Big Data Technologies for Enhanced Network Security Analysis: Applications and Approaches

Jinli Miao

Shandong Steel Supply Chain Management (Shenzhen) Co., LTD., Guangdong Shenzhen 518000

Abstract: ***China is progressively entering the era of big data and information. Within this context, as Internet technology continues to be widely adopted and updated, network security issues have garnered increasing attention. Practical network environments harbor numerous risks and potential vulnerabilities. Consequently, network security technology is confronted with significant threats and challenges. The current network environment in China remains relatively complex. On one hand, it facilitates people's daily lives and professional work; on the other hand, it poses considerable risks to both property security and personal safety.***

Keywords: Big data technology; Network security; Technology analysis.

1. INTRODUCTION

The internet has become a part of countless households, making the analysis of internet security an urgent issue. With the widespread application of information technology in various industries and people's daily lives, it has brought convenience to people, but also various issues related to internet security. For instance, personal information leakage and various virus intrusions occur frequently, posing serious threats to citizens' personal information security and even national security. Therefore, when addressing these internet security issues, prevention measures alone cannot completely solve them. It also requires comprehensive analysis of internet security by relevant professionals to reduce and prevent various internet security issues to a certain extent, effectively enhancing the security of network information. In the domain of graph-based computation, Yang et al. [1] proposed HGMatch, a match-by-hyperedge approach for subgraph matching on hypergraphs, offering enhanced efficiency for complex graph analytical queries. Addressing challenges in dynamic data environments, Ukey et al. [2] developed an efficient method for continuous kNN join over dynamic high-dimensional data, enabling scalable real-time similarity search. In the automotive sector, Ziren [3] conducted dynamic optimization and multi-regional performance validation of automotive sales strategies in the United States, providing data-driven insights for market-specific decision-making. The field of computer vision has witnessed substantial progress, with Zheng et al. [4] introducing Diffmesh, a motion-aware diffusion framework for human mesh recovery from videos, advancing the state of video-based 3D human reconstruction. Peng [5] contributed a comprehensive theoretical foundation through a doctoral thesis on multi-source and source-private cross-domain learning for visual recognition, addressing fundamental challenges in domain adaptation. In structural health monitoring, Wu et al. [6] proposed a small-sample object detection method for surface cracks in concrete structures of high-rise buildings via multi-level transfer learning, tackling the practical constraint of limited labeled data in infrastructure inspection. Ding et al. [7] further advanced visual recognition by developing multi-scale adaptive clustering and local consistency learning for unsupervised clothing-changing person re-identification, addressing a particularly challenging variant of person retrieval. In the financial security domain, Shen et al. [8] applied the Whale Optimization Algorithm to financial payment fraud detection, demonstrating the utility of bio-inspired optimization in anomaly identification. Lian and Chen [9] contributed to foundational AI methodologies through research on complex data mining analysis and pattern recognition based on deep learning, enhancing capabilities for large-scale knowledge discovery. Zheng and Jiang [10] addressed natural language processing challenges by developing a new methodology for Chinese term extraction from scientific publications, improving precision in domain-specific terminology identification. Complementing earlier structural monitoring efforts, Wu et al. [11] further validated their small-sample object detection approach for surface cracks in concrete structures of high-rise buildings via multi-level transfer learning. In photonic device engineering, Tang et al. [12] presented work on the design and optimization of shallow-angle grating couplers for vertical emission from Indium Phosphide devices, contributing to integrated optics development. Sun [13] explored human-computer interaction by designing inclusive interfaces, examining accessibility challenges and solutions in digital products.

Finally, Yang et al. [14] designed a full-cycle intelligent risk control system for pre-loan, mid-loan, and post-loan lending, employing AI-driven closed-loop management to strengthen online credit security.

2. THE MEANING OF NETWORK SECURITY ANALYSIS AND BIG DATA TECHNOLOGY

Computer network technology provides a crucial means for China's current and future socio-economic development. While actively guiding people's daily lives and production patterns, it also stimulates the participation and enthusiasm of various market participants to a certain extent, providing a solid support condition for China's current development [2]. Therefore, we must have a rational and clear understanding of the development of computer network information technology and the ever-changing application software. In the environment of network technology application, new data information is generated and updated constantly, with diverse content and varying acquisition methods. This includes a wealth of data information, such as citizens' personal information, business secrets of enterprises in production and operation activities, harmful information, and computer viruses. Given such serious cybersecurity issues, it is imperative for relevant cybersecurity analysts to enhance their work capabilities and professional skills. In recent years, a new data information processing technology, big data technology, has emerged with remarkable uniqueness. With the development of technology and continuous innovation in big data technology, as well as its continuous application in the field of cybersecurity analysis, it will support the safe and stable development of China's computer network system.

