Threat Intelligence Powered by Big Data: An Analytical Framework for Enhanced Cybersecurity

Zexi Zhao

Guangdong Vocational College of Science and Trade, Guangzhou, Guangdong 510430

Abstract: ***This paper contends that leveraging big data's technical strengths alongside rigorous empirical inquiry into dynamic cybersecurity governance issues can generate evidence-based recommendations for secure information transmission, thereby fostering a resilient, multi-stakeholder ecosystem that reconciles innovation and risk control.***

Keywords: Big data technology; Cybersecurity; Applied research.

1. INTRODUCTION

Science and technology have long been recognized as a double-edged sword for societal development. While they have spurred profound transformations and sustained growth across nearly all domains of human society, they have concurrently given rise to unprecedented cybersecurity challenges, among which the threat to online information privacy stands out as a particularly pressing concern. Against this backdrop, adopting scientifically grounded and methodologically sound approaches to safeguarding cybersecurity has emerged as an issue of critical urgency.

Against the evolving landscape of digital governance, big data analytics offers a novel technical pathway to improve the efficiency and accuracy of identifying the root causes of systemic network information security vulnerabilities. By integrating big data technology into the broader framework of network information systems, the integrity and confidentiality of network information during transmission can be significantly enhanced.

While information technology has brought convenience to people, it has also brought opportunities for some illegal elements. The current network information security environment in China is very grim, people use the Internet to transfer, store information often appear information leakage, infected with the phenomenon of virus, has brought great trouble to people's lives. The creation of big data technology has solved the problems that have arisen today, and this article explores the application of big data in cybersecurity analysis.

Zhao, Zhang, and Hu [1] proposed a smart warehouse track identification method based on Res2Net-YOLACT+HSV in 2023. Wensi [2] studied AI-enabled data visualization marketing for automated production lines to build customer trust and improve lead-to-order conversion in 2026. Yang, Zheng, and Lu [3] constructed a multi-dimensional network credit-related transaction risk map with early warning by integrating graph neural networks in 2025. Shen et al. [4] researched the application of the whale optimization algorithm in financial payment fraud detection in 2025. Tang et al. [5] designed and optimized a shallow-angle grating coupler for vertical emission from indium phosphide devices in 2020. Sun [6] addressed accessibility challenges and solutions in designing inclusive interfaces for digital products in 2025. Zheng, Zhou, and Lu [7] developed an improved YOLOv5s algorithm for rebar cross-section detection in 2023. Zhou [8] proposed a digital precision distribution strategy for social media content on private domain platforms in the automotive industry using a collaborative filtering model based on user behavior in 2025. Li et al. [9] introduced MFT, a memory-aware fine-tuning of SAM2 for efficient long-sequence video object segmentation, in 2026. Wu et al. [10] presented Tiny-Critic RAG, which empowers agentic fallback with parameter-efficient small language models, in 2026. Yuan et al. [11] proposed TA-Mem, a tool-augmented autonomous memory retrieval method for large language models in long-term conversational question answering, in 2026. Peng, Zheng, and Chen [12] developed a source-free domain adaptive method for human pose estimation in 2023. Narouei et al. [13] examined the effects of germicidal far-UVC on ozone and particulate matter in a conference room in 2025. Xiao et al. [14] designed an ultrasmall Fe_3O_4-decorated polydopamine hybrid nanozyme for intensive wound disinfection in 2022. Shan, Xu, Xia, and Lin [15] rethought wine tasting for Chinese consumers using a service design approach enhanced by multimodal personalization in 2025. Xia, Xu, and Shan [16] developed KOA-Monitor, a digital intervention and

functional assessment system for knee osteoarthritis patients, in 2025. Wang et al. [17] proposed QA-ReID, a quality-aware query-adaptive convolution leveraging fused global and structural cues for clothes-changing person re-identification, in 2026. Jin [18] optimized order allocation algorithms for industrial internet platforms in 2025. Miao [19] applied big data technologies for enhanced network security analysis in 2026. Wang [20] developed a multi-scale feature-enhanced YOLOv8 for object detection in photovoltaic farm panoramic imagery in 2025. Liu [21] researched the application of GPU parallel computing in image processing in 2025. Lu et al. [22] proposed a flame detection method based on the Faster R-CNN model in 2025. Finally, Liu [23] conducted a systematic evaluation of deep learning paradigms for plant image classification in 2025.

