Computer Network Security Management and Maintenance

Shengye Weng

Civil Aviation Administration of China East China Air Traffic Management Bureau Shanghai 200335

Abstract: ***Computer network security management and maintenance are key tasks to ensure data security and business continuity in network systems. By formulating and implementing comprehensive security management strategies, conducting risk assessments and vulnerability scans, establishing incident response mechanisms, and enhancing employee security awareness, network threats can be effectively resisted. At the same time, the security configuration of network devices, real-time monitoring and log analysis of network traffic, and regular backup and recovery drills of data provide solid guarantees for the stable operation of network systems. In summary, network security management and maintenance is a systematic project that requires continuous investment to ensure the security and stability of the network environment.***

Keywords: Computer network; Safety management; Maintenance.

1. INTRODUCTION

In the digital age, the popularization and widespread application of computer networks have greatly promoted social progress and development, but at the same time, it has also made network security issues increasingly severe. Frequent incidents such as personal information leaks, attacks on corporate data, and even threats to critical national infrastructure have caused significant economic losses and security risks to society. Therefore, strengthening the management and maintenance of computer network security has become an urgent need to safeguard personal privacy, ensure stable business operations, and national security. This article delves into the strategies and practices of computer network security management, and proposes effective maintenance measures aimed at building a more secure and stable network environment. A fundamental technical hurdle in computer vision is addressed by Peng, Zheng, and Chen (2024) with a dual-augmentor framework for domain generalization in 3D human pose estimation, and further by Peng et al. (2023) through RAIN, a method for black-box domain adaptation via input and network regularization [1, 2]. These adaptive AI principles extend beyond vision to logistics and innovation ecosystems, as seen in Zhang's (2024) use of cohesive hierarchical clustering for dynamic power emergency material allocation and Zhou and Cen's (2024) investigation into ChatGPT-like AI's impact on user entrepreneurship [3, 4]. The capture and analysis of human motion and physiological states are critical application areas. Guo (2025) utilized IMUs and LSTM networks for real-time motion recognition data completion [5], while We et al. (2025) leveraged multimodal physiological data for intelligent anesthesia depth monitoring [6]. On a societal scale, Su et al. (2025) structurally assessed family and educational influences on student health behaviors [7], and Yang (2025) optimized cloud site reliability via synthetic monitoring, underscoring the infrastructure supporting these applications [8]. For autonomous and generative systems, enhancing trust and fidelity is paramount. Tang et al. (2026) proposed SVD-BDRL, a blockchain-enhanced trustworthy framework for autonomous driving decisions [9], and Lu et al. (2025) developed NeuroDiff3D, a diffusion model for viewpoint-consistent 3D generation [10]. Complex data integration in governance is tackled by Zhang (2025) using a knowledge graph-enhanced multimodal AI framework for tax compliance [11]. Enhancing environmental perception, Xie et al. (2025) introduced MARNet for robust point cloud completion via cross-modal fusion [12], building upon earlier cyber-physical systems like the camera-based bridge monitoring framework by Hou et al. (2017) [13]. In the digital economy, Tian et al. (2025) applied cross-attention multi-task learning for innovative ad recall [14]. However, the security of the underlying data fabric is critical, as addressed by Zhang, Bai, and Luo (2025) with an AI-driven cloud security monitoring system [15]. The privacy challenge in collaborative AI is met by Deng and Yang's (2025) defenses against membership reasoning attacks in federated learning [16] and Sultan et al.'s (2026) FedGuard framework for secure collaborative anti-money laundering [17]. Finally, specialized motion analysis is advanced by Zhu, Yu, and Li (2025) through SAGCN, a spatiotemporal graph network integrated with IoT for tennis motion analysis [18].

2. OVERVIEW OF COMPUTER NETWORK SECURITY

2.1 Definition and Importance of Network Security

Network security is the process of protecting data in computer network systems from unauthorized access, leakage, modification, destruction, or theft. It covers the security of hardware, software, and all information transmitted during the network system. With the popularization of the Internet and the rapid development of technology, network security has become the key to maintain national security, social stability and personal privacy. It is not only related to technical defense and protection, but also involves comprehensive considerations from multiple dimensions such as laws and regulations, management strategies, and user behavior.

