The Evolution of Computer Information and Network Security Technology: Trends, Challenges, and Future Directions

Yajie Chai

Henan China Tobacco Co., LTD., Xuchang Cigarette Factory Xuchang, Henan 461000

Abstract: ***Informatization and digitization are typical signs of the development of modern society. The impact of computer and network technology on people's production and life is huge, but its safety management is also worthy of attention. The article expounds the basic concept and importance of computer information network security technology, and analyzes various factors that lead to computer information network security risks. The actual application of firewall technology, digital encryption technology, vulnerability scanning technology, and cloud security technology is analyzed, and the development direction of computer information network security technology is prospected, hoping to provide reference for relevant practitioners.***

Keywords: Computer; Information network; Security technology; Development direction.

1. INTRODUCTION

Today, with the rapid development of social and economic growth, computer software technology and communication network technology have played an increasingly crucial role in people's production and life, especially in the era of big data based on relevant technologies, which has allowed people to enjoy the convenience brought by informatization. However, the security problems that follow the high informationization also threaten people's information security, so the research of computer information network security technology has been attached great importance to. Especially in the context of China's comprehensive promotion of the construction of smart cities and the Internet of All Things system, it is even more necessary to adopt advanced and reliable security technology mechanisms to ensure the stable development of social and economic society. Lin, Wang, and Hong [1] developed computational methods for the Poisson multinomial distribution, with applications in ecological inference and machine learning. In photonics, Tang et al. [2] focused on the design and optimization of shallow-angle grating couplers for vertical emission from indium phosphide devices. Xiangyu et al. [3] investigated 3D printing parameters for polyolefin elastomers using response surface methodology to optimize mechanical properties. Wu [4] addressed fault detection and prediction in cloud infrastructure to optimize resource usage. Ge [5] examined the politics of technology deployment in peace and conflict contexts. Tang, Zhao, and Yanjun [6] conducted a qualitative analysis of regional housing supply and demand imbalances in the U.S. using big data. Tu [7] proposed a platform-aware framework for intelligent 5G network test automation and issue diagnosis. Wang [8] developed predictive modeling for sortation and delivery optimization in e-commerce logistics. Meng et al. [9] applied deep learning to green warehousing logistics site selection and path planning. Wu [10] further explored fault detection and prediction models for resource optimization in cloud infrastructure. Chen [11] introduced a data quality quantized framework to ensure large-scale data integration in gig economy platforms. Yuan [12] presented efficient transformer-based techniques for processing medical texts in legal documents. Li, Wang, and Zhang [13] examined gamified data visualization in smart cities to foster citizen engagement in urban monitoring. Deng [14] proposed a homomorphic encryption-based mechanism for data integrity verification and anti-tampering in cloud storage environments. Zhou [15] developed a collaborative filtering model for digital precision distribution of social media content on private domain platforms in the automotive industry. Ren [16] introduced an enhanced graph convolutional network model for text classification, and further enhanced seq2seq models for role-oriented dialogue summary generation through adaptive feature weighting and dynamic statistical conditioning [17]. Yang et al. [18] proposed HGMatch, a match-by-hyperedge approach for subgraph matching on hypergraphs. Ukey et al. [19] focused on efficient continuous kNN joins over dynamic high-dimensional data. Finally, Lian and Chen [20] conducted research on complex data mining analysis and pattern recognition based on deep learning. Collectively, these studies reflect a broad interdisciplinary effort to advance computational modeling, optimize system performance, and address complex challenges across engineering, data science, and social domains.

2. OVERVIEW OF COMPUTER INFORMATION NETWORK SECURITY TECHNOLOGY

2.1 Concepts of technology

Computer information network security technology mainly refers to computer software, Database, information processing system of all kinds of application scenarios, in order to fully ensure that computer hardware, software and data information will not be malicious change, damage or theft, the use of a series of software technology, information processing technology. The former refers to the information security which is well known to the Volkswagen in modern society. The protection of information integrity, privacy and exploitable value is mainly the protection of informationintegrity, confidentiality and exploitablevalue under the Internet, mobile communication networks and even big data systems on the basis of logical security [1]. Since the birth of computer software technology and network technology, a series of risks have arisen as the value of the information and data involved has been recognized. On the one hand, computer hardware and software may themselves have certain defects in manufacturing, design or technical application, which causes data to be exposed to security risks when stored, transmitted or used; On the other hand, when using computers and networks, data security may also be compromised due to human negligence or malicious intent. Therefore, research on computer information network security technology has always been highly valued.

