Research on Network Security in the Context of Big Data

Hao Rui

Northern Laboratory (Shenyang) Co., Ltd. Guangzhou Branch Guangdong Guangzhou 510000

Abstract: ***In the context of big data, research on network security is becoming increasingly important. With the surge in data volume, the risks of information leakage, hacker attacks, and network fraud have significantly increased. This article focuses on the challenges and response strategies of network security in the big data environment, including measures such as data encryption, access control, security auditing, and intelligent security protection systems. Through comprehensive analysis and practice, the aim is to enhance the security protection capabilities in big data applications, ensure the security and privacy of data assets, and safeguard the development of informatization.***

Keywords: Big data background; Network security; Strategies and technologies.

1. INTRODUCTION

The rapid development of big data technology has greatly enriched the boundaries of data processing and analysis, while also bringing unprecedented challenges to network security. The surge in data volume, diversification of types, and increased flow speed have made network threats increasingly complex and difficult to predict. This article aims to explore in depth the new situations, problems, and challenges faced by network security in the context of big data, and propose corresponding response strategies, in order to provide strong support for building a more secure, reliable, and efficient network environment. In sports analytics, Zhu, Yu, and Li (2025) proposed SAGCN, a spatiotemporal attention-weighted graph convolutional network integrated with IoT for adolescent tennis motion analysis [1]. For logistics and emergency management, Zhang (2024) applied cohesive hierarchical clustering to dynamically adapt the supply and demand of power emergency materials [2]. The impact of emerging AI on digital ecosystems is examined by Zhou and Cen (2024), who investigated the effects of ChatGPT-like technologies on user entrepreneurial activities [3].

The versatility of graph-based methods is further evidenced in recommender systems, where Yang, Wang, and Chen (2024) developed GCN-MF, a model combining graph convolutional networks with matrix factorization [4]. In computer vision, foundational work by Chen et al. (2022) presented a one-stage framework for object referring with gaze estimation, enhancing human-computer interaction [5]. Concurrently, the global imperative for sustainability drives research like that of Wu et al. (2025), who analyzed how supply chain digitalization and energy efficiency contribute to achieving carbon neutrality targets [6].

A critical technical challenge addressed across these studies is domain adaptation, essential for model robustness in real-world scenarios. Peng, Zheng, and Chen (2023) tackled source-free domain adaptation for human pose estimation [7], while Peng et al. (2023) proposed RAIN, a method applying regularization on both input and network for black-box domain adaptation [8]. This focus on adaptive and interactive systems extends to robotics, as seen in Guo and Tao's (2025) work on modeling and simulation analysis of robot-environment interaction [9]. Finally, in the high-stakes medical domain, We et al. (2025) leveraged multimodal physiological data towards intelligent monitoring of anesthesia depth, showcasing the critical application of integrated data fusion in healthcare [10].

2. OVERVIEW OF BIG DATA TECHNOLOGY AND NETWORK SECURITY

2.1 Fundamentals of Big Data Technology

Big data technology, as an important cornerstone of the information age, profoundly influences various fields of data processing and applications with its unique 4V characteristics - Volume, Velocity, Variety, and Veracity. Volume refers to the enormous amount of data that has jumped from TB level to PB or even EB level, requiring storage and processing systems to have extremely high scalability and efficiency. Velocity emphasizes the speed of data generation and processing, requiring the system to capture and process data streams in real-time or near real time. Variety reveals the diversity of data formats, including structured, semi-structured, and unstructured data, which places higher demands on data processing and analysis techniques. Veracity focuses on the authenticity and quality of data, ensuring that the information extracted from massive amounts of data is reliable and valuable. The key links of big data technology include data collection, storage, processing, and analysis. Data collection technology achieves comprehensive data collection through diverse data sources and efficient data capture tools. Storage technology utilizes innovative solutions such as distributed file systems and NoSQL databases to address the capacity, scalability, and performance issues of big data storage. The processing technology covers two methods: batch processing and stream processing, which are suitable for offline large-scale data analysis and real-time data stream processing, respectively. Analytical techniques rely on advanced algorithms such as data mining and machine learning to uncover hidden patterns and insights from massive amounts of data.