2.1.1 For individuals, network security is directly related to the protection of personal privacy

In the digital era, personal information such as ID number, bank card number, address and telephone has become an important target of network attacks. Once leaked, it may lead to serious consequences such as property damage and identity theft. Therefore, strengthening network security protection and protecting personal privacy are the basic needs and rights of every netizen.

2.1.2 For enterprises, network security is a matter of life and death

The core data, trade secrets, and intellectual property of a company are the key to its competitiveness. Once a cybersecurity incident occurs, it may not only lead to data loss and business interruption, but also trigger a chain reaction such as legal disputes and damage to brand image. Therefore, enterprises must attach great importance to network security work, establish a sound network security management system, and ensure the stability and security of business operations.

2.1.3 For society, cybersecurity is an important cornerstone for maintaining social stability and national security
With the popularization and application of the Internet, the network has become an important platform for information dissemination, social exchanges and public services. Once a cybersecurity issue erupts, it may quickly spread to various fields, causing social panic, chaos, and even crisis. Therefore, strengthening network security management, preventing and combating illegal and criminal activities on the internet, and maintaining order and security in cyberspace are the joint responsibilities of the state and society.

2.2 Types of Network Security Threats

There are various security threats in the computer network environment. Among them, viruses, hacker attacks, and malicious software are the three most common and serious threats. A virus is a type of malicious software that has the ability to self replicate and infect, and it can quickly spread and destroy data in computer networks. Hackers use technological means to illegally invade others' computer systems, steal data, tamper with information, or carry out other destructive behaviors. Malicious software encompasses various forms such as viruses, worms, Trojan horses, etc. They deceive users into downloading and executing through deception, disguise, and other means, thereby causing damage to computer systems. These cybersecurity threats manifest in various forms, including but not limited to email scams, phishing websites, malicious software download links, and more. They may not only lead to user data leakage and property damage, but also disrupt the normal operation of computer systems, affecting business continuity and stability. More seriously, some hacker organizations or attackers with national backgrounds may exploit cybersecurity vulnerabilities to engage in cyber warfare or information theft activities, posing a serious threat to national security and social stability. Therefore, strengthening the awareness of network security protection and the application of technological means are of crucial significance for resisting various network security threats.

3. COMPUTER NETWORK SECURITY MANAGEMENT

3.1 Security Management Strategies and Standards

3.1.1 The necessity of developing and implementing network security policies

Developing and implementing network security strategies is the primary task in building a network security system. With the increasingly complex network environment and diverse threats, a clear and comprehensive security strategy can provide organizations with clear guidance and ensure that all security activities revolve

around a common goal. Meanwhile, implementing these strategies can effectively prevent, detect, and respond to network security threats, reduce potential risks, and ensure data assets and business continuity.

3.1.2 Specific Content of Security Policy

Security policies should cover multiple aspects, including but not limited to access control policies, data protection policies, etc. Access control policy is a key measure to ensure that only authorized users can access specific resources. By implementing mechanisms such as identity authentication, permission allocation, and access auditing, unauthorized access and data leakage can be effectively prevented. The data protection strategy focuses on the security of data during transmission, storage, and processing, including measures such as data encryption, data backup and recovery, data classification and identification, to ensure the confidentiality, integrity, and availability of data.

3.2 Security Risk Assessment and Vulnerability Scanning

3.2.1 Methods and processes of risk assessment

Security risk assessment is the process of identifying, analyzing, and evaluating network security risks, providing a basis for developing targeted protective measures. The evaluation method includes qualitative and quantitative analysis, which involves collecting relevant information, identifying potential threats and vulnerabilities, assessing the likelihood and impact of risk occurrence, and forming a complete risk assessment report. The evaluation process should ensure comprehensiveness, objectivity, and reproducibility for continuous monitoring and updating of risk conditions.

3.2.2 Vulnerability scanning techniques and tools

Vulnerability scanning is an important means of discovering potential security vulnerabilities in network systems. Modern vulnerability scanning tools utilize automation technology and the latest vulnerability information database to comprehensively scan and detect network systems, quickly identifying potential security risks. These tools can not only help organizations discover known vulnerabilities, but also discover some unknown and hidden vulnerabilities, providing strong support for vulnerability repair.