2.2 Importance

Since the birth of computer and network technology, people have made great strides in the path of informatization and digitalization. To date, computer software and the Internet have penetrated into all aspects of people's production and life, and all kinds of activities and elements of people' production and life can be processed as information data by computer software, stored, shared, transmitted and applied. Especially in the context of big data, the mining of the value of data information is particularly important, which is also an important trend in future social development. However, throughout the process, computer information network security problems have always existed and have created increasingly serious threats as the informatization society deepens its development. First, in the network age, both individuals and enterprises are involved in a large amount of confidential information, and the confidentiality and security of such information are of concern. If it is compromised or stolen, it may result in damage to personal or business interests. Secondly, in the operation of modern society, a large amount of information and data are needed, and the accuracy and completeness of these information and data may be impaired, which may also adversely affect the stability and security of society. Therefore, enhancing the application level of computer information network security technology is the key to ensure data information security in the information age, and is also an important guarantee for the development and application of big data and intelligent technology [2].

3. TYPES OF FACTORS THAT CAUSE COMPUTER INFORMATION NETWORK SECURITY TO BE THREATENED

3.1 Hardware and Software Defects

In computer network systems, both hardware and software need to be scientifically designed, manufactured using reliable processes, and the software needs to be optimized using science and technology. Therefore, if in the design, manufacture or optimization debugging problems, it is easy to lead to computer network system defects, these defects may directly affect the data information security[3]. For example, the poor quality of the hardware causes various types of failures, which may cause the stored data information to be corrupted. For example, software systems have vulnerabilities that cause data to be lost or stolen. Although computer software design and manufacturing techniques are becoming more and more sophisticated today, the risk of this defect in itself remains.

3.2 Computer Viruses

Computer viruses have always been an important factor in threatening computer information network security, and as a destructive program, they have a strong latency, contagion and destruction. From common Trojan viruses and worms to various types of system viruses, once they bypass the system security system or program for intrusion, it is easy to cause the information data in the user's computer to be destroyed or stolen. In the context of the Internet,

computer viruses are constantly lurking in various fields, and the slightest inadvertence may threaten people's computer information network security.

3.3 Unlawful Hacking Factors

In the context of the information age, the value of data information is self-evident, so there are also people who use modern technology in the computer Internet to conduct unlawful activities such as hacking and theft for profit. Hackers primarily act against the interests of others by designing programs or exploiting vulnerabilities in computer networks to bypass cracking computer software security programs. Although China has now perfected relevant security regulations, the battle between computer information network security technology and hackers will be long-term, driven by interests.

3.4 Use of normative and rigorous elements

Now the computer network technology has entered all aspects of people's production and life, in people's daily use of computers and the Internet, may be due to the operation of the normative, rational, resulting in data information security threats [4]. For example, the most important passwords in a routine security procedure were compromised because of inadequate protection of encrypted information; Clicking on, visiting unexplained links, websites, or downloading files that are not proven secure enough can cause your computer to become infected with viruses or be hacked; Computer security systems are not updated in a timely manner and not maintained properly, resulting in system vulnerabilities that cannot be fixed in a prompt manner or ineffective identification of new network virus intrusions.

