DOI: 10.53469/ijomsr.2025.08(08).08

Computer Information Security Issues and Solutions

Yingying Sun

Xinjiang Tianshan Vocational and Technical University Urumqi 830017, Xinjiang

Abstract: ***With the rapid development of information technology, computer information security issues are becoming increasingly severe, including frequent data breaches, virus attacks, hacker intrusions, and so on. These issues not only threaten personal privacy, but also pose significant challenges to corporate and national security. To address these issues, it is necessary to strengthen security awareness training, improve virus killing technology, and implement multi-level security strategies such as data encryption, firewall settings, and regular security audits. At the same time, we will promote the construction of laws and regulations on cybersecurity, strengthen international cooperation, and jointly address increasingly complex cybersecurity challenges. Build a robust network security defense line through comprehensive measures.***

Keywords: Computer; Information security issues; Countermeasure.

1. INTRODUCTION

In today's rapidly developing information technology, computer information security issues are becoming increasingly prominent and have become a focus of attention for all sectors of society. From personal privacy breaches to corporate data theft, to national infrastructure being subjected to cyber attacks, information security risks are ubiquitous. Therefore, in-depth exploration of computer information security issues and proposing practical and feasible solutions are of great significance for protecting personal privacy, maintaining social stability, and promoting economic development. This article aims to analyze the current challenges faced and explore ways to address them. Ding and Wu (2024) provided a comprehensive systematic review of self-supervised learning techniques for biomedical signal processing, specifically focusing on ECG and PPG signals[1]. In recommendation systems, Han and Dou (2025) developed a novel user recommendation method integrating hierarchical graph attention networks with multimodal knowledge graphs[2], while Li, Wang, and Lin (2025) proposed a graph neural network enhanced sequential recommendation method for cross-platform ad campaigns[3]. Wang (2025) addressed data challenges in recommendation systems through joint training of propensity and prediction models using targeted learning for data missing not at random[12]. Content creation and authoring saw innovations with Hu (2025) introducing low-cost 3D authoring via guided diffusion in GUI-driven pipelines[4]. Industrial applications were advanced through multiple approaches: Tan et al. (2024) developed highly reliable CI-JSO based densely connected convolutional networks using transfer learning for fault diagnosis[5]; Tu (2025) created ProtoMind for modeling-driven NAS and SIP message sequence modeling for smart regression detection[6]; and Xie and Liu (2025) optimized industrial monitoring systems through InspectX, leveraging OpenCV and WebSocket for real-time analysis[7]. Advertising technology was enhanced by Zhang, Yuhan (2025) through AdOptimizer, a self-supervised framework for efficient ad delivery in low-resource markets[8], while the same author also contributed to development tools with InfraMLForge for rapid LLM development and scalable deployment[9]. System reliability engineering was addressed by Zhu (2025) through REACTOR, incorporating automated causal tracking and observability reasoning[10]. Finally, business applications were explored by Zhuang (2025) who examined the evolutionary logic and theoretical construction of real estate marketing strategies under digital transformation[11].

2. THE MAIN PROBLEMS FACED BY COMPUTER INFORMATION SECURITY

2.1 Physical security issues

Physical security is the first line of defense for computer information security. However, there are many potential threats in reality. Firstly, human destructive behavior cannot be ignored. Intentional destruction and illegal intrusion may not only cause physical damage to hardware devices, but also put important data at risk of leakage. These behaviors are often initiated by criminals or competitors with the aim of disrupting the normal operation of the system or stealing sensitive information. Secondly, force majeure factors such as earthquakes, fires, floods, and power outages can also have a devastating impact on computer systems. Equipment failures, such as sudden failures of critical hardware such as servers, routers, switches, etc., can also seriously affect the stable operation of information systems. Therefore, strengthening the security protection of physical facilities, such as establishing disaster prevention and preparedness systems, implementing strict security monitoring and inspection systems, is an important means to ensure computer information security.

2.2 Network level security issues

The network level is the focus and difficulty of computer information security protection. Hacker attacks are one of the biggest threats facing network security. Hackers can easily break through system defenses, steal, tamper with, or destroy data using techniques such as DDoS attacks, SQL injection, and cross site scripting. These attacks not only cause economic losses, but may also trigger social panic. Viruses and malicious software are also major threats to network security. Ransomware profits by encrypting user data and demanding ransom; Worm viruses can quickly replicate and spread in the network, causing system crashes; Trojan horses hide in seemingly normal programs, waiting for opportunities to launch attacks. In addition, phishing and social engineering attacks deceive users of sensitive information by disguising themselves as trusted entities, while distributed denial of service attacks (DDoS) occupy system resources through a large number of requests, making the system unable to provide services normally. To address these threats, it is necessary to strengthen the construction of network security protection systems, such as deploying firewalls, intrusion detection systems, anti-virus software, etc., and enhance users' security awareness and prevention capabilities.

