Advances in Computer, Signals and Systems (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2024.080310
ISSN 2371-8838 Vol. 8 Num. 3

Application Analysis of Computer Information Security under Big Data

Keke Zhang

Khoury College of Computer Science, Portland 04101, ME, United Stated
zkarena2209@163.com

Keywords: Internet Technology, Big Data Technology Application, Computer Information Security

Abstract: With the wide application of Internet technology, the application scope of big data technology in all walks of life is expanding. The widespread use of the Internet has led to the generation and accumulation of massive data, which is not only a valuable information resource, but also a challenge to information security. In the current big data environment, computer information security faces many key technologies and challenges, such as data privacy protection, network attack prevention, identity authentication, and so on. To address these challenges, this article will focus on exploring the application of big data technology in the field of computer information security. In the big data environment, data storage, transmission, and processing face more complex security issues. At the same time, the application of big data technology also provides new possibilities for information security, such as security event detection and response systems based on big data analysis and network intrusion detection systems based on behavior analysis. Through in-depth analysis and effective protection strategies in this article, the aim is to provide practical references for related research and promote the continuous development and innovation in the field of computer information security. In the research, we will further explore the integration of big data technology with emerging technologies such as artificial intelligence and blockchain to address the increasingly complex challenges in the field of information security and achieve a positive interaction between information security and technological innovation.

1. Introduction

As societal development and economic standards advance, the emergence of computer networks has changed the way of life, but information security issues still need to be strengthened protection and management [1]. Faced with a huge amount of data, a variety of large data sets, processing speed of the new data environment. The evolving landscape not only significantly impacts multiple sectors, enhancing convenience in daily life and work processes, but also introduces heightened security challenges to the computer network environment [2]. These hurdles encompass not only individual privacy and asset protection but also extend to critical national security and societal stability.

As Internet technology and big data become increasingly prevalent,we are increasingly concerned about data security and privacy issues. The rapid development of big data brings new challenges to the field of information security, but also provides us with opportunities to explore new solutions. Computer information processing technology represents a significant advancement in China's scientific and technological information sector, playing a crucial role in driving social development [3]. Hence, this paper seeks to delve into the fundamental technology of big data in computer information security and propose relevant protective strategies, and provide useful reference and guidance for the further development and practice of information security field.

2. Related Research

The emergence and widespread adoption of the big data era have elevated data security to a paramount concern. X Yu analyzed data security threats in computer networks [4] and proposed corresponding governance strategies. LL Xing reviewed analyzing China's network security governance policies through the lens of big data, and put forward optimization suggestions [5] to provide references for policy improvement. Z Wang used data mining and big data technology to build a public security information analysis system to quickly analyze police data, provide a basis for public security decision-making [6]. X Li proposed a network security framework, developing an efficient security model leveraging artificial intelligence technology,and verified its feasibility and effectiveness through typical cases [7].

3. Key Technologies of Computer Information Security in Big Data Environment

3.1 Big Data Backup

Managing data backup in the context of big data is a crucial aspect of data management, focusing on efficiently and reliably handling vast amounts of data backup needs. The primary goal is to maintain the integrity, reliability, and recoverability of backed-up data. This challenge has spurred ongoing advancements and implementations of technology in this domain, and distributed storage and distributed file system have become the basic framework of big data backup. Distributed architecture can utilize the method of decentralized storage of data on different nodes to achieve parallelization and expansion of backup operations. This can effectively solve the problems of single point of failure and large data volume.

In big data backup, we find that data redundancy and fault tolerance mechanisms are very important. To ensure the reliability and fault tolerance of backup data, backup systems are usually able to quickly recover in the face of node failures or data corruption. By combining incremental backup and differential backup strategies, we can achieve the goal of reducing the redundancy of backup data and storage costs. Incremental backup only backs up the data that has changed, while differential backup can back up different data blocks from the previous backup. Therefore, different methods can achieve different improvements in backup efficiency and save storage space.

The security mechanism ensures the confidentiality and integrity of backup data through security measures such as data encryption and access control, which can effectively prevent data leakage or tampering, increase the security and credibility of protecting backup data.

