DOI: 10.53469/wjimt.2025.08(04).10

Analysis on Network Information Security Guarantee System

Zhenyu Wang

Xinjiang Radio and Television Network Co., Ltd.,Urumqi, Xinjiang, 830000

Abstract: ***With the rapid development of information technology, the Internet has become an inseparable part of people's life, work and learning, and has a profound impact on our modern society. In particular, computer information systems, which use communication networks to achieve interconnection, data through the Internet for remote transmission, remote access and resource sharing process, hackers and illegal elements are also using them to implement network penetration, secret theft and even attack. With the increasing level of Internet informatization in all walks of life, the security of network information is becoming more and more important, and people are paying more and more attention to it. This paper mainly elaborates the main contents of network information security, and discusses the construction of network information security guarantee system from three aspects of security technology, laws and regulations and management system.***

Keywords: Network Information Security, Authentication Technology, Encryption Technology, Guarantee System.

1. INTRODUCTION

With the development of modern information technology such as "Internet plus", the integration and development of the Internet and traditional industries, and the deep integration of Internet information technology into personal, economic, social and other fields, the following network security incidents occur frequently, and network penetration and network attacks have become popular words. The deeper the integration and development of "Internet plus", the greater the impact and damage caused by network attacks. Network information security is not only related to personal information security, but also to the national economy and national security and stability. So network information security is a complex and comprehensive issue, and the rapid development of information technology has increased the difficulty of network security management. How to effectively ensure network information security has become an important issue worth pondering.

2. THE MAIN CONTENT OF NETWORK INFORMATION SECURITY

Network information security is a comprehensive discipline that involves multiple disciplines such as computer science, network technology, communication technology, cryptography, information security technology, and applied mathematics. With the development of network and information technology and changes in the real environment, network information security has extended from the "hard security" of physical and technological attributes to the "soft security" of media attributes. It mainly refers to protecting the security of hardware, software, and related data of the system in the network environment, preventing the network system from being damaged or leaking data information, and enabling the system to operate normally, reliably, and securely. Due to the wide coverage of network information security issues in current society, their nature often deviates from their true meaning, and even tends to generalize, especially politicize. Therefore, it is necessary to first have a clear understanding and comprehension of the main content and research scope of network information security.

In short, network information security refers to the security of physical lines and connections, network systems, operating systems and databases, application services, and personnel management involved in network interconnection and operation.

With the rapid development of computer and communication technology, computer information systems have been widely applied and penetrated into various industries and fields of society, and people's dependence on them is increasing. In fields such as politics, military, economy, science and technology, and business, important information resources are inputted, processed, stored, and transmitted through computer networks, providing people with rapid and efficient information services. If the protection of network information systems is not valued and the construction of information security guarantee systems is not strengthened, security vulnerabilities may cause huge economic losses and even threaten the survival of enterprises. The country's confidential information resources are bound to be easily stolen and destroyed illegally, which may cause huge losses to the national economy and even serious harm to national security. Network information security is an important issue related to national security and sovereignty, social stability, and economic development. Therefore, it is necessary to strengthen the construction of the network information security guarantee system, protect information assets that are crucial for its development and growth, and ensure the privacy, integrity, authenticity, and reliability of information. The need to protect the privacy, integrity, authenticity, and reliability of information has become one of the top priorities for the development of the whole society.

Lin et al. [1] employed transfer learning to enhance the modeling of annular aperture arrays and nanohole arrays, improving computational efficiency in optical simulations. For enterprise applications, Gong et al. [2] proposed an ensemble machine learning-based decision support system to optimize risk management strategies. In cybersecurity, Bohang et al. [3] developed an active learning framework with hyperparameter optimization for image steganalysis, significantly improving detection accuracy. Meanwhile, Zhao et al. [4] applied deep learning to optimize steel production scheduling, demonstrating AI's potential in industrial automation. AI has also been leveraged for disaster response, where Yao et al. [5] integrated drone technology with 3D printing to rapidly construct post-disaster shelters. In e-commerce, Song [6] explored AI-driven user-centric internal tools to enhance operational efficiency. For large-scale computational biology, Wu [7] investigated cloud infrastructure to support parallel computing in genetic disease research. In medical research, Wang et al. [8] constructed a cell atlas of the immune microenvironment in gastrointestinal cancers, providing insights into dendritic cell interactions. Smart city applications have also benefited from AI advancements. Li et al. [9] introduced gamified data visualization techniques to foster citizen engagement in urban monitoring, while Wang [10] applied Bayesian optimization for adaptive network reconfiguration in urban delivery systems. Further enhancing smart city data processing, Li et al. [11] proposed a named entity recognition framework for real-time urban data streams. In finance, Yang [12] demonstrated the effectiveness of LightGBM in predicting trends in the Chinese stock market. Lastly, Tang and Zhao [13] utilized neural networks to analyze the relationship between aging population distribution and real estate market dynamics, offering policy insights.