3.2.3 Vulnerability fixes and patch management

After discovering vulnerabilities, organizations should take timely measures to repair and reinforce them. This includes installing security patches, updating system configurations, adjusting security policies, etc. At the same time, the organization should establish an effective patch management mechanism, regularly detect and update the system patch library, and ensure that all systems can obtain the latest security fixes in a timely manner. Vulnerability repair and patch management is a continuous process that requires organizations to invest sufficient resources and energy to maintain the security of network systems.

3.3 Security Incident Response and Handling

3.3.1 Establish a network security incident response mechanism

Establishing a network security incident response mechanism is an important guarantee for addressing network security threats. The mechanism should include key elements such as event reporting process, composition and responsibilities of emergency response team, and event handling process. By clarifying the division of responsibilities, establishing emergency contact mechanisms, and developing detailed response plans, organizations can quickly initiate emergency response procedures in the event of a security incident, effectively control the development of the situation, and reduce losses.

3.3.2 Emergency Response Process for Events

The emergency response process usually includes stages such as event discovery and reporting, preliminary assessment and classification of events, initiation of emergency response, event handling and recovery, and event analysis and summary. At each stage, the organization should operate according to established procedures to

ensure fast and accurate handling of security incidents. Especially during the event handling and recovery phase, organizations should prioritize restoring critical business functions and reducing the impact on users.

3.3.3 Reducing the Impact of Events and Recovery Measures

In order to minimize the impact of security incidents on the organization and restore normal system operation as soon as possible, the organization should develop detailed recovery plans and measures. This includes data recovery and backup verification, implementation of Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP), establishment of communication and coordination mechanisms, and post event evaluation and improvement. By implementing these measures, organizations can minimize the losses caused by security incidents and quickly restore business operations.

3.4 Safety Training and Awareness Enhancement

3.4.1 Regularly provide network security training to employees

Regular cybersecurity training for employees is an effective way to enhance the overall security level of the organization. The training content should cover basic knowledge of network security, the latest threat trends, security operation norms, and emergency response processes. Through training, employees can understand the importance of network security, identify potential security risks, and take necessary preventive measures. In addition, training should also focus on practical operations and case analysis to enhance employees' practical and coping abilities.

3.4.2 Enhance employees' safety awareness and operational skills

In addition to regular training, organizations should also take various measures to enhance employees' safety awareness and operational skills. This includes developing and implementing security policies and operating procedures, establishing security incentive mechanisms and punishment measures, regularly issuing security alerts and warning information, and encouraging employees to participate in security vulnerability reporting.

The implementation of these measures can stimulate employees' attention and sense of responsibility towards network security, promote their conscious compliance with security norms and operating procedures, and thus enhance the overall security level of the organization.

4. MAINTENANCE OF COMPUTER NETWORK SECURITY

4.1 Security configuration and management of network devices

As the foundation of network connectivity, the security configuration and management of network devices are the first line of defense to ensure network security.

4.1.1 Firewall Configuration and Management

Firewall is an important barrier for network security. By formulating and implementing security policies, it filters and controls data packets entering and leaving the network, preventing potential malicious access and attacks. The configuration of firewalls should be customized based on the security needs of the organization, including defining access control lists (ACLs), implementing network address translation (NAT), configuring virtual private networks (VPNs), etc. In addition, regularly manage and maintain the firewall, such as updating the rule base, checking log files, etc., to ensure its effectiveness and responsiveness.

4.1.2 Deployment and Monitoring of Intrusion Detection Systems

Intrusion detection systems (IDS) can monitor abnormal behavior in the network in real-time, identify potential security threats, and issue timely alerts. The deployment of IDS should be reasonably planned based on network structure and security requirements to ensure comprehensive monitoring of critical areas and traffic. At the same time, it is necessary to regularly update the rule library and signature library of IDS to cope with the constantly

evolving network threats. Through real-time monitoring by IDS, organizations can promptly detect and respond to potential security incidents, preventing the deterioration of the situation.