3.2 Cloud Computing Technology

Artificial intelligence technology also involves the technology of indexing, storing and retrieving multimedia data such as images, video and audio. The development of technology enables users to obtain relevant text or other multi-media data through multimedia information such as images, audio or video, which can be more convenient to obtain the required information. When using the search engine, only need to search the picture directly stick to the search bar, the system can use the file recognition technology to analyze the picture, provide relevant parameters and source information. Intelligent AI technology can also be used for various intelligent processing of images, such as removing watermarks, so as to meet personalized search needs. Cross-language retrieval is a technique for information retrieval between different languages. With the increasing frequency of global information exchange, cross-language retrieval technology has attracted more and more attention. It can help users retrieve relevant information in different language environments and promote cross-cultural communication and information sharing.

4. Analysis of Problems Faced

Computer network security is faced with many challenges, and network security management and protection measures must be strengthened to improve network security [8].

Hacker intrusion is one of the main problems facing computer network security, mainly because big data systems contain a large amount of sensitive information and important data. Hackers can carry out network attacks through various attack methods, such as vulnerability exploitation, denial of service attacks, etc. This may result in data leakage, tampering, or service interruption for users, causing serious losses to businesses and individuals.

Virus intrusion is also one of the important issues in the application of big data technology in computer information security. Viruses can spread by infecting files, applications, or network transmissions in the system. Suffering from virus attacks can lead to damage to data integrity, decreased system stability, and even cause certain privacy leaks and network security threats.

The act of obtaining, collecting, or copying sensitive information or confidential data from others or organizations without authorization is called information theft, and the information leaked here includes personal identity, financial and trade secrets, etc. It is usually carried out by hackers and cybercriminals through illegal means, such as exploiting network vulnerabilities, malicious software, etc.

The security of big data systems still faces the problem of system vulnerabilities. Most big data systems have software vulnerabilities or security risks, which may exist due to software design flaws, configuration errors, or untimely updates. Hackers can exploit these issues to invade systems, which can lead to security issues such as unauthorized access, data leakage, or service interruption. Protecting the security of big data systems requires us to promptly discover and fix these vulnerabilities, security officers continuously strengthen system security audits and monitoring, and the country implements strict access control and permission management.

5. Effective Information Security Protection Measures in Response to Identified Issues

The key to maintaining the security of big data systems lies in establishing a complete firewall. Firewalls are the primary line of defense at network boundaries, and by monitoring and managing network traffic, they can effectively curb unauthorized access and malicious attacks. By implementing security policies such as access control, application layer filtering, and VPN tunneling, a strong security protection barrier can be established. Using firewall technology to protect sensitive data and important information also enhances the security and stability of big data systems.

Linking the use of WAF firewalls and intrusion detection systems is also an effective way to enhance network security. WAF firewall can block common web attacks; Intrusion detection systems monitor network traffic in real-time and promptly detect and handle abnormal behavior. The joint operation of two technologies can achieve more comprehensive security defense, effectively reducing the risk of unauthorized access and malicious attacks, and providing stronger security guarantees for big data systems

The establishment and improvement of a network protection system require a series of proactive measures.

- Comprehensive recording and monitoring of network activities, detailed recording of network activities and real-time monitoring, timely detection and analysis of potential security issues.
- Establish a sound safety incident response and emergency plan, clearly define the responsibilities and response procedures of team members, in order to quickly respond to any safety incident.
- Regularly conduct vulnerability assessments and security audits to maintain ongoing effectiveness. Utilize vulnerability scanning tools and penetration testing to identify and resolve potential issues in the system.
- Strictly implementing security policies and access controls, including password policies, managing user permissions, and network partitioning, can restrict unauthorized access and reduce malicious behavior.
- Continuously strengthen employee training and enhance security awareness, focusing on best practices and risk awareness in cybersecurity, and reducing the risk of human error and social engineering attacks.
- Adopting multi-level defense measures, including the use of firewalls, antivirus software, intrusion detection and prevention systems, to form a comprehensive security protection system.
- Regularly backup important data and establish a disaster recovery plan, store data in a secure location, and conduct regular testing to ensure data integrity and availability.

