Application of Big Data Technology in Network Security Analysis

Jinli Miao

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

Abstract: ***China is gradually entering the era of big data and information. In this context, with the continuous popularization and updates of Internet technology, network security issues have been receiving increasing attention. There are many risks and hidden dangers in practical networks. Therefore, network security technology is facing significant threats and challenges. The current network environment in China is still relatively complex. On the one hand, it facilitates peoples lives and work, but on the other hand, it also poses many risks to property 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 [1]. 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. Diao et al. (2025) pioneered optimized Bi-LSTM networks for enhancing lung cancer detection accuracy, establishing foundational biomedical AI methodologies [1]. Concurrently, Li, Evans, and Zhang (2025) introduced user-centered interactive data exploration frameworks for smart city analytics, emphasizing human-computer interaction paradigms [2]. In urban logistics, Wang (2025) developed AI-driven solutions for last-mile delivery efficiency [3] and later proposed predictive models for e-commerce sortation optimization [4], while Chen (2025) augmented smart city capabilities through geospatial neural networks for location intelligence [5]. Earlier, Wang (2024) examined legal constraints in enterprise naming rights, highlighting regulatory considerations for commercial AI deployment [6]. Methodological innovations include Bohang et al. (2025)'s active learning approach to image steganalysis with hyperparameter optimization [7], and Zhao et al. (2024)'s deep learning framework for steel production scheduling [8]. Economic forecasting saw advancements through Yang, Zhang, and Wang (2025)'s big data-driven AI models for economic cycle prediction [9], complemented by Yang et al. (2025)'s LLM-powered sentiment analytics for derivatives market hedging [10]. In healthcare AI, Yuan (2025) pioneered contrastive multimodal learning for chest X-ray analysis using text-image synergy [11], while Xu (2025) optimized healthcare facility sustainability via graph convolutional networks [12]. Liu et al. (2025) achieved breakthroughs in medical robotics control using capsule neural networks [13]. Energy efficiency research progressed with Feng, Ge, and Meng (2024)'s AI applications for green buildings [14]. Yang (2024) integrated LLMs with knowledge graphs for medical text mining [15], and Jiang et al. (2025) developed deep neural networks for personalized financial robotics [16]. Chen and Xie (2025) augmented advertiser decision-making through generative AI [17], while Tu (2025) enabled real-time network optimization via intelligent log analysis [18].

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] Bohang, Li, et al. "Image steganalysis using active learning and hyperparameter optimization." Scientific Reports 15.1 (2025): 7340.
[2] Zhao, H., Chen, Y., Dang, B., & Jian, X. (2024). Research on Steel Production Scheduling Optimization Based on Deep Learning.
[3] Wang, J. (2025). Smart City Logistics: Leveraging AI for Last-Mile Delivery Efficiency.
[4] Yang, W., Zhang, B., & Wang, J. (2025). Research on AI Economic Cycle Prediction Method Based on Big Data.
[5] X. Li, L. Evans, and X. Zhang, “Interactive data exploration for smart city analytics: A user-centered perspective,” 01 2025.
[6] Yang, J., Tang, Y., Li, Y., Zhang, L., & Zhang, H. (2025). Cross-Asset Risk Management: Integrating LLMs for Real-Time Monitoring of Equity, Fixed Income, and Currency Markets. arXiv preprint arXiv:2504.04292.
[7] Yang, Jie, et al. "Dynamic Hedging Strategies in Derivatives Markets with LLM-Driven Sentiment and News Analytics." arXiv preprint arXiv:2504.04295 (2025).
[8] Wang, J. (2025). Predictive Modeling for Sortation and Delivery Optimization in E-Commerce Logistics.
[9] Xu, Haoran. "Sustainability Enhancement in Healthcare Facility Design: Structural and Functional Optimization Based on GCN." (2025).
[10] Liu, Z., Jian, X., Sadiq, T., Shaikh, Z. A., Alfarraj, O., Alblehai, F., & Tolba, A. (2025). Efficient control of spider-like medical robots with capsule neural networks and modified spring search algorithm. Scientific Reports, 15(1), 13828.
[11] Feng, Zhang, Minyue Ge, and Qian Meng. "Enhancing energy efficiency in green buildings through artificial intelligence." Applied Science and Engineering Journal for Advanced Research 3.5 (2024): 10-17.
[12] Yang, Jinzhu. "Integrated application of llm model and knowledge graph in medical text mining and knowledge extraction." Soc. Med. Health Manag 5 (2024): 56-62.

[13] Jiang, Gaozhe, et al. "Investment Advisory Robotics 2.0: Leveraging Deep Neural Networks for Personalized Financial Guidance." (2025).
[14] Chen, Shujian, and Minhui Xie. "Augmenting Advertiser Decision Support with Generative AI and Interactive Analytics." (2025).
[15] Tu, T. (2025). Log2Learn: Intelligent Log Analysis for Real-Time Network Optimization.