Research on Intelligent Campus Information Security Optimization Path in the Age of Big Data

Yuxiang Long

Information Department, Changchun Medical College, Changchun, Jilin, 130031, China

Keywords: Big data; Intelligent campus; Network; Information security; Optimization path

Abstract: Intelligent campus is a huge and complex system project integrating intelligent education and information. Big data technology provides excellent technical support for it. At the same time, the failure of big data system security protection may also cause the teaching or scientific research information to be maliciously falsified, which directly leads to the failure of teaching and scientific research. Based on the author's learning and practical experience, this work first analyzed the importance of data security on the construction of intelligent campus in colleges and universities, then studied the challenges of intelligent campus big data security, and finally put forward the optimization strategy of intelligent campus information security.

1. Introduction

Cloud computing has become the focus of the construction of intelligent campus in universities, and it is also an effective way to improve the security of public data in universities. Therefore, it is particularly important to share data and ensure data security. At present, the core content of the construction of intelligent campus in universities is to give more protection to data security and vigorously promote data sharing [1]. Cloud technology has entered the intelligent campus and has been widely used in the management of information facilities in schools. However, there are still some defects in the data protection of intelligent campus in universities. Data security has become one of the recognized key issues, so it is necessary to actively explore the data security issues in the construction of intelligent campus [2].

2. The Importance of Data Security to the Construction of Intelligent Campus in Universities

The modern Internet has developed into the main way of information transmission. How to ensure the security of information in the complicated mainstream network has become a key issue to be considered in the current construction of intelligent campus in universities. The relationship between the advantages and disadvantages of data quality plays a crucial role in the construction of intelligent campus in universities. The constant promotion of information construction in universities is inseparable from data decision support, and it also puts forward higher requirements for data quality. With the increasing scale of data and the continuous improvement of data services, data collation and statistical analysis have been widely used in education departments, scientific research management institutions, university services, etc.

3. Big Data Security Challenges Faced by Intelligent Campus

3.1 Authenticity of data cannot be guaranteed

In the cloud era, the authenticity of data in the construction of intelligent campus in universities cannot be guaranteed, and data distortions have emerged. This phenomenon brings a certain threat to the construction of intelligent campus in universities. Some criminals falsified data information through the network, which infiltrated the university database, and the information illusion appeared. The relevant operators are misled by the wrong data when the security awareness is not strong, and it is easy to make a wrong decision, which is not conducive to the better development of the intelligent campus construction in universities.

DOI: 10.25236/mmmce.2019.019

3.2 Disclosure of privacy information

In the era of big data, the construction of intelligent campuses in some universities in our country is facing the problem of privacy leakage. The network is like a mirror. Some hacker organizations can use the network to spy on relevant information in university databases at any time, and use machine learning to conduct data mining [3]. They obtain data that is beneficial to them, which leads to the leakage of private information in the construction of intelligent campus in universities. It not only affects the smooth development of intelligent campus construction, but also brings unpredictable losses to universities.

The hacker organizations mainly attack the data of experimental information, consumption, student employment management information, etc., which are closely related to the construction of intelligent campus in universities and belong to sensitive data. For example, APT attack has a strong latent and advanced persistence, so it can be used to attack the target locked in the campus of universities, and remote control tools can be installed, which can trigger the occurrence of data leakage events in the educational information network of universities.

4. Intelligent Campus Information Security Optimization Strategy

4.1 Data acquisition security technology is large

Data use distributed technology to collect big data. In the process of collection, there may be hidden dangers and threats such as data damage, data loss, data leakage and data theft. Security mechanisms such as identity authentication, data encryption and data integrity protection should be adopted to ensure the security of the collection process.

4.2 Data storage security technology

First, the encryption of big data storage is mainly through cloud storage technology to store various data resources. In the cloud environment, the encryption of big data must adopt homomorphic encryption algorithm, due to the big data is cut into 64MB of small data blocks by the cloud file system, and the data originally encrypted with traditional encryption cannot be decrypted with the decryption key [4]. The homomorphic encryption algorithm is reversible and can achieve both encryption and decryption. Data encrypted using homomorphic encryption technology can still produce correct results during operations such as retrieval, comparison, access, analysis, etc.. In the whole operation process, it is not necessary to decrypt the encrypted data, which fundamentally solves the security of the big data storage and its operation.

Second, the purpose of data backup, recovery, and concurrency control is to prevent the loss or damage of important data caused by system failure or attack. The data recovery and recovery mechanism and concurrency control mechanism ensure that the recovered data is consistent with the original data. The transaction log is used to ensure the integrity and recoverability of the modification, and the security protection of data storage is realized.

4.3 Data transmission security technology

First, the purpose of data confidentiality detection is to detect whether the data transmitted during the communication of sensor network in the Internet of things is encrypted or not. Due to the network nodes of the wireless sensor network are exposed to the external environment, the wireless receiving device can easily receive the data signals sent by the nodes within the receiving range. If the communication between nodes is non-encrypted, it will inevitably cause leakage of communication data [5]. Therefore, it is necessary to detect the confidentiality of the communication data, capture the data transmitted in the sensor network with a professional capture device, and then parse the frame according to the protocol. It is judged whether the communication is in the ciphertext form. If it is not ciphertext, the non-encrypted data is backtracked, and the unencrypted data is encrypted to ensure that the important data is wirelessly transmitted in ciphertext form.