4. STATUS AND TRENDS OF APPLICATION OF COMPUTER INFORMATION NETWORK SECURITY TECHNOLOGY

4.1 Types of currently common technologies

4.1.1 Firewall technology

Firewalls are the most classic and common security technology since the birth of computer networks. It is mainly composed of computer hardware and software, which is deployed at the boundaries of the internal network to monitor all kinds of data entering and leaving the internal network, avoiding malicious code and programs from invading the internal network and has achieved the purpose of protecting the internal networks data security. Firewall security technology plays a key role in the security management of the computer information network of an enterprise, and can effectively filter and isolate risk factors. Modern firewall technology not only monitors, filters and protects external information, but also limits the types of websites users visit based on their identity to avoid risky behaviors of users. In addition, by dividing different protection areas within the internal network, it is possible to avoid situations where security risks in local areas cause all internal network security problems. It is worth mentioning that with the continuous development of relevant technologies, firewall technology is no longer just a defensive computer information network security technology. Instead, it can actively collect and analyze data to determine the risk of external attacks, and achieve the prevention and control effect of internal filtering and external monitoring [5].

4.1.2 Vulnerability detection and remediation techniques

As mentioned above, computer network hardware and software may have some vulnerabilities affected by the design, process, operation or use of the computer network, leading to the emergence of security risks. For this reason, security technologies for scanning, detecting and fixing vulnerabilities have emerged. The technology mainly scans the security of computer networks from the hardware and software levels, finds vulnerabilities in them, and then repairs them. From a broader technical perspective, the application of vulnerability detection and repair technology is complementary to computer hardware and software update and optimization technology. That is, a vulnerability presenting a security risk is discovered through vulnerability detection, which provides a reference basis for computer network update optimization, after study and processing, forms typical characteristics information and repair patches for the vulnerability, and delivers to a weakness scanner for a comparative scan, discovers the vulnerabilities, and then repairs. Vulnerability detection and repair technology is accompanied by the development of computer network technology, and it continuously improves its ability to resist security risks from the perspective of the computer network itself.

4.1.3 Security backup and encryption technology

Encryption is a technology used by users to avoid loss or theft of critical information when they use computers and the Internet. Security backup is usually done by automating backup of important information, data, and files and storing them in a secure database or in a cloud database. Encryption technology is used throughout the various scenarios in which users use to manage information data, and static encryption is generally used in the storage place of data, to detect access eligibility when externally accessed, and to determine whether security risks exist. Dynamic encryption is generally used to ensure that data is difficult to decipher and utilize even if it is illegally stolen by dynamic encryption means for different scenarios during the sharing of internal and external networks. With the further development of encryption technology, a higher level of security encryption mechanism has also emerged in the industry. In other words, when the encryption program determines that the data has been stolen or is in an externally deciphered state, it will automatically destroy the data, and the user can regain the data through the cloud backup platform. This approach can effectively avoid the illegal use of important data and has important applications in the management of work in today's enterprise units and key sectors.

4.2 Trends

4.2.1 Cloud Security Technology

Cloud security technology is a new computer information network security technology based on cloud computing and P2P technology in recent years. It mainly connects user computer equipment and information network platforms, based on big data analysis and monitoring, to form a larger security risk monitoring and virus killing network platform. In simple terms, this is a security monitoring and protection system based on the field of Internet, which can effectively utilize big data and modern software information technology, and form a large-scale, systematic security protection matrix by expanding the network virus resource library and technology resource library. In the future, cloud security technology will be the focus area of computer information network security technology research, and it will also be the key point of computer information networks security technology adaptation to socio-economic development.

4.2.2 Intelligent security technology

Intelligent intelligence is an important trend in the development of modern society, and the realization of intelligent intelligence mainly relies on computer software and network technology, so in computer information network security, intelligent intelligence is also a trend. At present, in the construction of smart factories, smart homes and even smart cities, through the configuration of expert system, intelligent analysis software and other forms, the initial formation of various viruses, security vulnerabilities and external intrusion risk intelligent monitoring, protection, repair mechanism. Smart security technology has typical automation, dynamic growth properties, It can effectively reduce the involvement of personnel to realize research and analysis of various security risks to continuously expand the scope of its security control, at the same time improve the ability of risk identification, security protection, and urgent handling of security issues, thereby promoting the continuous improvement of the security level of computer network systems. Obviously, the future computer information network security technology will be based on intelligent technology, achieving development from a static to a dynamic direction [6].

