Journal of Electronics and Information Science (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/jeis.2024.090212
ISSN 2371-9524 Vol. 9 Num. 2

Research on Network Information Security Control in the Big Data Era

Mingming Xu

Zhejiang Anyong Testing Technology Co., Ltd., Ningbo, Zhejiang, 315100, China
routeming@163.com

Keywords: Big Data; Network Information Security; Information Control

Abstract: With the rapid development of big data technology, computer networks have permeated all aspects of daily life, enriching information resources and communication methods effectively. However, this has also made computer network information security issues increasingly complex and severe. Ensuring the security of data information is therefore of greater significance for various network information security issues in the context of big data. This paper starts from the perspective of the three elements of environment, and technology in network information security control in the context of big data, and puts forward corresponding suggestions and strategies for network information security work, providing a reference for the development of network information security work and promoting effective implementation of network information security work in the context of big data.

1. Introduction

With the arrival of the 21st century, the rapid progress and vigorous development of Internet technology have ushered human society into a flourishing era of big data. The application of big data technology not only provides strong technical support for the in-depth mining of data but also brings various concerns, such as network system failures, information leaks, and many other cybersecurity issues[1-2]. Despite the elevation of cybersecurity control to a national strategic level, the vulnerability of China's cybersecurity foundation cannot be ignored, leading to a rising number of cybersecurity incidents year by year, posing unprecedented challenges to China's cybersecurity. In this context, ensuring the security of network information in the era of big data has become particularly urgent and crucial. Faced with this significant challenge, we must adopt a more vigilant approach, a firmer determination, and comprehensively utilize technical means, policies, and regulations to strengthen the protection of network information security from all aspects, ensuring the integrity of data, the stability of networks, and the security of information, thereby promoting the healthy development of the big data era.

2. The importance of information security

The era of big data has turned data information into a significant resource, presenting new challenges in network information security. With the continuous growth of data, there is a rising trend of security risks in big data, especially as the future competitive edge in the interconnected network shifts towards big data. Consequently, network information security issues under the umbrella of big data have become more severe.

Big data poses a significant threat in terms of network attacks due to its massive data scale stored in a distributed manner in the cloud. This form of storage makes data protection relatively simple, leaving vulnerabilities prone to exploitation by hackers. Advanced Persistent Threats (APTs) can easily implement high sustainability threats, leading to information security issues. Within the big data environment, the large number and diverse composition of end-users make it challenging for security inspection systems to promptly and accurately determine the legitimacy of network users. This complexity creates a conducive environment for APT attacks, making it difficult to effectively monitor and detect APT threats, which is a major reason for the heightened network security risks in the context of big data [3-4].

Furthermore, big data's capability to aggregate and store all network users' data creates a security vulnerability in the protection of users' personal data privacy. Without robust security mechanisms, improper handling of personal data may result in privacy breaches. Safeguarding the privacy of individual users' data in the realm of big data necessitates robust data analysis technologies and well-established privacy protection mechanisms to enhance data security levels. Issues may arise in defining or allocating user ownership and access to sensitive data if the data management mechanisms at the big data management end are inadequate, potentially leading to data security breaches.

In addition, the nature of data storage in big data presents inherent risks. The exponential growth rate of data in big data storage platforms and the concurrent operation of various types and structures of data in an unordered manner can result in misalignment and chaotic data management, laying the groundwork for security vulnerabilities during the storage and subsequent processing of big data. The capability of current big data storage management systems to meet the demands of storing massive amounts of data remains a subject for scrutiny, revealing significant security risks in big data storage.

3. Methods

(1) Network attack detection method based on machine learning

With the rapid development of network technology, the means of network attack are becoming increasingly rampant and more hidden, and the traditional means of network security defense gradually appear inadequate and can no longer meet the needs of the current changing network environment. Because of this, the exploration and research of network attack detection method based on machine learning has become one of the focuses of network information security field[3-4]. This machine learning-based network attack detection method, as an adaptive, dynamic and nonlinear detection method, shows excellent robustness and scalability. The core idea is to efficiently capture the clues of network attack behavior through feature extraction of network traffic data and intelligent classification of training data, so as to effectively ensure network security. The innovation of this method is that it can use machine learning algorithms to conduct deep learning analysis of network traffic information and realize intelligent network attack detection and response, which will give a new development prospect and application potential for the field of network security[5].

