

The Application of Computer Information Technology in Network Security under the Background of Big Data

Junshan Zhang

Huadian Qingdao Power Generation Co., Ltd. Qingdao 266031, Shandong

Abstract: *With the development of technology, the use of electronic computers and other cutting-edge facilities is becoming increasingly common, which has profoundly influenced people's daily lives and changed their way of thinking. However, due to the rise of big data, it is particularly necessary to improve the reliability of computer information systems. Therefore, we should double our attention and strengthen the application of network security technology to improve the reliability and operability of computer information systems. In response to this, we will focus on how to use big data to improve Internet security and give effective suggestions.*

Keywords: Big data; Computer; Computer information technology; Network security.

1. OVERVIEW AND APPLICATION OF COMPUTER NETWORK SECURITY TECHNOLOGY

Due to the rapid development of science and technology, the rise of the Internet and e-commerce is changing with each passing day. However, due to improper operation, hardware defects, and other reasons, computers may be damaged, causing huge trouble for users and even potentially resulting in significant personal information loss. In recent years, the existence of various vulnerabilities has led to cybersecurity issues, posing a huge threat to the security of users. Their personal privacy and sensitive information are likely to be illegally violated, resulting in a large amount of property and sensitive personal information being stolen. With the further development of society, it is necessary to strengthen the understanding of network security and actively research and develop more effective methods for management, maintenance, control, monitoring, and management, in order to effectively improve the user experience and maintain a good network environment. With the passage of time, more and more new types of computers and database systems have emerged. Among them, the security technology of computers and database systems is particularly important. They not only provide efficient services, but also have easy to maintain and update functions. For example, the antivirus and hacker attack capabilities of computers can monitor them in real-time and provide early warnings, thereby providing higher security guarantees for the operation of computers. Guo et al. [1] proposed an improved YOLOv8 network for vehicle detection, demonstrating superior performance in automotive applications. Building on this, Jin et al. [2] developed a hybrid task cascade framework combined with high-resolution networks for advanced object detection and pose estimation, achieving state-of-the-art results in complex scenarios. Meanwhile, Liu et al. [3] introduced a computational-friendly seq2seq personalized generation model (SPA) that integrates cloud-based and on-device collaboration through causal inference, offering new possibilities for real-time AI applications. The integration of AI in enterprise operations has also seen remarkable progress. Saunders et al. [4] explored AI-driven smart supply chains, identifying key pathways and challenges for enhancing operational efficiency. In the financial sector, Jiang et al. [5] developed Investment Advisory Robotics 2.0, leveraging deep neural networks to provide personalized financial guidance. Similarly, Chen and Xie [6] demonstrated how generative AI and interactive analytics can augment advertiser decision support systems. In intelligent transportation systems, Tu [7] investigated reliable vehicle platooning using redundant 5G link aggregation, highlighting its potential for smart road infrastructure. Concurrently, interdisciplinary applications of AI have expanded into healthcare and environmental science. Ma et al. [8] examined the correlation between maternal metal exposure and fetal liver function, while Lu et al. [9] explored chemotherapy-mediated lncRNA effects on immune cell plasticity in cancer. Jiang et al. [10] further advanced cancer treatment by designing a bimetallic nanostimulator for radio-cuproptosis-immunotherapy. Ma [11] also contributed to medical robotics with an automatic positioning system based on binocular vision. Renewable energy and logistics have benefited from AI-driven forecasting and optimization. Zhao et al. [12] proposed a CNN-Bi-GRU model for short- and long-term renewable electricity demand forecasting, while Luo et al. [13] introduced a transformer-GCN integrated algorithm for intelligent logistics path planning. In consumer behavior analysis, Xu and Lin [14] developed an empirical model to assess user-perceived value in new energy

vehicle enterprises. Shan et al. [15] extended AI research into cross-cultural studies, evaluating large language models' societal implications. Finally, Wang et al. [16] and Chew et al. [17] demonstrated AI's cross-industry potential, applying autonomous driving technology to FinTech and optimizing e-commerce financial risk assessment models through AI-driven data integration.

