Research on Big Data Security Protection System and Access Control Technology

Wang Weifeng, Xiao Bin, Pan Sikuo

University of Jinan, Jinan, Shandong, China, 250022

Keywords: big data; security protection system; access control technology

Abstract: Industrial development has a direct relationship with technological progress, and the continuous advancement of modernization has made information technology the backbone of industrial development. The state has also proposed a major policy that uses information technology to help the industry innovate and develop. The emergence of cloud computing, Internet of Things and big data technology has established a perfect information interconnection system for the modernization of the industry, and it has shown great utility in the big data security protection system in various industries. When operating the big data platform, the focus should be on building a security protection system and improving access control technology. In the analysis of big data security protection system and access control technology, this paper mainly discusses the architecture of big data security protection system and three construction measures, and finally puts forward the implementation points of specific access control technology.

1. Introduction

In the“13th Five-Year Plan”strategic development plan, the state put forward the requirements for strengthening the security protection of industrial data resources in response to the application of big data technology. Today's social development has increasingly demonstrated the characteristics of informationization, industrial data has grown exponentially, and under the big data technology, the efficient transmission and sharing of information has been realized. The increase in the scale of data information can obtain quantitative development indicators for various industries, but when applying big data technology, it is also necessary to recognize the problems in the data processing process, especially the security protection problem. Big data platform operation and maintenance personnel should effectively manage big data and strengthen data security management. At the same time, it must actively build a big data security protection system and strengthen access control to strictly resist illegal activities such as illegal intrusion, data theft, and tampering with data.

2. Comprehensive functional architecture of the big data security protection system

To analyze the big data security protection system, we should have a holistic and systematic thinking, and comprehensively grasp its main components from a system perspective. The functional architecture of the big data security protection system is relatively complete, manifested in security standards, security management and protection platforms. On the basis of grasping its main functional structure, it is necessary to carry out systematic design, and the design points are all levels in the big data security protection system. It is necessary to strengthen the hierarchical differentiation design, and at the same time, it is necessary to do a good level design. The following is a detailed analysis of each level:

2.1. Big data security standard layer

When designing the big data security standard layer, we must pay attention to the soundness of various laws and regulations, and make a scientific outline of the overall outline of big data security. The key point of the security standard layer is to master the standardization requirements of the big data platform, so as to further guide the standardization of big data security and improve the use efficiency of the big data security protection system.

2.2. Big data security management center

The Big Data Security Management Center has comprehensive functions and needs to comprehensively manage the operation and maintenance process of the big data platform. The security management tasks can be subdivided into data asset management, data service management, threat intelligence analysis management, security component management, risk situation management and audit monitoring management. Among them, data asset management needs to evaluate the security attributes of data assets, do a good job of data security attribute rating, and facilitate subsequent hierarchical management; data service management emphasizes the control of data usage rights and real-time control of data usage; Threat intelligence analysis management refers to tracking the threats appearing in the big data platform, and timely warning; security component management can dock the security management module, and deeply interpret the security policy package, based on the security mechanism, specific to the The configuration information is personalized and connected to each security component to receive configuration information; risk posture management emphasizes a comprehensive analysis of sensitive data, including location, scope of diffusion, and cost. For sensitive data whose partial security protection is not up to standard, clear identification should be made; in the case of audit monitoring management, the data flow graph of sensitive data should be monitored in real time, and for the data outside the data flow graph, the early warning management should be strengthened.

2.3. Big data security protection layer

Within the big data security protection layer, there are also many sub-levels. It is necessary to handle the access security layer, the cleaning security layer, and the storage security layer. In the access security layer, it is necessary to strengthen the interception of malicious code, and to detect and verify it in a targeted manner. To ensure the security of the imported data, in the cleaning security layer, the data should be cleaned and cleaned. The purpose is to ensure data consistency. After the cleaning is completed, the data can be efficiently filtered, and under the support of information technology, the printed labels are automatically printed and the data is classified. For the storage security layer, the data leakage protection at this level should be strengthened. When data is available, the data security level is mastered, and the data backup requirements are understood. The data is encrypted and processed, and fine-grained access control and integrity verification can be adopted for data encryption protection. In this level, the data security audit function can also be applied. For the confidential data of the platform, the access situation should be tracked, and the access record should be made to ensure the audit data is complete.

2.4. Cloud environment foundation support layer

Under the support of cloud computing technology, efficient processing and on-demand supply of data resources can be realized. In this process, the cloud environment of big data computing needs to be perfected, and the underlying resources should be enriched under the support of technologies such as upper-layer virtualization. Make sure in the process of building a resource pool, virtualization technology is needed to aggregate resources such as server resources, storage resources, and networks. In the process of building a cloud computing infrastructure, it is necessary to regard the construction of resource pools as a basic link, and focus on building computer resource pools, storage resource pools, and network resource pools.