(2) Threat intelligence analysis method based on deep learning

In the era of big data, network security is facing various threats and challenges. In order to realize the security control of network information, deep learning, as an important machine learning technology, is being widely studied and applied. The threat intelligence analysis method based on deep learning can effectively improve the network security defense capability. Through deep learning technology, a large number of network data can be learned and analyzed, and the rules and patterns can be automatically extracted. For various network attacks, such as DDoS attacks and SOL attacks, deep learning-based threat intelligence analysis methods can quickly identify them and take appropriate security defense measures in time[6]. In practical applications, threat intelligence analysis methods based on deep learning need to build corresponding deep neural network models and train the models to classify different types of cyber attacks. For different network attacks, it is necessary to collect a large amount of network data, carry out feature extraction and annotation for model training and testing. In the process of model training, it is necessary to combine the existing security defense knowledge and apply it to the deep learning model to enhance the learning ability and discrimination ability of the model.

(3) Network information security control method based on blockchain

As a decentralized, immutable, safe and reliable new technology, blockchain is widely used in the financial industry, government management and other fields. In terms of network information security control, blockchain also has unique advantages and application prospects. First, blockchain uses a decentralized, distributed storage method that does not rely on a single entity or organization, preventing the possibility of information being tampered with or deleted. Second, blockchain guarantees the privacy and security of data through cryptography[7]. The data can only be accessed by authorized persons, ensuring the security of the information.

(4) Network security defense methods based on cloud computing

The method of network security defense based on cloud computing mainly refers to the method of network security defense using cloud computing technology. The specific realization process is to provide the resources required for network security prevention to users in the form of services through cloud computing technology, so as to share the cost of security protection, improve security performance, and quickly respond to network security incidents. In this approach, cloud computing technology can provide powerful computing power, storage capacity, bandwidth capacity to ensure network security. At the same time, cloud computing also provides multiple rounds of security protection to ensure the highest level of control. The network security defense method based on cloud computing can monitor, warn and deal with network attacks in real time to protect the security of network resources. This method can not only improve the ability of network security protection, but also help the network system in time when the network is abnormal. The network security defense method based on cloud computing has the advantages of low cost, high performance and easy expansion. It is a security control method suitable for large-scale network systems.

4. The control strategies

With the advent of the era of big data, while improving the value of data mining, network security issues have also been put on the agenda, and the requirements for data security are higher than in the past. Therefore, actively catering to the development environment of big data has become a task that we must complete. While fully mining and utilizing a variety of massive data, we should effectively take countermeasures to actively defend and actively breach various network information security problems. Therefore, it is extremely necessary to pay attention to the construction of big data information security system, which can promote the continuous improvement of dynamic data security monitoring mechanism, accelerate the research and development and application of big data security technology, use access control and data encryption technology to improve the security of big data information, so that the economic and social value of big data can be effectively integrated and fully mined. So that big data can really play an important driving force to promote social and economic development. Through the establishment of network information security control mechanism and evaluation system, it can provide guidance for network information security control under the background of big data from both theoretical and practical perspectives, and improve the effect of network information security work. Starting from the three elements of network information security, this paper puts forward corresponding strategies for network information security control under the background of big data.

4.1 Personnel Perspective

(1) Pay attention to network user information behavior

First of all, the information security of network users is the focus of network information security under the background of big data. Only by effectively protecting the information security of network users can we create a psychological understanding of network trust and willfulness for users and promote their Internet use behavior. Secondly, network users, as the management objects of network information security, should carry out necessary education and training as well as guidance and protection on their network behavior, so as to ensure that they fully participate in network information activities, standardize their network behavior, and maintain network information security from the perspective of management objects.

(2) Attach importance to the security responsibilities of network information service providers

Network information service providers shoulder important responsibilities in network information security. For network service providers who fail to fulfill their data protection responsibilities, they should be punished according to the degree of their failure, including administrative penalties such as criticism of violations issued by the network information security authorities, ordering corrections, administrative fines, and revocation of business qualifications. At the same time, the user whose personal data is damaged has the right to claim civil damages to the network service provider; At the level of criminal law, Internet service providers should be included in the subject scope of the crime of infringing citizens' personal information, and the specific criteria for determining "serious circumstances" should be clarified.

(3) Cultivate high-quality network security managers

Under the environment of big data, network information security needs the support of technologies that adapt to the characteristics of The Times, and the holders of technologies are highly knowledgeable talents. Information security is a relatively narrow professional, wide knowledge involved, and high professional requirements, so the requirements for relevant talents are very strict. The shortage of network information security talents in our country makes it urgent to accelerate the training of information security talents. At the level of talents and science and technology, we must increase the relevant investment in the field of information science and technology, train network security and information technology talents with high professional quality, and build a professional team of network information security work. It is not only necessary to train network information security talents with high professional skills, but also to train talents with independent technological innovation ability, so as to lay the foundation for improving network infrastructure.