5. CONCLUSION

In summary, with the rapid development of modern society and economy, computer networks have played an important role in people's production life, but at the same time, they have created certain security risks. The current technical research on computer information network security has preliminarily formed a technical system represented by firewalls, vulnerability scanning and virus killing. However, in the context of further development in the information technology era, it is necessary to apply modern cloud technology and intelligent technology to computer information network security management through active technological upgrading and innovation, so as to lay a reliable foundation for the stable and healthy development of social and economic society.

REFERENCES

[1] Lin, Z., Wang, Y., & Hong, Y. (2023). The computing of the Poisson multinomial distribution and applications in ecological inference and machine learning. Computational Statistics, 38(4), 1851-1877.
[2] Tang, Y., Kojima, K., Gotoda, M., Nishikawa, S., Hayashi, S., Koike-Akino, T., ... & Klamkin, J. (2020). Design and Optimization of Shallow-Angle Grating Coupler for Vertical Emission from Indium Phosphide Devices.
[3] Xiangyu, G., Yao, T., Gao, F., Chen, Y., Jian, X., & Ma, H. (2024). A new granule extrusion-based for 3D printing of POE: studying the effect of printing parameters on mechanical properties with “response surface methodology”. Iranian Polymer Journal, 1-12.
[4] Wu, W. (2025). Fault Detection and Prediction in Models: Optimizing Resource Usage in Cloud Infrastructure.
[5] Ge, J. (2024). Technologies in Peace and Conflict: Unraveling the Politics of Deployment. Review International Journal of Research Publication and Reviews (IJRPR), 5(5), 5966-5971.
[6] Tang, Y., Zhao, S., & Yanjun, C. (2024). Regional Housing Supply and Demand Imbalance Qualitative Analysis in US based on Big Data.
[7] Tu, Tongwei. "AutoNetTest: A Platform-Aware Framework for Intelligent 5G Network Test Automation and Issue Diagnosis." (2025).
[8] Wang, J. (2025). Predictive Modeling for Sortation and Delivery Optimization in E-Commerce Logistics.
[9] Meng, Q., Wang, J., He, J., & Zhao, S. (2025). Research on Green Warehousing Logistics Site Selection Optimization and Path Planning based on Deep Learning.
[10] Wu, W. (2025). Fault Detection and Prediction in Models: Optimizing Resource Usage in Cloud Infrastructure.
[11] Chen, J. (2025). Data Quality Quantized Framework: Ensuring Large-Scale Data Integration in Gig Economy Platforms.
[12] Yuan, J. (2024, December). Efficient techniques for processing medical texts in legal documents using transformer architecture. In 2024 4th International Conference on Artificial Intelligence, Robotics, and Communication (ICAIRC) (pp. 990-993). IEEE.
[13] Li, X., Wang, J., & Zhang, L. (2025). Gamifying Data Visualization in Smart Cities: Fostering Citizen Engagement in Urban Monitoring. Authorea Preprints.
[14] Deng, X. (2025). Homomorphic Encryption-Based Data Integrity Verification and Anti-Tampering Mechanism in Cloud Storage Environment.
[15] 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).
[16] Ren, Z. (2024). VGCN: An Enhanced Graph Convolutional Network Model for Text Classification. Journal of Industrial Engineering and Applied Science, 2(4), 110–115. https://doi.org/10.5281/zenodo.13118430
[17] Z. Ren, "Enhancing Seq2Seq Models for Role-Oriented Dialogue Summary Generation Through Adaptive Feature Weighting and Dynamic Statistical Conditioninge," 2024 6th International Conference on Communications, Information System and Computer Engineering (CISCE), Guangzhou, China, 2024, pp. 497-501, doi: 10.1109/CISCE62493.2024.10653360.
[18] 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.
[19] 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.
[20] 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.

Author Profile

Yajie Chai male, Henan Province Xuchang City, zip code: 461000, Henan Tobacco Xuchang Cigarette Factory, November 1979, undergraduate.