Through these measures, we can establish a network protection system, effectively reduce data security risks, and protect the confidentiality, integrity, and availability of data and systems.

The importance of ensuring information security is becoming increasingly evident in today's digital environment. To safeguard sensitive information from unauthorized access and theft,information encryption processing has become a key measure.

Choosing the right encryption algorithm is the first prerequisite. Different types of information may require different levels of encryption protection. For highly sensitive data. At the same time, ensure that the encryption algorithm is currently secure and reliable, and avoid using known weak encryption algorithms.

Manage the encryption key well, the security of the key directly affects the security of encrypted information. Adopting a key management system can help securely generate, store, and distribute keys, and ensure key rotation and update.

The scope of encryption must be carefully defined, ensuring that sensitive data is encrypted both during storage in databases and during transmission. At the same time, for scenarios such as mobile devices and cloud storage, encryption protection should also be considered to prevent data from being leaked during transmission or storage.

Strengthen training and awareness raising on encryption technology. All employees who use encryption technology should receive relevant training to understand the principles, use methods and precautions of encryption, and enhance the attention and prevention awareness of information security.

These measures can effectively protect sensitive information from unauthorized access and theft, and maintain information security.

6. Conclusion

In today's digital age and the rapidly developing Internet environment, the problem of computer information security has become increasingly severe and complicated. The rise of big data technology provides us with new opportunities and challenges, and provides a new way and solution for solving information security problems. Through the data processing, analysis and mining of big data technology. Identifying potential security threats promptly enables us to enhance early warning and response capabilities in information security. Big data technology also facilitates the creation of detailed and comprehensive security policies, and controls to strengthen the protection of sensitive data in response to the growing number of cyber attacks and malicious actions. The use of big data technology also presents challenges in ensuring privacy protection, data security and algorithm bias, which requires us to constantly explore and innovate and improve the technical means and strategies of information security to ensure that the digital assets of users and organizations are effectively protected. Your focus on big data technology in information security and privacy protection is crucial given the increasing complexity of security threats. Maintaining the security and stability of the digital world requires continuous attention and effort.

References

[1] Lijiang X. Analysis of Computer Network Information Security and Protection Strategy in the Era of Big Data. Foreign Science and Technology Journal Database (Abstract Edition) Engineering Technology, 2021, 89-97.

[2] Jiang L. The Application Analysis of Computer Network Security Data Encryption Technology. 2020 International Conference on Applications and Techniques in Cyber Intelligence: Applications and Techniques in Cyber Intelligence (ATCI 2020). Springer International Publishing, 2021: 137-144.

[3] Wang P, Hu Y, Huo J. Analysis on the Application of Computer Information Processing Technology under the Background of Big Data. Journal of Physics: Conference Series, 2021, 1881(3): 32052-32059. DOI:10.1088/1742-6596/ 1881/3/032052.

[4] Yu X. Analysis of the Security Strategy of Computer Network Data under the Background of Big Data. 2021 4th International Conference on Artificial Intelligence and Big Data (ICAIBD). 2021. DOI: 10.1109/ICAIBD51990. 2021. 9459026.

[5] Xing L L. Computer Network Security Maintenance and Management in the Era of Big Data. International Journal of Frontiers in Sociology, 2021. DOI:10.25236/IJFS.2021.030113.

[6] Wang Z, Wang J. Applications of Machine Learning in Public Security Information and Resource Management. Hindawi Limited, 2021. DOI:10.1155/2021/4734187.

[7] Li X. Research on Network Information Security Service Model Based on User Requirements under Artificial Intelligence Technology. 2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA), 2023, 1568-1572. DOI:10.1109/ICPECA56706.2023.10075946.

[8] He X. Analysis of Network Intrusion Detection Technology Based on Computer Information Security Technology. Journal of Physics: Conference Series, 2021, 1744(4): 42038. DOI:10.1088/1742-6596/1744/4/042038.