2.2 Basic Concepts of Network Security

Network security refers to comprehensive measures to protect hardware, software, and data in computer network systems from unauthorized access, use, leakage, interruption, modification, or destruction. It covers multiple dimensions such as physical security, system security, network security, and data security. Physical security focuses on the physical protection of network equipment and facilities; System security emphasizes the stability and security of operating systems, databases, and other system software; Network security involves protective measures at the network level, such as network protocols, firewalls, and intrusion detection; Data security is the core of protecting data integrity, confidentiality, and availability. The network security architecture framework is a systematic methodology used to guide the planning, implementation, and management of network security. It usually includes components such as security policies, security management, security technology, and security operations, aiming to build a comprehensive, dynamic, and sustainable network security protection system.

2.3 The Relationship between Big Data and Network Security

Big data technology plays an important role in enhancing network security monitoring, analysis, and defense capabilities. By collecting and analyzing big data such as network traffic and logs, potential security threats and abnormal behaviors can be detected in a timely manner, improving the intelligence and automation level of security monitoring. At the same time, big data technology can enhance the depth and breadth of security analysis, quickly identify and respond to security incidents such as network attacks and malicious software. In addition, prediction models based on big data can also evaluate the security situation of network systems, providing strong support for formulating forward-looking defense strategies. However, the widespread application of big data technology has also brought new security challenges. The centralized storage and processing of big data make it a key target for hacker attacks, and once data is leaked or tampered with, it will cause serious consequences. In addition, the diversity and complexity of big data also increase the difficulty of data protection, and traditional security measures may be difficult to cope with new challenges. Therefore, while utilizing big data technology to enhance network security capabilities, it is necessary to attach great importance to the security risks it may bring and take corresponding protective measures to ensure network security in the big data environment.

3. CHALLENGES FACED BY NETWORK SECURITY IN THE CONTEXT OF BIG DATA

3.1 Risk of Data Privacy Leakage

Privacy protection is particularly prominent in the entire chain of big data collection, storage, and processing. Firstly, there is a risk of privacy breaches during the data collection phase. Some companies, in pursuit of commercial interests, collect personal information on a large scale without the consent of users, even including sensitive data such as personal financial and health conditions. This not only violates users' privacy rights, but also lays hidden dangers for subsequent data leaks. Secondly, security vulnerabilities in data storage processes are also a major threat. The centralized storage of big data increases the risk of illegal access and theft of data, especially when storage system protection measures are not in place, hackers can easily obtain large amounts of sensitive data. Finally, in the process of data processing, without effective privacy protection mechanisms such as data anonymization and anonymization, users' privacy information may also be inadvertently leaked.

3.2 Advanced Persistent Threat (APT)

APT attacks pose a serious threat to network security in the big data environment due to their high concealment, long duration, and strong targeting. APT attackers often possess highly specialized skills and resources, and can lurk in the attacked network for a long time, gradually infiltrating through carefully designed attack chains, ultimately achieving the goal of stealing sensitive information, damaging systems, or engaging in other malicious activities. For big data environments, due to their large amount of data and wide sources, APT attackers are more likely to find a breakthrough and carry out more covert and complex attacks. In addition, APT attacks often utilize advanced techniques such as zero day vulnerabilities to bypass traditional security measures, greatly increasing the difficulty of defense.

3.3 Difficulties in Data Security Governance

In the big data environment, data security governance faces many challenges. Firstly, the unclear definition of data ownership, usage rights, and management rights is the fundamental reason for governance difficulties. Different organizations and individuals often have conflicts of interest and disputes over rights in the process of data sharing and exchange, making it difficult to form a unified data security management standard. Secondly, data security governance requires cross domain and cross departmental collaboration and cooperation, but the current collaboration mechanism is not yet perfect, resulting in low governance efficiency and poor effectiveness. In addition, the liquidity and dynamism of big data also increase the difficulty of data security governance. Frequent transmission and interaction of data between different systems and applications increases the number of data security risk points, making it difficult to conduct comprehensive and effective monitoring and management.

3.4 Technical and Management Bottlenecks

The current security technology and management methods are inadequate in the big data environment. Firstly, the development of security technology cannot keep up with the rapid pace of big data. The massive amount of data and complex scenarios in big data pose higher requirements for the real-time, accuracy, and intelligence of security technology, but existing technologies often struggle to fully meet these needs. Secondly, the lack of security management is also a key factor restricting the security of big data. Many organizations lack sufficient attention and investment in data security management, resulting in frequent problems such as incomplete security management systems, non-standard management processes, and inadequate implementation of security systems. Finally, the shortage of talent and the lag in laws and regulations have also exacerbated the dilemma of big data security. With the widespread application and development of big data technology, the demand for professional talents is increasing day by day. However, there is a relative shortage of talents with big data security skills and experience in the current market. Meanwhile, the lag of laws and regulations also limits the effective protection of big data security. Existing laws and regulations often fail to fully cover various security issues and challenges in the big data environment, resulting in legal gaps or ambiguous areas in data protection, cross-border data flow, and data accountability. This not only increases the risk of data leakage and abuse, but also brings uncertainty to the protection of data rights for enterprises and individuals.