2.3 Security Issues at the Data Level

Data is the core asset of computer information systems, and its security is directly related to personal privacy, trade secrets, and national security. Data leakage and illegal acquisition are currently one of the most serious data security issues. Criminals steal sensitive data through hacking attacks, insider leaks, and other means, which not only damages the interests of individuals and businesses, but may also trigger a crisis of social trust. Data tampering and destruction undermine the integrity and authenticity of data, leading to information distortion and misleading. Privacy infringement refers to the unauthorized collection, use, or disclosure of personal privacy information, which seriously violates the right to privacy of individuals. Insufficient protection of sensitive data is also an important aspect of data security issues. Once data in fields such as finance and healthcare is leaked, it will cause incalculable losses to society and individuals. In order to strengthen data protection, it is necessary to adopt strategies such as data encryption, access control, data backup and recovery, and establish a sound data security management system.

2.4 Security Issues at the System and Management Level

The security issues at the system and management level are one of the weak links in computer information security. System vulnerabilities and defects are one of the main entry points for hacker attacks. These vulnerabilities may be caused by programming errors, design flaws, or improper configuration, and once exploited by hackers, they will pose a serious security threat to the system. Improper security settings can also expose the system to potential security risks. For example, not turning on the firewall or not updating security software in a timely manner. Poor access control may lead to unauthorized users accessing sensitive information or engaging in illegal operations. The lack or ineffective implementation of security management systems exacerbates system security risks.

3. ANALYSIS OF THE CAUSES OF COMPUTER INFORMATION SECURITY ISSUES

3.1 Technical factors

3.1.1 Technical factors are one of the important root causes of computer information security issues

The lag of security technology behind the development of threats is an issue that cannot be ignored. With the continuous upgrading of hacker technology and the emergence of new network attack methods, traditional security defense measures are often difficult to cope with. This technological lag makes information systems particularly vulnerable and vulnerable to new threats.

3.1.2 System architecture and design flaws are also key factors leading to information security issues

Unreasonable system architecture, design negligence, or errors can all leave security risks. For example, high coupling between system modules, non-standard interface design, and incomplete security control strategies may all provide convenience for hacker attacks. In addition, with the development of new technologies such as cloud computing and the Internet of Things, the complexity and interdependence of the system have further increased, which also puts higher demands on the security of the system [2].

The inadequacy of encryption algorithms and key management is also an important issue in technical factors

Encryption algorithm is one of the core technologies for protecting data security, but if the algorithm itself has defects or is cracked, the security of the data cannot be guaranteed. Meanwhile, key management is also a crucial step in ensuring data security. If the management of key storage, distribution, updates, and other processes is improper, it may lead to key leakage or abuse, thereby causing serious security incidents.

3.2 Human factors

3.2.1 Weak user security awareness is one of the important reasons for frequent security issues
Many users lack sufficient security awareness and vigilance towards potential security threats when using computers and networks, making them easy targets for hacker attacks. For example, randomly clicking on unknown links, downloading unknown files, using weak passwords, and other behaviors may leave opportunities for hackers to take advantage of.

3.2.2 Operational errors and improper behavior are also important factors leading to safety issues

Users may encounter security issues due to negligence or misoperation when using computers and networks. For example, behaviors such as accidentally deleting important files, configuring system parameters incorrectly, and leaking sensitive information can all pose security risks to the system.

Malicious operations by internal personnel are one of the threats to computer information security that cannot be ignored

Internal personnel usually have a deep understanding of the internal structure and operational processes of the system, so their attacks are often more targeted and destructive. Malicious operations by internal personnel may be due to various reasons, such as personal gain, retaliatory mentality, or external forces' instigation. These behaviors may have a serious impact on the system, even leading to system paralysis.

3.3 Management Factors

3.3.1 The imperfect safety management system is one of the important reasons for the frequent occurrence of safety issues

Many organizations lack systematic planning and institutional safeguards in information security management, making it difficult to effectively carry out security management work. The lack or imperfection of security management systems has led to frequent issues such as unclear security management responsibilities and inadequate implementation of security strategies.

3.3.2 The lack of regulatory and auditing mechanisms is also one of the important reasons for information security issues

Effective regulatory and auditing mechanisms can promptly identify and correct security issues, but many organizations have significant shortcomings in this regard. The lack of regulatory mechanisms has led to a lack of effective supervision and constraints in security management, resulting in security vulnerabilities not being detected and fixed in a timely manner; The lack of audit mechanisms makes it difficult to hold accountable and prevent security incidents.