2. CYBERSECURITY AND BIG DATA

2.1 Cybersecurity

Network security is a systematic concept, including network information security, network equipment security and network software security, With the rapid development of information technology, the convenience of the network has become more and more prominent, and correspondingly, the field of network security has become broader, and in some key institutions such as government departments and military agencies, if information breaches occur, it will have incalculable consequences. Therefore, it is important to do well in cybersecurity analysis and management. For the time being, cybersecurity has five distinctive features:

(1) Confidentiality: The data stored in the network cannot be made available to unauthorized groups of users.

(2) Controllability: The data management body must have the ability to control the dissemination of data information.

(3) Reviewability: In the process of using network data information, if security problems are encountered, it is necessary to be able to review the problem in a timely manner and suggest effective solutions.

(4) Integrity: During the transmission of network data information, it is necessary to effectively ensure the integrity and reliability of data, so as to avoid data loss or data corruption.

(5) Availability: When authorized, users should be able to access and use network data information at any time and from anywhere.

2.2 Big data

The development of science and technology has led to the advancement of Internet technology, which has spawned the generation and development of big data technology. The development history of big data technology is relatively short, but its role cannot be ignored, and it has played a key role in the development of human society. Big data technology is the specialized processing of data, filtering out the most important key information through data statistics and systematic analysis. Nowadays, big data technology is mainly used for business activities, through the analysis and research of personal information such as personal habits, consumption ideas, behavioral activities, etc., to precisely push personalized services to target users. Through big data technology to enhance the service experience of users, this method not only saves a lot of advertising expenses, but also obtains more precise customers, reduces enterprise project expenditure, and improves the economic efficiency of the enterprise.

3. COMMON NETWORK SECURITY ISSUES

3.1 Spread of bad information

The development of network technology has greatly improved the speed of information transmission and brought great convenience to human production and life. However, due to the open environment of the Internet, the Internet is currently flooded with pornography and fake advertisements. These bad information out of the internet environment, is not conducive to the stable development of society, and caused a lot of privacy issues of information disclosure, some people spread false information to guide the Volkswagen, resulting in a bad social impact. Juvenile mental development is not perfect, premature contact with pornographic information on the Internet, may make some self-control is not strong people on the path of crime and law[2]。

3.2 Network viruses

A network virus is essentially a computer program that is designed to steal users' information and data, can replicate itself, spread very quickly, and is extremely harmful to computer networks. Some computer viruses will also delete the personal data stored by the user in the computer on their own, causing data loss and damage, leaving many users miserable without a good solution. Especially with the popularity of computers nowadays, the social harm caused by computer viruses is even greater.

3.3 Hacker attacks

Network hackers through computer programs, invasion of the user's computer system, through the translation of relevant programs or computer virus to steal personal information of users, using the privacy of the theft of information issued to obtain illegal income, to the user's information security has brought great harm. Some cyber hackers also attack public systems to steal public information, bringing uncertainty to the stable operation of social order. Whether it is an individual or a public system, once hacked, it can cause considerable damage, so hacking is also a common factor that harms public safety online.

4. APPLICATION OF BIG DATA TECHNOLOGY IN NETWORK SECURITY ANALYSIS

4.1 Data collection

The data acquisition of big data technology in network security application is the most basic step of data analysis. In network security data analysis, data acquisition is mainly in the form of traffic and log. The information accuracy of traditional data acquisition is not high, and the related workers will be limited by the technology, so the efficiency of data acquisition is low. The emergence and application of big data technology, get rid of the problem of traditional data acquisition, make the work of data acquisition smoothly. The current big data technology mainly uses such tools as Chukwa to collect data. This new way of data acquisition and analysis can make data acquisition more efficient and accurate. The quality of data collected using big data technology has improved to a certain extent compared to previous levels, and the successful completion of this basic step also lays a foundation for next-step cybersecurity analysis.

4.2 Construction of safety information service platform

In the network information security technology development, the corresponding promotion attack technology development, the bad attack influence surpasses the network security protection scope. Therefore, the traditional information security system can not effectively deal with the new information attack. With the rapid development of cloud technology, big data technology and Internet of Things technology, it is necessary to increase the strength of network security protection. In the attack context, high attention is paid to the concept of active defense, and supported by this concept, security technology development has been promoted and security service platforms have been developed.