3. BUILD A NETWORK INFORMATION SECURITY GUARANTEE SYSTEM

The construction of a network information security guarantee system mainly focuses on three aspects: security technology, laws and regulations, and management systems. Technology is the premise, law is the guarantee, and system is the norm. All aspects are interconnected and mutually constrained, forming an organic whole. Network information security itself is a comprehensive governance issue that needs to be strengthened and improved in all aspects of development, continuously promoting the development of security technology, the soundness of laws and regulations, and the improvement of management systems.

3.1 Network Information Security Technology

Technology is the foundation and prerequisite of the network information security guarantee system. The struggle between network viruses and anti-virus, as well as infringement and anti infringement, is mainly reflected in the technical aspect. So focusing on the technical aspects of information security will effectively curb cybercrime. At present, security technology mainly adopts the following key technical means.

3.1.1 Network Authentication Technology

Due to the continuous increase in internet users and the rapid development of technology, some malicious individuals use hacking techniques to illegally steal and destroy information, endangering network security. Authentication technology is an important technique for preventing proactive attacks, aimed at checking the consistency of network information, verifying the authenticity of the sender's identity, determining whether the identity is genuine and legitimate, and then authorizing the sender to access information resources based on the determination results. At present, the main authentication technologies include identity authentication, message authentication, and digital signatures.

The authentication system is very important in network information security systems. Although it is the most basic security service, other security technology services must be based on the security of the authentication system, which is also the first line of defense for network information security. If the authentication system is attacked and invaded, other security technology measures may not be effective, and the authentication system is also the preferred target of hacker intrusion. Therefore, the security of network authentication technology should be highly valued.

3.1.2 Network Firewall Technology

Despite the emergence of various network security technologies in recent years, firewalls are still one of the most commonly used technologies for network system security protection. A firewall system can be software or hardware. The firewall is located at the boundary between the protected network and other networks, receiving data streams entering and exiting the protected network. It can prevent unauthorized access to important information in the internal network by external networks, and filter or control it according to the access control policies configured by the firewall. The firewall system not only protects network resources from external intrusion, but also intercepts confidential information transmitted by the protected network. Common firewall technologies include proxy service technology, packet filtering technology, etc., which can effectively enhance network security.

3.1.3 Network Information Encryption Technology

Network information encryption technology mainly encrypts information at the sending end during network transmission, uses certain encryption algorithms to convert plaintext into ciphertext, and then decrypts and restores the information at the receiving end. This can prevent illegal users from obtaining and intercepting the original data, thereby ensuring the confidentiality of network information.

At present, there are mainly two types of cryptographic technologies: conventional cryptography and public key cryptography. In regular passwords, the recipient and sender use the same key, meaning that the encryption key and decryption key are the same or equivalent. Famous conventional cryptographic algorithms such as DES in the United States and its various variants Triple DES, GDES, IDEA, etc., among which the DES cipher is widely used and has the greatest impact. The advantage of regular passwords is that they have strong confidentiality, but their keys must be transmitted through secure means. In public key cryptography, the recipient and sender use different keys, and it is almost impossible to derive the decryption key from the encryption key. Famous public key cryptography algorithms include RSA, knapsack cipher, elliptic curve EIGamal algorithm, etc. The most influential public key cryptographic algorithm is RSA, which can resist all known cryptographic attacks so far. The advantage of public key cryptography is that it can adapt to the openness requirements of the network, especially for convenient implementation of digital signatures and verification. But its algorithm is complex and the rate of encrypting data is relatively low. Of course, in practical applications, people usually combine conventional passwords with public key cryptography, such as using DES or IDEA to encrypt information and RSA to transmit session keys.

3.1.4 Disaster recovery mechanism

Another necessary measure to ensure network information security is to establish a reasonable and reliable data backup and recovery mechanism. The 9/11 attacks in the United States highlighted the importance of information backup. In this incident, some companies' core databases, including a large number of trade agreements, transaction records, and other archival information, could no longer be restored due to the lack of remote backup, resulting in incalculable losses. After this incident, various industries have increased their attention to information backup systems. Before the 9/11 attacks, although backing up data was also a necessary task, its execution process was not as precise or regular. However, it has now become a necessary task, and various data disaster recovery technologies for remote database backup, such as DataGuard and GoldGate for Oracle databases, have rapidly developed and become popular in the past decade. The National Library of Medicine in Washington, D.C., in the United States, remotely backs up its data information to Pennsylvania through the internet. The reason for choosing this state is because it has been found through statistics that the probability of earthquakes occurring there is the lowest, indicating the importance it places on data backup. The disaster recovery mechanism is crucial for the recovery of data information whose security has been compromised.

3.2 The soundness of laws and regulations

The establishment of sound laws and regulations on network information security is mainly reflected in the establishment of the main body, responsibilities, and obligations in network information security management. It mainly elaborates on the goals and principles of the law, clarifies the rights and obligations of various entities in the network, establishes website identity authentication, implements network backend real name system, protects the privacy rights of network entities, promotes network information confidentiality system, and improves the regulatory procedures of administrative organs for network information security.