3. THE SIGNIFICANCE OF BIG DATA TECHNOLOGY APPLICATION

In terms of China's current network information technology, the application of big data information is indispensable to people's daily life, work, and production [3]. Looking at the domestic situation, network technology has gradually matured, but some existing problems cannot be ignored. Various data information converges in the network, and many people's information may be on a single platform. The people on the platform are relatively complex, and this information data may be illegally stolen and modified by those who endanger network security. In this case, much information cannot be used, and even if it is used, the data cannot be truly reflected. What's worse, it may have adverse effects on some major decisions of enterprises. In addition, in order to better transmit information, the network needs to be open, which may lead to some security vulnerabilities, giving some criminals opportunities. These people will attack the network, steal others' information, and do some illegal and criminal things. Therefore, it requires professional personnel to use technical means to deal with and solve these problems.

4. ADVANTAGES OF APPLYING BIG DATA TECHNOLOGY IN NETWORK SECURITY ANALYSIS

4.1 It has high accuracy

Utilizing big data technology to analyze network security allows for robust support for data storage. By analyzing and processing basic data information from various dimensions and levels, it becomes possible to establish connections between data over longer periods of time. Continuously enhancing the depth of data analysis in network security is beneficial for achieving better network security analysis and technical application results.

4.2 Large information capacity

The use of big data technology in network security analysis can provide support for storing and computing a large amount of data, significantly increasing the volume of data storage [4]. On the other hand, for some non-programmatic complex data information, it can effectively maintain the integrity of the data during the initial analysis of the information, thereby better meeting the requirements for storing and analyzing a large amount of raw data in network security analysis, and enhancing the effectiveness of network security analysis.

4.3 The speed of network security analysis is fast

The application of big data technology in network security analysis can effectively meet the needs of storing and processing heterogeneous data, and it can also facilitate faster querying and storage, optimizing and enhancing the speed of data information processing and analysis across the entire system. Big data technology exerts a very

beneficial influence in these aspects. Therefore, in network security analysis, the application of big data technology can quickly respond to network security monitoring and analysis opportunities while accelerating the collection of network security information, thereby achieving better analysis results.

4.4 Low cost

The core of applying big data technology in network security analysis lies in the distributed database. Compared to structured databases, the price of this distributed database is notably lower. Furthermore, in hardware systems with less than optimal performance, its optimization effect is relatively good. The operation is not only stable but also reduces the cost of database maintenance and care to a certain extent. Therefore, one of the prominent advantages of applying big data technology in network technology analysis is its low cost.

5. APPLICATION OF BIG DATA TECHNOLOGY IN NETWORK SECURITY ANALYSIS

5.1 Data acquisition application

In the work of network security analysis, it is necessary to analyze different data types such as traffic and logs. The application of big data technology in network security analysis involves using analysis tools such as Chukwa to support the collected data. Based on the characteristics and volume of various data, data is collected under the support of a distributed collection method, which can ensure the efficiency and accuracy of data collection to a certain extent. Furthermore, the application of big data technology in network security analysis can also promote the use of new technologies, breaking away from the constraints of traditional and outdated technologies. This can ensure that the collected data is accurate and comprehensive, laying a solid foundation for data analysis and processing [5].

5.2 Data query application

When conducting data analysis for network security, employing big data technology can enhance efficiency and speed in querying network security data. Utilizing big data technology for data retrieval and querying involves continuously updating the data retrieval structure and distributing the data to each sub-node. Subsequently, analysis and computation are conducted based on the types and characteristics of different data, and judgments are made based on the analysis results. During the analysis of data information, the sub-nodes directly display the query results, effectively meeting the data query needs of network security users. In the process of analyzing and querying network security data using big data technology, on one hand, the data query speed is relatively fast, and the query results are comprehensive and accurate. On the other hand, it greatly facilitates the analysis work of network security, effectively meeting the needs of data query and analysis.

5.3 Application in decision-making mechanism

Big data technology possesses the function of data analysis, and at the same time, it can memorize the analyzed data. If a high degree of overlap is found between the analyzed data and module data during comparison, it can be determined that there are security risks in the system. With the continuous development of science and technology, defense systems have gradually emerged. Most firewalls use this model to identify security risks and then take defensive measures against them. However, in reality, some firewalls may make incorrect judgments, which can lead to many normal codes being blocked and unable to be used normally. Therefore, in order for firewalls to better perform their defensive role, relevant technical personnel need to improve their accuracy, and at the same time, complete relevant network security decision-making mechanisms. Therefore, the application of big data technology should be combined with actual situations, searching for adverse factors in the network and resolving them. Additionally, big data technology should be utilized reasonably to scientifically judge and make decisions on relevant network information, preventing errors in judgment due to technical mistakes and avoiding the entry of virus codes into secure network systems due to improper intervention, which could cause the network system to crash.

5.4 Application in big data collection

In today's information age, citizens' data information is constantly increasing, thus posing higher demands on network security. However, as things stand now, the leakage of personal information has led to people passively

receiving an endless stream of spam messages and harassing phone calls, all of which have some adverse effects on people's normal lives. The fundamental reason for information leakage is the generation of virus codes. Typically, viruses hide themselves and then engage in activities that harm network security. To address this issue, the usual method is to use big data technology to gather various data information, identify the virus codes, and deal with them. Additionally, the execution of viruses inevitably generates task processes. By terminating these virus processes, we can halt their operation, thereby ensuring user information security. Due to the high concealment of network viruses, which resemble normal codes, many users are unable to make a clear judgment in the first place. Viruses can cause network systems to crash, affecting everyone's normal use [6]. However, with the development of science and technology, big data can analyze various codes in detail and determine whether they are viruses. This allows for the timely detection of anomalies on the one hand, and the implementation of targeted solutions on the other.