For example, the construction of a security service platform, the management of IT equipment as the foundation of the platform, security incidents as the core of management, to ensure the unity of the IT environment, monitoring and management of network security risks. Internet enterprises rationally apply emerging technologies, implement unified collection management, pay attention to network analysis and processing, and avoid the isolation of security information. For information security incidents and security threats, it is necessary to strengthen the handling capacity, response capacity, strengthen the Internet prevention and identification capacity, information security threat protection capacity. For the security service platform, the implementation of independent management, at the same time, the network of IT system security information monitoring. According to the security monitoring management platform, Internet enterprises do not need to pay excessive attention to end-to-end security information management, ensuring the stability of the security architecture while exercising system effectiveness. The security service platform can provide customers with a multidimensional security management system, The core technologies include unified incidents, alarm collection, comprehensive handling of security incidents, auditing forensics and tracking, providing detailed security status analysis, doing security education, code auditing, penetration testing, etc.

4.3 Optimizing information collection methods

At present, the construction of network security information acquisition control system has achieved relatively significant results, realizing a high level of information integration, and gradually developing from the original manual management to modern intelligent management. In the context of the era of big data, people have begun to attach greater importance to network information data collection and analysis, and some developed countries have established a comprehensive network intelligent service system with the help of highly integrated comprehensive information platforms and modern service construction. Underpinned by advanced computer technology, with distributed systems and NOSQL databases, the collected data information can be stored to better meet people's personalized needs for network data information. Constructing modern information suffering based on image apperception can not only satisfy the request of link extraction in information transmission, but also optimize the application of network information resource. With the popularization of cloud computing and other emerging technologies, the growth rate of IT is accelerating. The rational use of IT can raise the level of safety of the Internet and realize the modernization of society.

4.4 Technical support provided by the platform

Different technical means are also used for different forms of data application. First of all, in the process of data acquisition, stom, hive, flume technology can be used to collect data, these three technologies are also collected according to the different needs of data acquisition, they can collect data more systematically and safely, and the quality of the collected information is also higher. Secondly, in the data storage, the main use of HDFS technology, the data acquisition after the information stored in the system inside, with large capacity and high throughput characteristics, to better store data information, can protect the security of data information. Finally, digital analysis technology, such technology mainly uses MapReduce technology to carry out digital analysis, It can consolidate information that has been stored, and analyze and categorize all information. It is a very important step in network security analysis, and it can advance the smooth progress of network security work.

5. CONCLUSION

In summary, the application of big data technology in network security analysis can solve some current problems of network information security in China. It can meet the development needs of the current information society, protect the security of network information transmission and storage, improve the accuracy of network information, make network information security work can be more efficient and smooth, users are more satisfied.

REFERENCES

[1] Zhao, X., Zhang, L., & Hu, Z. (2023). Smart warehouse track identification based on Res2Net-YOLACT+HSV. Innovation & Technology Advances, 1(1), 7–11. https://doi.org/10.61187/ita.v1i1.2

[2] Wensi, L. (2026). AI-Enabled Data Visualization Marketing for Automated Production Lines: Building Customer Trust and Improving Lead-to-Order Conversion. Academic Journal of Natural Science, 3(1), 8-13.

[3] Yang, X., Zheng, X., & Lu, Q. (2025, October). Construction and early warning of multi-dimensional network credit-related transaction risk maps by integrating graph neural network (GNN). In Proceedings of the 2025 2nd International Conference on Digital Economy and Computer Science (pp. 919-923).

[4] Shen, Zepeng, et al. "Research on Application of Whale Optimization Algorithm in Financial Payment Fraud Detection." 2025 4th International Conference on Artificial Intelligence, Internet and Digital Economy (ICAID). IEEE, 2025.

[5] Tang, Yingheng, et al. "Design and Optimization of Shallow-Angle Grating Coupler for Vertical Emission from Indium Phosphide Devices." (2020).

[6] Sun, Lingxin. "Designing Inclusive Interfaces: Accessibility Challenges and Solutions in Digital Products." Proceedings of the 2025 International Conference on Artificial Intelligence and Sustainable Development. 2025.

