internet user should establish account security awareness and pay attention to account security to avoid unnecessary losses. Network information security technology is not omnipotent, as long as every user can realize the importance of network information security and take the initiative to take security measures to provide reliable security guarantee for network information.

3.2. Strengthen network monitoring and monitoring

To monitor the network information, we should monitor the information data in real time and detect and deal with the problems in the information in a timely manner. With the advent of the era of big data, the amount of information on the Internet is becoming increasingly complex, and its fields are becoming increasingly extensive. Therefore, effective network monitoring of the Internet can provide a strong guarantee for the safe and stable operation of the Internet. At present, there are two main methods for monitoring computer networks: statistical analysis and characteristic analysis. When evaluating the network operation, the basic basis is statistical data. The characteristic analysis method is to record the known system failure. Whether it is statistical analysis of data or feature extraction, we should carry out in-depth research on this technology in order to better play its role.

3.3. Strengthen confidentiality measures for data

With the progress of science and technology, the means people can use are also increasing, and technological progress has also brought new opportunities to the security of network information. Therefore, when transmitting information and data, users should strengthen the confidentiality of data, and use passwords in the transmission process, which can help users avoid being used by hackers or criminals to intercept user data by taking advantage of the network gap. At the same time, due to the use of password technology, attackers It is difficult for criminals to break the data content and reduce the probability of tampering with users. Therefore, it can effectively enhance the network information security. The use of encryption technology for data transmission is a very effective method, which also has great benefits for the security of user's personal information. In this case, users must consciously use password technology to avoid data theft or interception, so as to better protect the security of user data.

3.4. Develop relevant technologies and regularly maintain equipment

In the big data environment, the construction of network information security system needs to update, implement, manage and maintain corresponding technologies and equipment. Enterprises should grasp the trend of industrial development and introduce it to the public. In the normal work process, professional personnel should also pay special attention to the normal operation of relevant technologies and equipment, and timely repair the damaged equipment or purchase new equipment to prevent network information security vulnerabilities

caused by the failure to repair the equipment in time. When constructing our country's network information security system, we should not only base on the traditional network information security system, but also pay attention to the traditional network information protection system, and learn from each other to complement each other . we should establish a new network information security system in line with China's national conditions, with the network information security as the core, under the premise of legal permission.

4. Conclusion

To sum up, in the big data environment, the security of network information has become increasingly prominent, which has attracted the general attention of the whole society. The use of big data has played a huge role in promoting the transformation and development of human society. However, while using big data, it is also necessary to carry out effective information security protection to ensure its security when using big data. In addition the computerized network, with its open characteristics, has been completely covered, which makes its information security more necessary. Establishing a network security management system and taking effective measures to ensure the security of network information has become an important issue that needs to be solved urgently.

References

- [1] Hao Cai. Research on Control Mechanism and Evaluation of Network Information Security in the Context of Big Data [J]. *Wireless Internet Technology*, 2021,18 (07): 33-34.
- [2] Huabin Duan. On Computer Network Information Security Risks and Solutions under the Background of Big Data [J]. *Information Record Materials*, 2021,22 (04): 235-236.
- [3] Yan Chang. Computer Network Information Security Risks and Solutions in the Context of Big Data [J]. *Information Record Materials*, 2021,22 (04): 198-199.