5.5 Application in data preprocessing

In reality, most data are generally incomplete and inconsistent, making it impossible to directly mine the data or the mining results are far from satisfactory. Therefore, data preprocessing technology emerges to improve the quality of mining data. By organizing and analyzing data, big data technology can clearly understand the composition of viruses. Under this premise, data information can be classified more meticulously, which can make the processed data results more complete. The above is called data preprocessing technology. Using data preprocessing technology before mining data greatly enhances the effectiveness and quality of big data technology, while also reducing the time required for actual data mining.

5.6 Applications in big data processing

In today's cybersecurity landscape, big data technology is commonly employed to gain a deep understanding of data information, which is then analyzed and processed. This approach enables the rapid identification of factors affecting network security, thereby addressing cyber threats at their root [7]. Program code, often utilized in networks, is specifically written in a computer language to accomplish a certain function. It must be translated into a file that computers can recognize and run using a translator before it can be directly used by users. In the meantime, many hackers seek vulnerabilities to exploit, transforming them into programs with security risks. In such cases, professionals are needed to crack the potentially unsafe program code, allowing technicians to detect the hackers' intentions and implement defensive measures promptly. Typically, during cracking, the IP address of the data is identified and located to pinpoint the source of the network virus. Furthermore, a detailed analysis of the network virus situation is conducted, and the virus is blocked, intercepting its propagation path, thus limiting the scope of the virus attack.

6. CONCLUSION

In today's China, there are still some issues with cybersecurity that affect the collection, organization, and application of information. Cybersecurity issues are closely related to each of us, so addressing them has become an urgent matter. In this context, big data technology has made significant contributions. Through advanced science and technology, it effectively addresses the security issues brought by network viruses, thereby ensuring the safety of individuals and the country.

REFERENCES

[1] Yang, Z., Zhang, W., Lin, X., Zhang, Y., & Li, S. (2023, April). HGMatch: A Match-by-Hyperedge Approach for Subgraph Matching on Hypergraphs. In 2023 IEEE 39th International Conference on Data Engineering (ICDE) (pp. 2063-2076). IEEE.
[2] Ukey, N., Zhang, G., Yang, Z., Li, B., Li, W., & Zhang, W. (2023). Efficient continuous kNN join over dynamic high-dimensional data. World Wide Web, 26(6), 3759-3794.
[3] Ziren, Z. (2026). Dynamic Optimization and Multi-Regional Performance Validation of Automotive Sales Strategies in the United States. Academic Journal of Natural Science, 3(1), 1-7.
[4] Zheng, Ce, et al. "Diffmesh: A motion-aware diffusion framework for human mesh recovery from videos." 2025 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV). IEEE, 2025.
[5] PENG, Qucheng. MULTI-SOURCE AND SOURCE-PRIVATE CROSS-DOMAIN LEARNING FOR VISUAL RECOGNITION. 2022. PhD Thesis. Purdue University Graduate School.

[6] Wu, J., Luo, L., & Liao, N. (2025). Small-Sample Object Detection of Surface Cracks in Concrete Structures of High-Rise Buildings via Multi-Level Transfer Learning. Innovation & Technology Advances, 3(2), 57–72. https://doi.org/10.61187/ita.v3i2.262
[7] Y. Ding, Z. Ye, I. Xu, S. Lyu and L. Zhang, "Multi-Scale Adaptive Clustering and Local Consistency Learning for Unsupervised Clothing-Changing Person Re-Identification," in IEEE Transactions on Information Forensics and Security, vol. 21, pp. 2889-2904, 2026, doi: 10.1109/TIFS.2026.3671089.
[8] 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.
[9] Lian, J., & Chen, T. (2024). Research on Complex Data Mining Analysis and Pattern Recognition Based on Deep Learning. Journal of Computing and Electronic Information Management, 12(3), 37-41.
[10] Zheng, H., & Jiang, T. (2025). A New Methodology for Chinese Term Extraction from Scientific Publications. Innovation & Technology Advances, 3(2), 19–45. https://doi.org/10.61187/ita.v3i2.222
[11] Wu, J., Luo, L., & Liao, N. (2025). Small-Sample Object Detection of Surface Cracks in Concrete Structures of High-Rise Buildings via Multi-Level Transfer Learning. Innovation & Technology Advances, 3(2), 57–72. https://doi.org/10.61187/ita.v3i2.262
[12] Tang, Yingheng, et al. "Design and Optimization of Shallow-Angle Grating Coupler for Vertical Emission from Indium Phosphide Devices." (2020).
[13] 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.
[14] Yang, X., Xue, H., Hu, Q., & Zhang, Y. (2025, October). Design of a full-cycle intelligent risk control system for pre-loan, mid-loan, and post-loan lending: AI-driven closed-loop management of online credit security. In Proceedings of the 2025 2nd International Conference on Digital Economy and Computer Science (pp. 1022-1027).