3.3.3 Insufficient emergency response capability is also an important issue in management factors

Faced with sudden security incidents, many organizations often lack effective response measures and emergency plans, leading to the expansion of the impact of the incident and increased losses. Therefore, strengthening the construction of emergency response capabilities is of great significance for improving the level of computer information security.

4. SOLUTIONS TO COMPUTER INFORMATION SECURITY ISSUES

4.1 Technical Countermeasures

The technical countermeasures are the first line of defense for computer information security protection, and their core lies in using advanced technological means to enhance the system's defense capabilities and data protection level.

4.1.1 Strengthen protection technology

Security devices such as firewalls and intrusion detection systems (IDS/IPS) should be deployed, which can monitor network traffic in real-time, identify and intercept potential malicious attacks, and provide initial security protection for the system. As a security barrier between internal and external networks, firewalls can control the flow of data entering and leaving the network, preventing unauthorized access. IDS/IPS can deeply analyze network traffic, discover and respond to potential security threats, including known and unknown attack methods.

4.1.2 Data Encryption

Data encryption is an important means of protecting data confidentiality. By using advanced encryption standards such as AES and RSA to encrypt sensitive data, it can be ensured that even if the data is intercepted during transmission or storage, it cannot be understood by unauthorized users. Data encryption should run through the entire lifecycle of data, including multiple levels such as transmission encryption, storage encryption, and application layer encryption.

4.1.3 Regular backup and recovery

Data backup and recovery are key measures to ensure data availability and integrity. Enterprises should establish a comprehensive data backup mechanism, regularly backup important data, and ensure the reliability and recoverability of backup data. In the event of data loss or damage, the system can be quickly restored to normal operation through backup data, reducing losses.

4.1.4 Application security technology

In addition to the above measures, other security technologies such as vulnerability scanning, security auditing, log management, etc. should also be actively applied. Vulnerability scanning can regularly detect security vulnerabilities and weaknesses in the system, providing a basis for security reinforcement. Security auditing can record system operations and security incidents, providing important basis for accident investigation and risk assessment. Log management can collect and analyze system logs, promptly identify and respond to potential security threats.

4.1.5 Introduction of Artificial Intelligence and Machine Learning

With the continuous development of artificial intelligence and machine learning technology, their application in the field of computer information security is becoming increasingly widespread. By introducing these technologies, the automation and intelligence level of threat detection and response can be improved. For example, using machine learning algorithms for deep analysis of massive network traffic can discover and predict potential security threats; Utilizing intelligent analysis engines to quickly respond and handle security incidents, improving the efficiency and accuracy of security protection.

4.2 Management level countermeasures

The countermeasures at the management level are an important support for computer information security protection, and their core lies in improving the overall security level of the organization through sound management systems and effective management measures.

4.2.1 Improve safety management system

Enterprises should establish detailed information security management systems, clarify the responsibilities and authorities of management personnel and employees at all levels, standardize security operation procedures and emergency response procedures. At the same time, regular security assessment and audit mechanisms should be established to supervise and inspect the implementation of the system, ensuring its effective execution.

4.2.2 Strengthen safety training

Employees are the first line of defense for enterprise information security protection. Therefore, it is crucial to strengthen safety training and enhance employees' safety awareness and skills. Enterprises should regularly carry out safety education activities, including safety knowledge popularization, safety skills training, case analysis, etc., to enable employees to understand common safety threats and preventive measures, and master basic safety operation skills.

4.2.3 Strengthen Access Control

Access control is an important means of protecting sensitive data. Enterprises should implement role-based and rule-based access control policies, manage sensitive data in a hierarchical manner, and ensure that only authorized users can access the corresponding level of data. At the same time, establish strict procedures for permission changes and approvals, and track and manage the entire process of permission application, approval, grant, and revocation. In addition, access control policies should be regularly evaluated and audited to ensure their effectiveness and adaptability.

4.2.4 Implement multi factor authentication

In order to further enhance the security of accounts, enterprises should implement a multi factor authentication mechanism. Compared with traditional single factor authentication (such as relying solely on passwords), multi factor authentication combines multiple verification methods, such as passwords, phone verification codes, fingerprint recognition, biometric recognition, etc., greatly improving the security of accounts. This method can effectively prevent unauthorized access, and even if attackers have access to the user's password, it is difficult to pass multi factor authentication.