Given the fast pace of development in the online society and the lagging behind of regulatory legislation, a separate law can be established specifically to protect the security of online commercial information and personal information. For example, legislation can be enacted to safeguard various aspects of network information security, such as electronic payments, to ensure personal information security, timely address issues in network development, network regulation, and network services, and improve relevant provisions for network information security.

Each enterprise and institution shall formulate and organize the implementation of its own network and information security management rules and regulations in accordance with relevant laws, regulations, and work requirements on network and information security. To clarify the various responsibilities in network and information security work, standardize the internal control and management system of computer information network systems, and effectively ensure the network and information security of our unit.

3.3 Improvement of Management System

Network information security not only involves technology and legislation, but also management. It is important to enhance the security of important network information by strengthening and improving management systems. In order to adapt to the rapid development of information technology and the prominent demand for information security, many international standardization organizations and institutions have started researching and developing information security standards early on to strengthen network information security management, such as the Department of Defense (DOD) of the United States and the International Organization for Standardization (ISO). As early as 2014, China established the "Central Leading Group for Cybersecurity and Informatization", indicating that the country attaches great importance to cybersecurity and informatization work. At the same time, it requires the Ministry of Industry and Information Technology and the Ministry of Public Security to do a good job in cybersecurity and related information security management, maintain national information security, supervise and handle cybersecurity public opinion, and build a national information security guarantee system.

Developing and improving network security management systems is to clarify the permissions and responsibilities of management personnel in network information systems, establish personnel management systems, and also improve basic security measures such as network usage permissions, identity authentication, firewalls, and data backup, and develop computer information system management systems. Strengthen the management of information security technical personnel, improve management systems, implement responsibility systems, while enhancing the comprehensive quality of network information security management practitioners, improving their ability in network security protection technology, strengthening their awareness of network security, and taking the management of network information security work to a new level to meet the practical needs of rapid development of information technology.

4. CONCLUSION

Building a network information security guarantee system is a systematic project that requires the gradual construction and development of various aspects such as security technology, laws and regulations, and management systems. However, network information security guarantee work is crucial for personal information, enterprise development, social stability, national economic development, and national security. We must attach great importance to network information security work. In short, "without network security, there can be no national security, and without informatization, there can be no modernization." In the new environment, the network security situation is becoming increasingly severe. In order to ensure national security and social stability, we need to increase the importance of network information security, strengthen research on network information security technology, enhance awareness of network information security, and attach importance to the application of network information security technology, establish and improve laws and regulations, strengthen information security management, and ensure the security of network information.

REFERENCES

[1] Lin, Y., Liu, J., Cao, Y., Cao, Y., & Wang, Z. (2025). Transfer learning-enhanced modelling of annular aperture arrays and nanohole arrays. Physica Scripta, 100(3), 036003.

[2] Gong, C., Lin, Y., Cao, J., & Wang, J. (2024, October). Research on Enterprise Risk Decision Support System Optimization based on Ensemble Machine Learning. In Proceeding of the 2024 5th International Conference on Computer Science and Management Technology (pp. 1003-1007).

[3] Bohang, L., Li, N., Yang, J. et al. Image steganalysis using active learning and hyperparameter optimization. Sci Rep 15, 7340 (2025). https://doi.org/10.1038/s41598-025-92082-w

[4] Zhao, H., Chen, Y., Dang, B., & Jian, X. (2024). Research on Steel Production Scheduling Optimization Based on Deep Learning.

[5] Yao, T., Jian, X., He, J., & Meng, Q. (2025). Drone-3D Printing Linkage for Rapid Construction of Sustainable Post-Disaster Temporary Shelters.

[6] Song, X. (2025). User-Centric Internal Tools in E-commerce: Enhancing Operational Efficiency Through AI Integration.

[7] Wu, W. (2024). Research on cloud infrastructure for large-scale parallel computing in genetic disease.

[8] Wang, Y., Yang, T., Liang, H., & Deng, M. (2022). Cell atlas of the immune microenvironment in gastrointestinal cancers: Dendritic cells and beyond. Frontiers in Immunology, 13, 1007823.

[9] Li, X., Wang, J., & Zhang, L. (2025). Gamifying Data Visualization in Smart Cities: Fostering Citizen Engagement in Urban Monitoring. Authorea Preprints.

[10] Wang, J. (2025). Bayesian Optimization for Adaptive Network Reconfiguration in Urban Delivery Systems.

[11] Li, X., Wang, J., & Zhang, L. (2025). Named entity recognition for smart city data streams: Enhancing visualization and interaction. Authorea Preprints.

[12] Yang, J. (2025). Application of LightGBM in the Chinese Stock Market.

[13] Tang, Y., & Zhao, S. (2025). Research on Relationship Between Aging Population Distribution and Real Estate Market Dynamics based on Neural Networks.