Data Governance Network Security Countermeasures Based on Big Data Background

Li Bin

North Sichuan Medical College, Nanchong, Sichuan, China

Keywords: big data; data governance; network security

Abstract: In the era of big data, the potential of data has been further tapped, which not only provides great convenience for people's production and life, but also promotes the continuous development of big data analysis. With the development of the open concept of data sharing, the leakage and loss of data in practical applications are becoming more and more frequent, which seriously threatens the personal privacy and security of citizens, the business development of enterprises and the stability of society. Therefore, at present, the network security strategy of data security governance in the era of big data has attracted much attention. This paper briefly introduces the formation and connotation of big data background, and puts forward effective network security countermeasures combined with the current situation and existing problems of data governance. Through the joint efforts of the state, enterprises, citizens and network data management departments, create a good network environment for the development of the big data era and promote the further development of China's social economy.

1. Introduction

With the continuous development of computer network technology, data in various fields shows a soaring trend, and big data also covers many sensitive and privacy components. Therefore, network security under big data has become a hot topic of concern. Big data has brought convenience to people's life and work, making people more and more dependent on computer network technology. It has become an important driving force for enterprise development to analyze and integrate enterprise data through computer network technology, make rational use of data, find competitive advantages and create value. Therefore, in the context of complex big data, how to effectively ensure the network security of data has become an important issue in the development of computer network technology.

2. Data Governance in the Context of Big Data

2.1. Data governance

In the big data environment, data governance mainly refers to the organization, norms, standards, policies and other related activities required for the effective use of data. Data governance is to transform scattered data into unified basic data, reduce the confusion of basic data and realize the comprehensive management of data. Privacy security in big data environment has become the focus of data governance. As shown in Figure 1:

  DOI: 10.25236/icmmct.2022.010

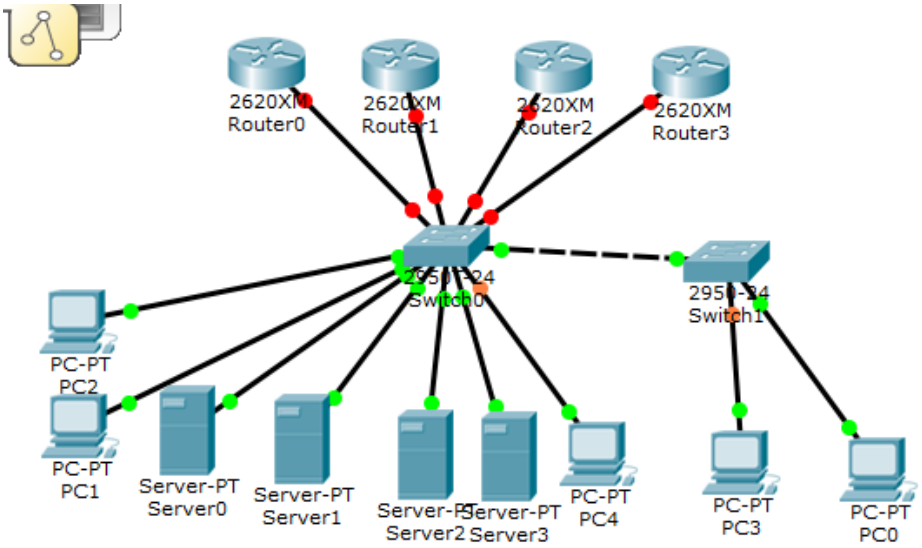

Figure 1 Network governance system display.

2.2. Privacy protection

Big data plays a dual role in China's social and economic development. On the one hand, the advent of the big data era has provided a continuous driving force for the sustainable development of China's social economy and greatly facilitated people's life and work*(Jiang Wenjun,2018)*. On the other hand, in the process of data transmission and storage, people are vulnerable to the influence of network security factors and violate the right of privacy, which eventually leads to users unable to find the location of data storage and effectively control the collection, storage, application and sharing of data. Based on this, in the context of the big data era, privacy protection has become an important content of data governance.

3. Current Situation and Existing Problems of Network Security under the Background of Big Data

At present, the concept of big data is gradually derived under the background of the development of the times, but data governance and network security have become the focus of attention, mainly in the following aspects.

3.1. Data destruction and disclosure

In recent years, network security has been destroyed and attacked, which makes the privacy and confidentiality of data become the focus of attention. With the development of the Internet, the problem of data destruction and leakage has become more and more serious. The most famous cases include malicious attacks and theft of user email and password information by hackers from Time Warner, the largest limited television company in the United States, the explosion of Apple App store, the disclosure of private data and user privacy of more than 10 million users, and the lack of guarantee of data security in the era of big data. This problem seriously hinders the utilization and extraction of massive information.

3.2. Inadequate awareness of data network security

People's concept of network security is weak. Generally speaking, all kinds of information entered in online shopping, sending e-mail, user registration and login account do not pay attention to the surrounding environment, or leave traces when browsing and clicking on the network, which will leak the user's secret information. In addition, some users do not have enough information filtering ability when using the Internet. They click to enter the pop-up link or dialog box at will, which is easy to be attacked and deceived by malicious websites or fraudsters. Moreover, because most users do not have professional network security protection technology, the information data

can not be repaired after being damaged, which brings a lot of inconvenience to their life and work and weakens the effectiveness of information data.