4.2.5 Establish an emergency response mechanism

The emergency response mechanism is the key for enterprises to quickly respond and reduce losses when facing security incidents. Enterprises should establish detailed emergency response plans, clarify the emergency response process, responsible persons, and resource allocation methods. At the same time, regular emergency drills should be organized to verify the feasibility and effectiveness of emergency response plans and improve employees' ability to respond to safety incidents. In addition, establish cooperative relationships with third-party security service agencies to obtain timely external support in the event of major security incidents.

4.3 Legal and Policy Countermeasures

Legal and policy measures are important guarantees for computer information security protection. By improving the legal and regulatory system, increasing law enforcement efforts, and promoting international cooperation, a more favorable legal environment can be created for computer information security.

4.3.1 Strengthening legislation

The government should accelerate the improvement of the legal and regulatory system related to information security, clarify the basic principles, management requirements, legal responsibilities, and other contents of information security. At the same time, in response to emerging information security threats and challenges, relevant laws and regulations should be revised and improved in a timely manner to ensure the timeliness and applicability of the law. In addition, legal publicity and education should be strengthened to enhance public awareness of information security laws.

4.3.2 Increase law enforcement efforts

The government should increase law enforcement efforts against information security violations and crack down on cybercrime. By establishing cross departmental and cross regional law enforcement cooperation mechanisms, a strong deterrent force against information security violations can be formed. At the same time, we will strengthen the investigation and exposure of information security cases, give full play to the warning role of typical cases, and enhance society's awareness of the importance of information security.

4.3.3 Promoting International Cooperation

Information security is a global challenge that requires joint efforts from all countries. The government should strengthen cooperation and exchanges with other countries in the field of information security, and jointly study and solve the problem of transnational information security threats. By participating in the formulation of international information security standards and norms, sharing intelligence information, and conducting joint law enforcement, we aim to enhance the international community's attention and response capabilities to information security issues. In addition, we should actively participate in the activities of international information security organizations and strengthen dialogue and cooperation with the international community on information security.

5. CONCLUSION

In summary, computer information security is an important cornerstone of information construction, and the challenges it faces are complex and varied, requiring us to take comprehensive measures from multiple levels such as technology, management, and law. By strengthening technological innovation and enhancing defense capabilities; Improve management systems and strengthen personnel training; By strengthening the construction of laws and regulations and promoting international cooperation, we can effectively respond to current information security threats. In the future, with the continuous advancement of technology and the increasingly perfect management, we have confidence in building a more secure and trustworthy computer information environment, providing strong guarantees for the harmony, stability, and sustainable development of society.

REFERENCES

[1] Ding, C.; Wu, C. Self-Supervised Learning for Biomedical Signal Processing: A Systematic Review on ECG and PPG Signals. medRxiv 2024.

[2] Han, X., & Dou, X. (2025). User recommendation method integrating hierarchical graph attention network with multimodal knowledge graph. Frontiers in Neurorobotics, 19, 1587973.

[3] Hu, Xiao. "Low-Cost 3D Authoring via Guided Diffusion in GUI-Driven Pipeline." (2025).

[4] Li, X., Wang, X., & Lin, Y. (2025). Graph Neural Network Enhanced Sequential Recommendation Method for Cross-Platform Ad Campaign. arXiv preprint arXiv:2507.08959.

[5] Tan, C., Gao, F., Song, C., Xu, M., Li, Y., & Ma, H. (2024). Highly Reliable CI-JSO based Densely Connected Convolutional Networks Using Transfer Learning for Fault Diagnosis.

[6] Tu, Tongwei. "ProtoMind: Modeling Driven NAS and SIP Message Sequence Modeling for Smart Regression Detection." (2025).

[7] Xie, Minhui, and Boyan Liu. "InspectX: Optimizing Industrial Monitoring Systems via OpenCV and WebSocket for Real-Time Analysis." (2025).

[8] Zhang, Yuhan. "AdOptimizer: A Self-Supervised Framework for Efficient Ad Delivery in Low-Resource Markets." (2025).

[9] Zhang, Yuhan. "InfraMLForge: Developer Tooling for Rapid LLM Development and Scalable Deployment." (2025).

[10] Zhu, Bingxin. "REACTOR: Reliability Engineering with Automated Causal Tracking and Observability Reasoning." (2025).

[11] Zhuang, R. (2025). Evolutionary Logic and Theoretical Construction of Real Estate Marketing Strategies under Digital Transformation. Economics and Management Innovation, 2(2), 117-124.

[12] Wang, Hao. "Joint Training of Propensity Model and Prediction Model via Targeted Learning for Recommendation on Data Missing Not at Random." AAAI 2025 Workshop on Artificial Intelligence with Causal Techniques. 2025.