4. BIG DATA NETWORK SECURITY STRATEGIES AND TECHNOLOGIES

4.1 Data Encryption and Privacy Protection Technologies

Data encryption is one of the core means of protecting data confidentiality and integrity, while privacy protection focuses on safeguarding the privacy rights of individuals or organizations during data processing. In the era of big data, with the explosive growth of data volume, how to efficiently and securely process this data has become a major challenge.

4.1.1 Advanced encryption algorithms.

AES (Advanced Encryption Standard): As one of the most widely used symmetric encryption algorithms, AES plays an important role in big data encryption due to its high security and efficiency. In the AES encryption process, data is divided into fixed length blocks and encrypted through multiple rounds of complex substitution and permutation operations to ensure data confidentiality even under the most powerful computational attacks.

RSA: Although primarily used for asymmetric encryption and key exchange, RSA also plays a critical role in the big data security system. By generating public and private key pairs, RSA can achieve data encryption, decryption, and authentication, ensuring the security and integrity of data during transmission [2].

4.1.2 Differential Privacy Protection Technology

Differential privacy technology is a statistical data analysis method aimed at adding appropriate randomness to a dataset to protect individual privacy while allowing for statistical analysis of the data. In big data analysis, differential privacy technology adds an appropriate amount of noise to the query results, so that even if a record in the dataset changes, the distribution of the output results will not change significantly. This method is particularly important in data analysis in fields such as healthcare and finance, as it can effectively prevent the leakage of sensitive personal information.

4.2 Anomaly Detection and Intrusion Prevention System

In the big data environment, the types and complexity of network attacks are constantly increasing, and traditional security defense methods are no longer sufficient to meet the needs. Intelligent anomaly detection models and intrusion detection and defense systems based on big data have become new solutions.

4.2.1 Intelligent anomaly detection model

The intelligent anomaly detection model utilizes advanced technologies such as machine learning and deep learning to automatically extract feature patterns of normal behavior by analyzing and learning massive amounts of data. When there is behavior in the network that does not match these feature patterns, the model can quickly identify and mark it as abnormal behavior. This method can not only discover known attack patterns, but also discover unknown and covert attack behaviors, improving the accuracy and timeliness of security detection [3].

4.2.2 Intrusion Detection and Defense Mechanisms

Intrusion detection systems (IDS) can monitor network traffic and system logs in real-time, analyze and identify potential intrusion behaviors. When abnormal behavior is detected, IDS will immediately trigger an alert and generate a corresponding security event report. Intrusion prevention systems (IPS) go further by not only detecting intrusion behavior, but also automatically taking response measures after detecting intrusion, such as blocking attack sources, adjusting firewall rules, etc., to prevent further spread of attacks. In the big data environment, the coordinated use of IDS and IPS can form a more effective security protection system.

4.3 Security Risk Assessment and Management

Security risk assessment and management are important components of building a big data network security system. By regularly assessing the security status and risk level of network systems, security vulnerabilities and hidden dangers can be discovered and fixed in a timely manner, improving overall security protection capabilities.

4.3.1 Network Security Risk Assessment System

Building a comprehensive network security risk assessment system requires starting from multiple dimensions, including identification of network assets, threat analysis, vulnerability assessment, and risk quantification. Firstly, it is necessary to conduct a detailed identification and classification of all assets in the network system, including hardware devices, software systems, data resources, etc., to clarify their value and importance. Secondly, conduct a comprehensive threat analysis on these assets, identify potential attack methods and means, and evaluate their likelihood and harmfulness of occurrence. At the same time, it is necessary to discover security vulnerabilities and weaknesses in the system through vulnerability scanning and penetration testing. Finally, based on the severity of the threat and the ease of exploitation of the vulnerability, a quantitative assessment of the risk is conducted to determine the priority risk items for processing.

4.3.2 Dynamic Security Management Strategy

Faced with the constantly changing network environment and security threats, traditional static security management strategies are no longer sufficient to meet the needs. The dynamic security management strategy emphasizes the flexibility and adaptability of security policies, which can be adjusted and optimized in real time according to actual situations. This includes establishing real-time security monitoring mechanisms to continuously monitor and analyze key information such as network traffic and system logs; Establish an emergency response mechanism that can quickly activate emergency plans and handle security incidents promptly; And implement continuous safety training and education to enhance employees' safety awareness and response capabilities. By implementing dynamic security management strategies, it is possible to ensure that the security protection capability of the network system is always maintained at a high level.