2. THE ADVANTAGES OF ANALYZING THE APPLICATION OF BIG DATA

Despite the potential risks of big data, its use will be severely restricted if not prevented. However, its strength is not only reflected in this aspect, but its superiority is even more evident. It is not only a derivative of cloud computing technology, but also emphasizes its practical applications, such as collecting, processing, transmitting, sharing, etc., to more effectively meet the constantly changing social needs and comply with the principle of privacy protection. With the development of technology, the internet has become ubiquitous and a part of life and work. People obtain a large amount of personal and business information through it, which is difficult to forget or damage. At the same time, its convenience and flexibility make it even more powerful. It does not require any material resources and is fearless in terms of time, place, and complexity. Although adopting big data cloud storage technology has more advantages, such as more robust systems, more flexible operations, stronger access speeds, lower maintenance costs, etc., they still have extremely strong security and can better protect users' privacy. At the same time, they can also access and update accounts, enabling timely detection and handling of leaked privacy at any time.

3. COMMON PROBLEMS OF INFORMATION MANAGEMENT TECHNOLOGY IN NETWORK SECURITY UNDER BIG DATA

3.1 Imperfect information security management system

With the advancement of technology, more and more enterprises are adopting the CIO mechanism to improve management efficiency and enhance service quality. However, according to the development data of Chinese enterprises, most companies still adhere to traditional management models, lack flexibility, and the division of labor and coordination between departments are ineffective. There are also certain risks in network information security. Therefore, enterprises should strengthen their management of information security and improve their network management level to ensure their long-term development. Due to the lack of effective laws, regulations, and constraint mechanisms, coupled with insufficient awareness of information technology and network security construction by enterprises, the network security construction and management of Chinese enterprises have been seriously affected, leading to increasingly prominent network security issues.

3.2 Insufficient investment and construction in information system security management

With the advancement of science and technology, many developing economies have begun to strengthen their control over network information security to ensure the sustainability of their companies. However, in comparison, we still lack sufficient resources to support the development of this field. Especially for large companies that are constantly expanding in scale, their information technology investment accounts for only 2% of their total sales, while for some small, micro, and private companies, their information technology investment is less than 1%. According to recent statistical data, it can be seen that many companies only focus on pursuing short-term economic growth and neglect basic network security guarantees. The result of this is that the internal network security management organization lacks practical role and necessary technical support, leading to frequent network security vulnerabilities and posing huge challenges to enterprises.

4. THE MAIN FACTORS CONTRIBUTING TO NETWORK SECURITY IN THE ERA OF BIG DATA

4.1 Openness of the Internet

With the rapid progress of network science, the era of big data has arrived rapidly, profoundly affecting people's daily lives. Due to its openness, it has been widely applied in various fields, providing valuable information for enterprises and governments. Although today's Internet technology is promoting the rapid development of society, there are also many network security challenges. Some illegal individuals, tempted by wealth and other factors, may cross the border and invade, resulting in serious consequences. Although large computers can implement

self-protection through IP protocols, their effectiveness will be greatly reduced when viruses invade, thereby affecting the robustness and reliability of the entire system. With the continuous development of science, the reliability of information is increasingly improving, but the reliability of information has been seriously affected. Therefore, it is necessary to strengthen the reliability of information and develop more advanced information security defense technologies to effectively prevent various network attacks.

4.2 Incorrect usage by computer network operators

For computer networks, their substantive security depends on their users. Therefore, they must possess good professional knowledge and abilities to effectively master and operate computers, thereby maximizing resource utilization and avoiding serious network attacks caused by improper behavior. Due to the development and popularization of technology, many new types of computers can monitor and control the running status of the system in real time through simple programming and configuration, effectively preventing abnormal operation of the computer. In addition, proper computer operation can also protect the security of the computer, prevent it from being stolen, tampered with, or destroyed, thereby protecting the normal operation of the computer and the integrity of data. Through in-depth research and practice, we should strive to improve our grasp of the usage process to avoid the occurrence of such problems. Only by operating in the correct way can the normal operation of the system be maintained.