3. Three-dimensional construction of big data security protection system

3.1. User dimensions

In the cloud platform, users can achieve instant interactive communication. To build a big data security protection system from the user dimension, it is necessary to emphasize different categories of users, and to place different categories of users in different security management domains. Within each management domain, users have corresponding internal resource usage rights, and internal resources can be managed accordingly. When users need to perform internal resource

operations across regions, user authentication and authorization are required to ensure access rights management. Based on the user's demand for resource usage, and the cloud platform itself is dynamic and open, from the user dimension, when constructing the security protection system, the security protection technologies that should be used include authentication and authorization technologies, and access control technology, user behavior trust management technology, etc.

3.2. Data dimensions

The traditional data processing process requires the coupling of data and infrastructure, and the emergence of cloud computing has formed a powerful data center, which can automatically collect and store data, and at the same time, can intelligently calculate and analyze data. Based on this, under the information technology, for the construction of the big data security protection system, it is necessary to strengthen the security protection of the data center. In the big data platform, the whole process of data processing mainly involves data collection and storage, and calculation. Therefore, when constructing the data dimension security protection system, it needs to be from the data collection layer sub-dimension and big data storage and computing platform. The computing platform sub-dimensions are controlled separately.

3.2.1. Data acquisition layer security protection technology

At the data acquisition layer, the key to doing a good job of security protection lies in the following four points: First, we must strengthen the collection and verification management. It is necessary to strengthen the verification of the collected objects and the collected data sources to improve the reliability of the collected objects and the collected data sources. Second, it is necessary to do a good job of data screening management. The data screening work should be connected with the data review work. The suspicious data discovered through data review, including erroneous data, abnormal data, duplicate data, malicious code and viruses, should be transmitted to the data filtering level and realize the security of suspicious data delete or convert. When the conversion is performed, the data is processed to meet the data usage requirements, and the processed data source is stored; at the data classification storage level, the data needs to be identified. In the identification, the data classification storage hierarchy needs to set the classification criteria, including the format, content, etc., after the identification is completed, the classification and storage, so that the entire data resource library is more orderly; finally, the data label management should be strengthened. After the data identification is completed, the data needs to be label-managed. Generally, the security data identifier is clearly defined according to the format and label of the embedded object, which can ensure the security benefits of the stored data and provide support for data security control.

3.2.2. Big data storage and computing platform security protection technology

For the security protection of big data storage and computing platforms, the following links need to be strengthened: First, data storage isolation control. In this link, we must use distributed storage software, and use the data identification method to classify and identify the data, and then store it in the corresponding logical storage area, so as to effectively store and isolate the data; Strengthen data desensitization control. In the process of enterprise operation, privacy data protection needs to be done, and data desensitization technology is to prevent privacy leakage by processing private data. Commonly used data desensitization methods include data randomization and hiding association rules. For personal privacy information, the commonly used data desensitization method is anonymized. However, with the increasing complexity of the network environment, in the desensitization of data, comprehensive data desensitization should be the main method; third is data encryption and decryption technology. The information security of big data needs the support of encryption and decryption technology. In the security protection process, the commonly used encryption policy level is secondary protection, which can protect all aspects of data uploading; the fourth is to perform data integrity verification. The main purpose of verification is to check whether there are data theft, tampering, loss, etc. In the specific verification process, the method used is mainly based on the combination of algebraic signature and erasure code. The reliability of storage

data of cloud big data is guaranteed; the fifth is data fine-grained access control technology. When applying this technology, the technical principle is to authorize and manage fine-grained access by means of the attribute access control model. This technology has high flexibility in application, can adjust access rights according to different needs of users, and improve authorization management targeted; the last is data operation audit control. In the process of security protection of big data storage and computing platform, it is necessary to audit and supervise the execution process of various security protection means, including data encryption and decryption, fine-grained access control, etc. Through scientific audit monitoring, it can ensure timely discovery sudden situations, and try to avoid security issues such as data leakage.

3.3. Basic dimension

The basic dimension of the big data security protection system refers to the infrastructure such as the basic network and the application system server. When the security protection system of the basic dimension is constructed, it needs to be improved from the basic network sub-dimension and the application system service sub-dimension.

3.3.1. Basic network security protection technology

In the security protection of the basic network, it is necessary to strengthen the control of the following links: First, address binding. To strengthen the IP planning of the underlying network, the IP address and MAC address are effectively bound on this basis; the second is redundant backup. At the peak of data access, instability of big data platforms is prone to occur. At this point, you need to adopt the corresponding technology to achieve redundant backup. Commonly used methods include link aggregation and device hot backup. The third is to install a firewall. To install the firewall between the Internet access point and the demilitarized zone (DMZ zone), you should also install the firewall between the internal networks of the DMZ zone, between the system and the untrusted network, and the wireless network. Finally, increase traffic. Monitor and continuously improve the traffic monitoring system, and discover and stop the DDOS attack phenomenon in time.