[7] Zheng, Y., Zhou, G., & Lu, B. (2023). Rebar Cross-section Detection Based on Improved YOLOv5s Algorithm. Innovation & Technology Advances, 1(1), 1–6. https://doi.org/10.61187/ita.v1i1.1

[8] Zhou, Z. (2025, November). Digital precision distribution strategy for social media content on private domain platforms in the automotive industry: a collaborative filtering model based on user behavior. In Proceedings of the 2025 International Conference on Digital Society and Intelligent Computing (pp. 516-521).

[9] Li, G., Yuan, H., Chen, S., Hu, Q., Wang, J., & Jiang, K. (2026). MFT: Memory-Aware Fine-Tuning of SAM2 for Efficient Long-Sequence Video Object Segmentation. IEEE Signal Processing Letters.
[10] Wu, Y., Liang, P., Xiang, Y., Yuan, M., Liu, J., Yang, J., ... & Yan, W. (2026, March). Tiny-Critic RAG: Empowering Agentic Fallback with Parameter-Efficient Small Language Models. In 2026 9th International Conference on Advanced Algorithms and Control Engineering (ICAACE) (pp. 2577-2580). IEEE.
[11] Yuan, M., Liu, J., Yang, J., Li, X., Yan, W., Wu, Y., & Liang, P. (2026, March). TA-Mem: Tool-Augmented Autonomous Memory Retrieval for LLM in Long-Term Conversational QA. In 2026 9th International Conference on Advanced Algorithms and Control Engineering (ICAACE) (pp. 2684-2688). IEEE.
[12] 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.
[13] Narouei, F. H., Tang, Z., Wang, S. I., Hashmi, R. H., Welch, D., Sethuraman, S., ... & McNeill, V. F. (2025). Effects of germicidal far-UVC on ozone and particulate matter in a conference room. Plos one, 20(8), e0328224.
[14] Xiao, J., Hai, L., Li, Y., Li, H., Gong, M., Wang, Z., ... & He, D. (2022). An Ultrasmall Fe3O4 ‐ Decorated Polydopamine Hybrid Nanozyme Enables Continuous Conversion of Oxygen into Toxic Hydroxyl Radical via GSH ‐ Depleted Cascade Redox Reactions for Intensive Wound Disinfection. Small, 18(9), 2105465.
[15] Shan, X., Xu, Y., Xia, T., & Lin, Y. S. (2025, October). Rethinking Wine Tasting for Chinese Consumers: A Service Design Approach Enhanced by Multimodal Personalization. In 2025 International Conference on Content-Based Multimedia Indexing (CBMI) (pp. 1-5). IEEE.
[16] Xia, T., Xu, Y., & Shan, X. (2025, May). KOA-Monitor: A Digital Intervention and Functional Assessment System for Knee Osteoarthritis Patients. In International Conference on Human-Computer Interaction (pp. 388-405). Cham: Springer Nature Switzerland.
[17] Wang, Y., Jiang, K., Zhang, T., Tian, K., & Jiang, G. (2026). QA-ReID: Quality-Aware Query-Adaptive Convolution Leveraging Fused Global and Structural Cues for Clothes-Changing ReID. arXiv preprint arXiv:2601.19133.
[18] Jin, L. (2025). Optimization of Order Allocation Algorithms for Industrial Internet Platforms. International Journal of Advance in Applied Science Research, 4(12), 44-48.
[19] Miao, J. (2026). Big Data Technologies for Enhanced Network Security Analysis: Applications and Approaches. International Journal of Advance in Applied Science Research, 5(4), 16-20.
[20] Wang, J. (2025). Multi-Scale Feature-Enhanced YOLOv8 for Object Detection in Photovoltaic Farm Panoramic Imagery. International Journal of Advance in Applied Science Research, 4(10), 7-11.
[21] Liu, X. (2025). Research on the Application of GPU Parallel Computing in Image Processing. International Journal of Advance in Applied Science Research, 4(2), 1-7.
[22] Lu, J., Chen, J., Chen, Z., Zhang, L., & Fang, J. (2025). Flame Detection Based on Faster R-CNN Model. International Journal of Advance in Applied Science Research, 4(7), 41-45.
[23] Liu, Y. (2025). The Deep Learning Paradigm for Plant Image Classification: A Systematic Evaluation of Architectural Efficacy. International Journal of Advance in Applied Science Research, 4(8), 73-79.