5. SECURITY PRECAUTIONS FOR COMPUTER NETWORKS UNDER THE BACKGROUND OF BIG DATA

5.1 Strengthen the prevention of computer viruses

With the rapid advancement of network science, the virus attack capability of computers has significantly increased. However, the complexity and diversity of viruses still exist, making virus cleaning tasks increasingly difficult. For this reason, we should take more advanced warning measures to maximize the security of computers. In order to effectively address computer security risks, we must take proactive measures. Firstly, we must take preventive measures, such as establishing a comprehensive firewall system and equipping it with various protection programs to prevent malicious attacks. In addition, our network security managers must also strengthen their personal professional knowledge, increase the ability of computers to resist viruses and hacker attacks, timely detect and deal with malicious programs on computers, reinforce computer hardware and software, take effective measures in a timely manner, effectively resist malicious attacks, and ultimately achieve effective computer security. By strengthening the protective measures of the computer network, the stability of the system has been greatly improved.

5.2 Repairing and Improving Computer Vulnerabilities

Users will generate a lot of data in the working process of computer systems. Under this background, the storage of network resources will also increase rapidly, and even show an explosive increase. This situation will also make the Internet network have many defects on the basis of bringing convenience to our daily life and management work. Therefore, in the process of users' work on the Internet network information system, various defects must be repaired. In order to fully adapt to the rapid development of Internet network information technology under the information background, relevant application personnel must recognize and realize the necessity of network vulnerability repair, and scientific and technological personnel should also increase the research on application software for network system defect recovery, which is conducive to solving the problem of Internet network defects and avoiding information leakage. Whether the network leakage recovery software can quickly repair the network leakage of the Internet, corresponding to the R&D personnel and scientific and technological workers, it is necessary to enhance the system's defense against viruses in the context of ensuring the safe and stable operation of the computer network system, and then optimize the original leakage recovery tools. In addition, in order to further improve the skills of network system leakage recovery, users must pay attention to the early use of recovery techniques when the computer system is not operating normally. This will be very important for further improving the efficiency of network operation.

6. ELABORATE ON COMPUTER NETWORK SECURITY TECHNOLOGY AND ITS APPLICATION IN NETWORK SECURITY MAINTENANCE

6.1 Firewall Technology

Firewall, as an important computer network security measure, has become a common phenomenon. Whether it is a private or commercial computer, almost every computer is equipped with a firewall, which includes application layer firewalls, packet filtering firewalls, etc. Their functions are different. The former aims to prevent unauthorized use, while the latter aims to prevent illegal activities and protect the normal operation of the computer system. Application layer firewalls are usually deployed on servers, which can fundamentally detect malicious software on the network and take effective measures to prevent its spread. Despite differences in the methods used, the combination of the two defense techniques can effectively reduce the threat of network viruses, thereby protecting the normal operation of the network.

6.2 Encryption Technology

By using advanced encryption algorithms, the original files can be encrypted, giving them higher privacy and integrity. The encrypted file cannot be cracked by any external attacker, greatly increasing the security of the data. With the rapid development of technology, data encryption technology has also made significant progress. Technical experts can easily implement symmetric encryption, where the encryption and decryption passwords are the same, effectively preventing data leakage. In addition, asymmetric encryption can also provide more comprehensive data encryption services, with more flexible, stable, and effective passwords.

6.3 Antivirus software

Antivirus software plays an important role in protecting computer network security. They can effectively detect and prevent malicious attacks. Almost every computer is equipped with 360 antivirus software, which can effectively protect the data in the computer. Therefore, it is increasingly favored by more and more people. In order to maximize the effectiveness of antivirus software, we must regularly update the virus database to detect and remove new viruses in a timely manner. Only in this way can we continuously improve the security and stability of computer networks.

7. CONCLUSION

Due to the flourishing development of science, current computer science technology is becoming increasingly sophisticated and applied in various fields. However, we must be vigilant because it has the advantages of openness, communication, reliability, and autonomy. Many malicious attackers can steal their sensitive personal information through their vulnerabilities, causing great harm to people's privacy and property. So, in order to ensure the security and robustness of computers, we must take effective measures, not only to strengthen network security, but also to better grasp big data and related computer network technologies, and thus achieve higher-level control.