3.3. Risk of centralized data distribution is high

At present, many companies, enterprises or banks keep a large amount of available information. Such a huge amount of data collection means that the data will bear greater losses after being attacked, and it is easy to become the primary target of hackers. The institutions of these data clusters usually operate on a large scale and seek higher wealth by stealing information and data. These institutions are weak in data preservation and security protection. Once the data is lost, it will cause huge losses. For high-risk situations with centralized data distribution, this will become the goal of key governance.

4. Research on Network Security of Data Security Governance

4.1. Firewall interception function

In the network system, as an isolation technology, the firewall will ask the user whether to allow other people or other data to enter the network when performing two network communications. If not, it can effectively prevent hacker intrusion and virus intrusion, so as to protect network data. In the era of big data, the protective wall can monitor internal and external systems in real time, apply advanced information technology and intelligent management network system, effectively identify viruses, quickly intercept dangerous programs, accurately analyze and process data, so as to reduce the risk of virus intrusion and ensure the safe operation of network system. As shown in Figure 2:

Figure 2 Tool computer.

4.2. Intrusion detection system

Intrusion detection system (IDS) monitors the operation of the network system through professional software and hardware, finds malicious attacks in time, and ensures the integrity and confidentiality of system data. IDS is like the monitoring system in the building, and firewall is like the door lock of the building. If the thief enters the building, the monitoring system will give a warning in time and actively take protective measures. If IDS issues a warning, data security inspectors can solve the problem quickly and timely according to the warning information, and take targeted measures to prohibit intrusion, so as to ensure the security of network information and the stability of network system.

4.3. Enhanced attack Traceability Technology

In the construction of network security system, network attack source tracking technology is very necessary. Under stable conditions, when analyzing the attack of network information security system, it analyzes from multiple key kernel structure diagnosis, file and program levels, and assists in the analysis of initialization system and network traffic. At the same time, through the supervision of the unified and multi-level network security attack description model, the correlation analysis of massive log attack information is carried out in strict accordance with the relevant rules, so as to find the possible attack problems in the computer system faster and more accurately, and provide a reliable data basis for the follow-up network attack tracking work. However, in the application of network security attack Traceability Technology, there are still some deficiencies to be improved. On the one hand, the processing of heterogeneous data sources includes the processing of database and document database. On the other hand, in massive data processing, with the development of economic globalization and the combination of the Internet and the Internet of things, the amount of knowledge network data information has doubled, and there is still much room for progress in improving the implementation efficiency of large-scale network data traceability processing technology.

4.4. Anti-virus software

To strengthen data network security governance, we should establish a perfect information management system, strengthen virus intrusion prevention, establish a network vulnerability security sharing platform, develop targeted anti-virus software in combination with various data defense needs, and update it regularly to strengthen information protection. All equipment in the network system shall be installed with professional anti-virus software to prevent viruses from invading the computer and threatening network data. Strengthen the supervision and management of computer system data information, avoid malignant virus invasion, establish automatic virus detection and anti-virus system, and respond quickly when virus invasion is found. Building a vulnerability security sharing platform can reduce system vulnerabilities, do a good job in prevention and control in time, improve the security prediction ability of the network system, and greatly reduce the data security risk.

4.5. User safety awareness

At this stage, China’s computer information network has been popularized. People are very skilled in computer operation and have a certain understanding of software functions. However, some personnel do not pay enough attention to data security and lack awareness of security protection. Therefore, it is necessary to strengthen personnel safety education and training, improve users’ awareness of prevention, and let users pay attention to the security of network data. In the application, users can carefully read the prompt information, selectively upload personal information, pay attention to the concealment and privacy of information, and set a security password for important information*(He Jiang,2020)*. Relevant enterprises should strengthen data security management, do a good job in user information protection, and avoid criminals from using user information; With the development of network technology, many viruses bind the intrusion system with other software through camouflage. When applying software, users should be careful of unknown source links to avoid high-risk viruses having the opportunity to invade the system.

4.6. Identity authentication technology

User identification is an effective measure to ensure the security of network data. The traditional identification method is password. Many users use simple numbers as passwords. Criminals can easily crack and obtain system data, leading to the disclosure of personal information. It is applied in various fields of face recognition and fingerprint recognition, and provides a certain guarantee for people’s safety. But at the same time, hackers are also trying to find technical loopholes, and these identification methods need to be further strengthened. The application of red film technology can effectively improve the disadvantages of the system and strengthen data security protection.

Through the combination of various charging technologies such as identity authentication and data signature, the system can automatically recognize handwritten signatures. Once a forged signature is found, it will be processed quickly to ensure the security of network data.

5. Conclusion

In short, big data network security is a comprehensive discipline, which is widely used and involves a wide range of fields, which has brought great changes to all walks of life, but network security has also become an important factor restricting the development of big data technology. Therefore, in order to ensure network security in the context of big data, relevant departments must further study the technology to strengthen network security in the context of big data, ensure the real-time security and integrity of network information, and provide network security services for data in the context of big data.

References

[1] Jiang Wenjun.*Discussion on Computer Network Information Security in the Era of Big Data*[J]. Network security technology and application,2018(2):69-73.

[2] He Jiang.*Explore the Computer Network Security and Preventive Measures in the Era of Big Data*[J]. Information recording materials,2020(3):77-79.