3.3.2. Application system server security protection technology

In the big data platform system, the application server is a basic system component, generally composed of a host, and can support the normal operation of the cloud server, the operation management system, and other application systems. The main points of security protection for the application system server are as follows: First, the system security protection should be strengthened. To install the corresponding protection software in the system, to achieve timely removal of viruses and malicious code, and to closely monitor the illegal intrusion behavior, strengthen the early warning mechanism; second, strengthen the system security reinforcement. The specific reinforcement method is to perform port maintenance and patching maintenance on the basis of comprehensive security assessment; third, system access control should be strengthened. Common access control methods include account management, identity authentication, and remote control.

4. Big data platform access control technology

The access control technology of the big data platform is mainly 4A (Account, Authentication, Authorization, Audit) and other technologies. The purpose of access control is to strengthen security protection. The main control links are account number, authentication and authorization management, and at the same time, data identification, Security auditing and agent engine functions. The ultimate goal of secure access control technology is to integrate management of each link and form unified management data to achieve full access protection. The specific implementation is shown in Figure 1 below.

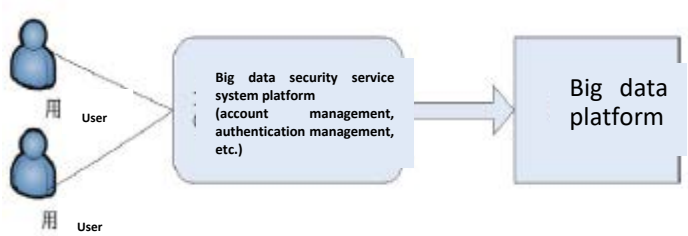

Figure 1 Schematic diagram of security access control for big data platform

The first is account management. At this stage, centralized management of big data application accounts is required to effectively control the management of managed resource accounts, including account creation, deletion, and synchronization management. At the same time, account passwords can be controlled; Certification management. For the big data platform, a unified security certification system should be established, and a targeted authentication method should be established to ensure that the authentication method is diversified and meets the certification strength requirements; Emphasis is placed on strengthening the authorization management of different roles, and at the same time, authorizing the management of application system resources. In the authorization management process, it is also possible to perform authorization management for a specific role with a specific IP or a specific instruction set for a specific role; the next step is data identification and access restriction management. The essence of data identification lies in the classification and identification of the data of the big data platform, and the identification of the completed data should be marked with the security data label and stored in the data resource library. On this basis, the classification data can be further linked with specific roles to achieve access restriction management; in the access control technology, there is also a key link, namely security audit. The main object of security audit is the platform operation and maintenance process. At the same time, the access behavior of the big data platform should be controlled, and it should be controlled from the agent layer to closely monitor user behavior and obtain audit data. When security issues arise, they can provide an important basis for the identification of security responsibilities; finally, agent engine management. When accessing big data platforms, you need to set up a unified portal, generally a big data security service system platform. In the process of accessing resources, the proxy engine can be used for mapping, and when the user performs operations, it needs to be forwarded through the proxy engine. In this way, effective control over the behavior of the user accessing the big data platform can be realized.

5. Conclusion

Information technology has become an important support for national development, and is of great significance for realizing industrial innovation and improving industrial competitiveness. In the application of information technology for industrial upgrading and development, we need to pay attention to the construction of big data platform, rely on big data technology to process massive information, and use the big data platform to achieve information transmission and sharing. As an operation and maintenance personnel of the big data platform, we must pay attention to the security protection needs of data, actively build a big data security protection system, and strengthen the application of security access control technology to effectively avoid big data security issues and promote big data technology in the deep application of industry.

References

[1] Yang Jiwu. Research on Computer Information Security Precautions in the Age of Big Data[J]. Communication World, 2019, 26(03)

[2] Wang Fei. Building a Security Protection System to Consolidate User Data Security [J]. China New Communications, 2019, 21 (04)

[3] Yuan Li, Xu Guiming, Wang Mengxiao. Engineering Design of Security Control for Display and Control Terminal [J]. Network Security Technology and Application, 2018(11)

[4] Zhang Jiansheng, Zhang Xiaohong, Peng Linhua. Computer Network Information Security and Protection Countermeasures under the Background of Big Data[J]. Information and Computer (Theoretical Edition), 2018(20)

[5] Chen Tao. Research on Data Security Protection Scheme of Information System in New Period [J]. Shanghai Construction Science & Technology, 2018(05)

[6] Chen Zhen. Research on the Construction of Big Data Information Security Risk Framework[J]. Information and Computer (Theoretical Edition), 2018(19)