Second, data integrity and consistency detection data are missing or illegally tampered with during transmission, and the consequences are unimaginable. Data integrity and consistency detection can be conducted by analyzing the captured data packets and analyzing the frames to find the fields that guarantee the integrity of the data, accurately identify the defective or tampered data, and discard them. It is required to retransmit the original data to ensure that the data received by the receiver is the original data.

Third, data network filtering uses network filters to monitor the transmitted data. Once the identified data leaves the authorized user network, it automatically blocks the data transmission and effectively avoids data leakage.

4.4 Data distortion technology

The technology needs to perturb the data to make the data distorted, so that the attacker can not restore the original real data according to the distorted data, and realize the hiding of the real data. Data mining security technology is the core of big data application, and it integrates theories and technologies in many fields, such as database, artificial intelligence, machine learning, statistics, high-performance computing, pattern recognition, neural network, data visualization, information retrieval and spatial data analysis [6]. Through data analysis and mining, all kinds of hacker attacks, illegal operations, internal and external threat sources and other security events are mined from big data, and security alarms and dynamic responses are issued in time. If you use the deep learning algorithm to analyze the big data in multiple dimensions, you can find all kinds of potential low-level local features, regional combination features and high-level overall features of the attacker.

4.5 Data publishing security technology

First, security audit is a complete recording, management, classification and storage of events, and afterwards analysis, query and statistics of the collected security events, as well as mining the underlying knowledge model behind the data, which is used for subsequent intrusion detection (discovering potential attack behaviors, etc.). Its core role is to accurately record the attack behavior, trace the security incident and find out the attribution of the accident liability.

Second, data traceability has undergone rigorous security audits, and there may be omissions. After the release of data, once data security problems such as leakage of confidential and private information are found, the security protection system must have a data traceability mechanism, which can quickly trace back to the link where the problem occurred, accurately locate the link where the problem occurred, quickly block the leakage link, trace the responsible person and prevent similar problems from happening again. Such as the use of digital watermark technology for data trace-ability [7].

4.6 Guard against Advanced Persistent Threat

Advanced Persistent Threat has strong concealment, long-term latency, continuous attack, uncertainty of attack path, advanced attack technology and great harm to information security. The clear purpose of APT attacks is to steal confidential information from the target organization [8]. The APT attack generally adopts the 0day vulnerability acquisition authority, and its efficiency and capability are significantly higher than ordinary attacks, and the attack methods and technologies are constantly evolving. In the big data application environment, the security threat of APT attacks is more prominent [9]. With the help of big data technology real-time and efficient processing capability, the security auditing scheme for real-time detection and comprehensive monitoring of collection behavior can be designed, and big data is generated by intrusion detection system log files, and timely use of countermeasures to effectively resist APT attacks.

5. Conclusion

In the era of big data, the construction of intelligent campus in universities has been widely used. In order to actively respond to the challenges of the big data era, universities need to improve data security, strengthen system management and supervision, ensure that data in intelligent campus construction is not stolen, actively create a harmonious internal network environment for universities and give full play to the advantages of cloud computing. Intelligent campus makes education become intelligent at the same time, its big data security is facing unprecedented challenges, the construction of intelligent campus security protection system is very important. Through systematic analysis of the security problems existing in the acquisition, transmission, storage and audit of big data in intelligent campus, this work proposed corresponding security strategies and constructs a complete big data security protection system to ensure the normal operation of intelligent campus.

References

[1] Hu, H. , & Long, D. . (2016). A study on key techniques of wisdom campus information recommendation platform based on big data. International Conference on Intelligent Transportation. IEEE.

[2] Ma, X. X. , & Wu, D. . (2014). Research on information security issues facing the era of big data. Applied Mechanics and Materials, 651-653, 1913-1916.

[3] Wei, L. , Daoping, Y. , Yan, J. , & Maoqiang, Y. . (2015). The Era of Big Data Information Security Issues to Explore. Sixth International Conference on Intelligent Systems Design & Engineering Applications. IEEE Computer Society.

[4] Li, Y. , Gai, K. , Qiu, L. , Qiu, M. , & Zhao, H. . (2016). Intelligent cryptography approach for secure distributed big data storage in cloud computing. Information Sciences, S0020025516307319.

[5] Gang, W. . (2015). Information Use and the International Intellectual Property Protection in Big Data Era. 2015 International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS).

[6] Hu, H. , & Yan, H. . (2016). A Study on Discovery Method of Hot Topics Based on Smart Campus Big Data Platform. International Conference on Intelligent Transportation. IEEE Computer Society.

[7] Xhafa, F. , & Barolli, L. . (2014). Semantics, intelligent processing and services for big data. Future Generation Computer Systems, 37, 201-202.

[8] Gai, K. , Qiu, M. , & Elnagdy, S. A. . (2016). Security-Aware Information Classifications Using Supervised Learning for Cloud-Based Cyber Risk Management in Financial Big Data. 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS). IEEE.

[9] Yan, H. , Hu, H. , Yan, H. , Hu, H. , Yan, H. , & Hu, H. . (2016). A Study on Association Algorithm of Smart Campus Mining Platform Based on Big Data. International Conference on Intelligent Transportation. IEEE Computer Society.