4.1.3 Regular updates and upgrades of network equipment

With the continuous evolution of network threats, security vulnerabilities in network devices are also constantly being discovered. Therefore, regular updates and upgrades of network equipment are crucial. This includes updates to the operating system, security software, firmware, etc., to ensure that the device can withstand the latest security threats. At the same time, it is necessary to pay attention to the security announcements and patches released by manufacturers, and timely manage the patches of devices to prevent known vulnerabilities from being exploited.

4.2 Network Traffic Monitoring and Log Analysis

Network traffic monitoring and log analysis are important means of maintaining network security. Through real-time monitoring of network traffic and in-depth analysis of logs, potential security threats can be identified.

4.2.1 Real time monitoring of network traffic

Real time monitoring of network traffic can help organizations understand network usage and potential security risks. By analyzing traffic data, abnormal traffic patterns can be identified, such as DDoS attacks, malicious scans, etc. In addition, monitoring network traffic can help organizations optimize network performance and enhance user experience. To achieve real-time monitoring, organizations can deploy network traffic analysis tools such as NetFlow, sFlow, etc. to collect and analyze traffic data.

4.2.2 Collection, Analysis, and Storage of Logs

Logs are important sources of information for recording network devices and system activities. By collecting, analyzing, and storing logs, organizations can identify potential security threats, trace attack sources, and assess the scope of impact of security events. In order to effectively manage log data, organizations should establish a log management system to centrally store, classify, and index log data. At the same time, it is necessary to regularly review and analyze the logs to identify potential abnormal activities and security incidents. In addition, to ensure the integrity and traceability of log data, it is necessary to encrypt and backup the log data.

4.2.3 Identify potential security threats through log analysis

Log analysis is a crucial step in identifying potential security threats. Through in-depth mining and correlation analysis of log data, security incidents such as abnormal login attempts, malicious software activity, and data breaches can be discovered. In order to improve the efficiency and accuracy of log analysis, organizations can introduce automated analysis tools and machine learning algorithms to intelligently analyze and alert log data. In addition, establish an emergency response mechanism to quickly take action and reduce losses when security threats are detected.

4.3 Backup and Recovery Management

Backup and recovery management is an important means to ensure data security and business continuity.

4.3.1 Regularly backing up important data and systems

Regularly backing up important data and systems can prevent data loss caused by hardware failures, human errors, or malicious attacks. The backup strategy should be customized based on the importance of the data and the recovery time objective (RTO). For critical business data and systems, a strategy combining regular full backup and incremental backup should be implemented to ensure the integrity and availability of backup data.

4.3.2 Development and Implementation of Disaster Recovery Plan

A disaster recovery plan is an important solution for dealing with serious cybersecurity incidents or catastrophic accidents. The plan should clearly define the goals, scope, processes, and resource requirements for disaster recovery, and conduct regular drills and validations. By developing and implementing disaster recovery plans, organizations can quickly restore business operations and data access capabilities in the event of a serious security incident.

4.3.3 Data recovery drill and verification

Data recovery drills and validation are key steps in ensuring the effectiveness of disaster recovery plans. By simulating actual security incidents or disaster scenarios, organizations can verify the execution of recovery processes and whether the recovery time meets expectations. At the same time, potential issues and deficiencies during the recovery process can be identified and adjusted and optimized in a timely manner. Through regular data recovery drills and validation, organizations can continuously improve their ability to respond to security threats and the efficiency of data recovery.

5. CONCLUSION

In summary, computer network security management and maintenance is a complex and ongoing task that requires us to work together at multiple levels, including technology, management, and personnel, to form a comprehensive security protection system. By formulating scientific security strategies, strengthening security monitoring and emergency response, and enhancing personnel security awareness and skills, we can effectively resist various network threats and ensure the security of data assets and business continuity. In the future, with the continuous advancement of technology and changes in the threat situation, we still need to constantly explore and innovate to cope with new challenges, ensure the security and stability of the computer network environment, and provide strong guarantees for the healthy development of the digital economy.