4.4 Cross domain collaboration and legal and regulatory construction

The cross domain flow and sharing characteristics of big data require strengthening cross departmental and cross domain collaboration and regulatory construction to ensure data security and privacy rights.

4.4.1 Cross departmental and cross domain data sharing and protection mechanisms

In the process of data sharing, it is necessary to establish a sound data protection mechanism, clarify data usage permissions and responsible parties, and ensure that data is not illegally obtained, tampered with, or abused during the sharing process. This can be achieved by developing data sharing protocols, establishing data sharing platforms, strengthening data encryption and access control, and other means. At the same time, it is necessary to strengthen cross departmental and cross domain collaboration, jointly develop data sharing standards and norms, and promote the orderly development of data sharing and protection work.

4.4.2 International Cooperation and Regulation Development

With the globalization of big data technology, international cooperation and regulatory development have become particularly important. Governments, businesses, and international organizations should strengthen communication and cooperation to jointly address cross-border data security challenges. By formulating international data security protection conventions or agreements, clarifying security standards and rules for cross-border data flow, and establishing cross-border data protection cooperation mechanisms. In addition, it is necessary to strengthen international cooperation in areas such as data security technology research and development, talent cultivation, and information sharing, and jointly promote the improvement and development of the global data security governance system.

5. CONCLUSION

In the context of big data, network security research is not only about technological innovation, but also a profound reflection on social governance and privacy protection. Through the discussion in this article, we realize that big data brings both opportunities and challenges, and it is necessary to continuously optimize security strategies, strengthen technical support, and achieve a win-win situation between the reasonable application of data and security protection. Looking ahead to the future, research on cybersecurity will continue to deepen, building a solid defense line for the healthy development of the big data era and safeguarding the security and prosperity of cyberspace.

REFERENCES

[1] Zhu, Y., Yu, W., & Li, R. (2025). SAGCN: A spatiotemporal attention-weighted graph convolutional network with IoT integration for adolescent tennis motion analysis. Alexandria Engineering Journal, 128, 652-662.

[2] Zhang, X. (2024). Research on Dynamic Adaptation of Supply and Demand of Power Emergency Materials based on Cohesive Hierarchical Clustering. Innovation & Technology Advances, 2(2), 59–75. https://doi.org/10.61187/ita.v2i2.135

[3] Zhou, J., & Cen, W. (2024). Investigating the Effect of ChatGPT-like New Generation AI Technology on User Entrepreneurial Activities. Innovation & Technology Advances, 2(2), 1–20. https://doi.org/10.61187/ita.v2i2.124

[4] Yang, J., Wang, Z., & Chen, C. (2024). GCN-MF: A graph convolutional network based on matrix factorization for recommendation. Innovation & Technology Advances, 2(1), 14–26. https://doi.org/10.61187/ita.v2i1.30

[5] Chen, J., Zhang, X., Wu, Y., Ghosh, S., Natarajan, P., Chang, S. F., & Allebach, J. (2022). One-stage object referring with gaze estimation. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 5021-5030).

[6] Wu, W., Bi, S., Zhan, Y., & Gu, X. (2025). Supply chain digitalization and energy efficiency (gas and oil): How do they contribute to achieving carbon neutrality targets?. Energy Economics, 142, 108140.

[7] Peng, Qucheng, Ce Zheng, and Chen Chen. "Source-free domain adaptive human pose estimation." Proceedings of the IEEE/CVF International Conference on Computer Vision. 2023.

[8] Peng, Qucheng, et al. "RAIN: regularization on input and network for black-box domain adaptation." Proceedings of the Thirty-Second International Joint Conference on Artificial Intelligence. 2023.

[9] Guo, Y., & Tao, D. (2025). Modeling and Simulation Analysis of Robot Environmental Interaction. Artificial Intelligence Technology Research, 2(8).

[10] We, X., Lin, S., Pruś, K., Zhu, X., Jia, X., & Du, R. (2025). Towards Intelligent Monitoring of Anesthesia Depth by Leveraging Multimodal Physiological Data. International Journal of Advance in Clinical Science Research, 4, 26–37. Retrieved from https://www.h-tsp.com/index.php/ijacsr/article/view/158