REFERENCES

- [1] Guo, Haocheng, Yaqiong Zhang, Lieyang Chen, and Arfat Ahmad Khan. "Research on Vehicle Detection Based on Improved YOLOv8 Network." *Applied and Computational Engineering* 116 (2025): 161-167.
- [2] Jin, Yuhui, Yaqiong Zhang, Zheyuan Xu, Wenqing Zhang, and Jingyu Xu. "Advanced object detection and pose estimation with hybrid task cascade and high-resolution networks." In *2024 International Conference on Image Processing, Computer Vision and Machine Learning (ICICML)*, pp. 1293-1297. IEEE, 2024.
- [3] Liu, Y. et al. (2025). SPA: Towards A Computational Friendly Cloud-Base and On-Devices Collaboration Seq2seq Personalized Generation with Causal Inference. In: Hadfi, R., Anthony, P., Sharma, A., Ito, T., Bai, Q. (eds) *PRICAI 2024: Trends in Artificial Intelligence. PRICAI 2024. Lecture Notes in Computer Science()*, vol 15282. Springer, Singapore. https://doi.org/10.1007/978-981-96-0119-6_25
- [4] Saunders, E., Zhu, X., Wei, X., Mehta, R., Chew, J., & Wang, Z. (2025). The AI-Driven Smart Supply Chain: Pathways and Challenges to Enhancing Enterprise Operational Efficiency. *Journal of Theory and Practice in Economics and Management*, 2(2), 63–74. <https://doi.org/10.5281/zenodo.15280568>
- [5] Jiang, Gaozhe, et al. "Investment Advisory Robotics 2.0: Leveraging Deep Neural Networks for Personalized Financial Guidance." (2025).
- [6] Chen, Shujian, and Minhui Xie. "Augmenting Advertiser Decision Support with Generative AI and Interactive Analytics." (2025).
- [7] Tu, Tongwei. "Reliable Vehicle Platooning via Redundant 5G Link Aggregation in Smart Roads." (2025).

- [8] Ma, Haowei, et al. "Maternal and cord blood levels of metals and fetal liver function." *Environmental Pollution* 363 (2024): 125305.
- [9] Lu, Jingyuan, et al. "Chemotherapy-mediated lncRNA-induced immune cell plasticity in cancer immunopathogenesis." *International Immunopharmacology* 141 (2024): 112967.
- [10] Jiang, Xiaohong, et al. "Tumor Microenvironment Reprogrammed Bimetallic Hybrid Nanostimulator for Triggering Radio - Cuproptosis - Immunotherapy." *Advanced Healthcare Materials* 13.30 (2024): 2401902.
- [11] Ma, Haowei. "Automatic positioning system of medical service robot based on binocular vision." 2021 3rd International Symposium on Robotics & Intelligent Manufacturing Technology (ISRIMT). IEEE, 2021.
- [12] Zhao, S., Xu, Z., Zhu, Z., Liang, X., Zhang, Z., & Jiang, R. (2025). Short and Long-Term Renewable Electricity Demand Forecasting Based on CNN-Bi-GRU Model. *IECE Transactions on Emerging Topics in Artificial Intelligence*, 2(1), 1-15.
- [13] Luo, H., Wei, J., Zhao, S., Liang, A., Xu, Z., & Jiang, R. (2024). Intelligent logistics management robot path planning algorithm integrating transformer and gcnn network. *IECE Transactions on Internet of Things*, 2(4), 95-112.
- [14] Xu, Y., & Lin, Y. (2024, November). Exploring the Influence of User-Perceived Value on NEV-Enterprises Using an Empirical Computer Model. In 3rd International Conference on Financial Innovation, FinTech and Information Technology (FFIT 2024) (pp. 4-10). Atlantis Press.
- [15] Shan, X., Xu, Y., Wang, Y., Lin, Y. S., & Bao, Y. (2024, June). Cross-Cultural Implications of Large Language Models: An Extended Comparative Analysis. In International Conference on Human-Computer Interaction (pp. 106-118). Cham: Springer Nature Switzerland.
- [16] Wang, Y., Shen, Z., Chew, J., Wang, Z., & Hu, K. (2025). Research on the Cross-Industry Application of Autonomous Driving Technology in the Field of FinTech. *International Journal of Management Science Research*, 8(3), 13-27.
- [17] Chew, J., Shen, Z., Hu, K., Wang, Y., & Wang, Z. (2025). Artificial Intelligence Optimizes the Accounting Data Integration and Financial Risk Assessment Model of the E-commerce Platform. *International Journal of Management Science Research*, 8(2), 7-17.

Author Profile

Junshan Zhang (1987.11-), male, Han ethnicity, from Qingdao, Shandong Province, China. He holds a bachelor's degree and is an assistant engineer. His main research interests include network security management and information technology.