REFERENCES

[1] Peng, Qucheng, Ce Zheng, and Chen Chen. "A Dual-Augmentor Framework for Domain Generalization in 3D Human Pose Estimation." Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2024.
[2] Peng, Qucheng, et al. "RAIN: regularization on input and network for black-box domain adaptation." Proceedings of the Thirty-Second International Joint Conference on Artificial Intelligence. 2023.
[3] Zhang, X. (2024). Research on Dynamic Adaptation of Supply and Demand of Power Emergency Materials based on Cohesive Hierarchical Clustering. Innovation & Technology Advances, 2(2), 59–75. https://doi.org/10.61187/ita.v2i2.135
[4] Zhou, J., & Cen, W. (2024). Investigating the Effect of ChatGPT-like New Generation AI Technology on User Entrepreneurial Activities. Innovation & Technology Advances, 2(2), 1–20. https://doi.org/10.61187/ita.v2i2.124
[5] Guo, Y. (2025, May). IMUs Based Real-Time Data Completion for Motion Recognition With LSTM. In Forum on Research and Innovation Management (Vol. 3, No. 6).
[6] We, X., Lin, S., Pruś, K., Zhu, X., Jia, X., & Du, R. (2025). Towards Intelligent Monitoring of Anesthesia Depth by Leveraging Multimodal Physiological Data. International Journal of Advance in Clinical Science Research, 4, 26–37. Retrieved from https://www.h-tsp.com/index.php/ijacsr/article/view/158
[7] Su, Z., Yang, D., Wang, C., Xiao, Z., & Cai, S. (2025). Structural assessment of family and educational influences on student health behaviours: Insights from a public health perspective. Plos one, 20(9), e0333086.
[8] Yang, Y. (2025). Research on Site Reliability Optimization Technology Based on Synthetic Monitoring in Cloud Environments.
[9] Tang, Z., Feng, Y., Zhang, J., & Wang, Z. (2026). SVD-BDRL: A trustworthy autonomous driving decision framework based on sparse voxels and blockchain enhancement. Alexandria Engineering Journal, 134, 433-446.
[10] Lu, K., Sui, Q., Chen, X., & Wang, Z. (2025). NeuroDiff3D: a 3D generation method optimizing viewpoint consistency through diffusion modeling. Scientific Reports, 15(1), 41084.
[11] Zhang, T. (2025). A Knowledge Graph-Enhanced Multimodal AI Framework for Intelligent Tax Data Integration and Compliance Enhancement. Frontiers in Business and Finance, 2(02), 247-261.

[12] Xie, J., Zhang, L., Cheng, L., Yao, J., Qian, P., Zhu, B., & Liu, G. (2025). MARNet: Multi-scale adaptive relational network for robust point cloud completion via cross-modal fusion. Information Fusion, 103505.
[13] HOU, R., JEONG, S., WANG, Y., LAW, K. H., & LYNCH, J. P. (2017). Camera-based triggering of bridge structural health monitoring systems using a cyber-physical system framework. Structural Health Monitoring 2017, (shm).
[14] Q. Tian, D. Zou, Y. Han and X. Li, "A Business Intelligence Innovative Approach to Ad Recall: Cross-Attention Multi-Task Learning for Digital Advertising," 2025 IEEE 6th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), Shenzhen, China, 2025, pp. 1249-1253, doi: 10.1109/AINIT65432.2025.11035473.
[15] Y. Zhang, Z. Bai and Q. Luo, "AI-Driven Cloud Computing Data Security Monitoring and Response System," 2025 International Conference on Advances in Electrical Engineering and Computer Applications (AEECA), Dalian, China, 2025, pp. 817-821, doi: 10.1109/AEECA65693.2025.00148.
[16] Deng, X., & Yang, J. (2025, August). Multi-Layer Defense Strategies and Privacy Preserving Enhancements for Membership Reasoning Attacks in a Federated Learning Framework. In 2025 5th International Conference on Computer Science and Blockchain (CCSB) (pp. 278-282). IEEE.
[17] Sultan, N., Patwar, N., Wei, X., Chew, J., Liu, J., & Du, R. (2026). FedGuard: A Robust Federated AI Framework for Privacy-Conscious Collaborative AML, Inspired by DARPA GARD Principles. International Academic Journal of Social Science, 2, 1–16. https://doi.org/10.5281/zenodo.18253151
[18] Zhu, Y., Yu, W., & Li, R. (2025). SAGCN: A spatiotemporal attention-weighted graph convolutional network with IoT integration for adolescent tennis motion analysis. Alexandria Engineering Journal, 128, 652-662.