4.2 Environment Perspective

(1) Emphasizing the Construction and Maintenance of Network Infrastructure

It is essential to focus on the construction and maintenance of network infrastructure and utilize various security technologies to protect network information systems and databases. By making full use of security mechanisms in database systems, application systems, and network systems, a comprehensive and professional network information security system should be established and maintained. While strengthening the development of external hardware facilities, effective security management of internal networks and databases should be conducted to ensure the security of stored information. Additionally, it is crucial to have a proactive security awareness, establish disaster recovery backup systems, provide information security protection from the architecture of the network information security system. Implementing a distributed data storage system, managing data in a decentralized manner, establishing local backup systems to ensure the security of critical data and the stable and reliable operation of data centers[8]. Moreover, besides ensuring data centers can avoid network attacks, they should also prevent data loss caused by natural disasters such as earthquakes, fires, or other human-made disasters.

(2) Establishing Network Information Security Evaluation Standards

Establishing network information security evaluation standards aims to provide a basis for network information security work, facilitating the regulation of network information security work with unified standards. Currently, there are various existing network information security standards issued by different departments with different reference standards and scopes, leading to a situation where multiple standards coexist, hindering further progress in the work.

(3) Enacting Network Information Security Regulations

Since the 1990s, China has successively introduced multiple laws, regulations, and measures related to internet information security, such as the "Computer Virus Prevention and Management Measures," "Internet Network Security Information Reporting Measures," and "Computer Information Network International Interconnection Security Management Measures." These regulations and measures have stipulated and standardized activities of internet entities from various aspects. Internet information security has garnered significant attention in China's legislative field, indicating the establishment of a fundamental framework for legislation on internet information security [9].

4.3 Technical Perspective

From a technical perspective, big data security technology can protect network information from various angles such as physical security, system security, network security, storage security, access security, audit security, and operational security. Throughout the lifecycle of big data, encompassing stages like data generation, collection, transmission, storage, processing, analysis, publishing, display, and application, big data security technology can provide security protection for network information at any stage. By leveraging existing big data security technology, it is possible to maximize the security of big data itself, preventing issues like data leakage, unauthorized access, data tampering, data loss, key exposure, and infringement of user privacy. Therefore, designing and building more technical standards, security specifications, tools, products, and security services are necessary forms to safeguard the security of big data. Relying on relevant tools, applying certain security strategies, establishing a comprehensive model for big data information security, and ensuring the security of data information are all part of big data information security technology.

The fluidity and openness characteristics of big data have led to a high frequency of risks related to network information leakage or illegal exploitation in the context of big data. Continued innovation in technological means is a key method to protect network information security. With the rapid development of new technologies such as cloud computing, the Internet of Things, and mobile internet, new security challenges have emerged for the collection, processing, and application of big data. However, the pace of technological development still lags behind, and core key technologies remain in the hands of foreign network information service providers, highlighting a lack of independent innovation in China's information industry technology. Therefore, emphasizing independent innovation in network information security technology and increasing investment are crucial directions to ensure the future security of China's network information.

5. Conclusion

The arrival of the big data era highlights the value of information and data, making network information security a hot topic of concern. To better serve people with computer network information technology, it is necessary to strengthen the management of computer network information security. Therefore, relevant departments must prioritize the maintenance of computer network security, conduct effective network security education, and standardize user operations. Users also need to understand the application of network information security technologies, utilize firewall technology, antivirus software, encryption technology, etc., to protect computer network information, prevent security issues, and meet the needs of people's daily lives.

References

[1] Benaroch M, Chernobai A, Goldstein J. An internal control perspective on the market value consequences of IT operational risk events [J]. International Journal of Accounting Information Systems, 2012, 13(4):357-381.

[2] Gu Wenhua. Research on Legislation of Network Information Security [D]. Inner Mongolia University, 2012.

[3] Zhao Xiaoyu, Liu Tingting. Research on Network Information Security in the era of Big Data [J]. Computer and Network, 2019(11) : 51

[4] Chen Shuhong. Discussion on Network Information Security and Protection in the Era of Big Data [J]. Network security technology and application, 2021(8): 167-168.

[5] Zeng Desheng, He Jian, Ning Jianfei et al. Analysis of Computer network information security protection strategy in the era of Big Data [J]. Software, 2022, 43 (9): 64-66.

[6] He Yarong. Research on Enterprise Information Security Management System in the era of Big Data [J]. Communications World, 2020, 27(07):105-106.

[7] Zhang Jing. Research on Network Information Security Control in the Era of Big Data [J]. Shanxi Electronic Technology, 2024, (01):119-122.

[8] Tian Qiu. Discussion on Computer network Information Security in the era of Big Data [J]. Office Automation, 2024, 29(04):36-38+8.

[9] Zheng Yuze. Computer Network Information Security and protection Strategy based on Big Data technology [J]. Information and Computer (Theoretical Edition), 2018, 36(02):218-220.