Woody International Publish Limited
An Multidisciplinary Academic Journal Publisher
Journal of Artificial Intelligence and Information, Volume 2, 2025
https://www.woodyinternational.com/

Analysis of Computer Information Security and Protection Strategies in the Era of Artificial Intelligence

Xiaofei Sun[1], Xiaoliang Zhou[2]

Guangdong ATV Performing Arts Vocational College, Zhaoqing, Guangdong 526000

Abstract: ***Currently, there are still some problems and shortcomings in the operation of computer systems, such as illegal attacks, malicious destruction, and information leakage, which affect the stability of computer system development.In response to this, industry related technical personnel need to investigate and analyze current information security issues, realize the importance of information security protection, and develop scientific and specific solutions to the exposed problems to ensure the stability of computer system operation.This article explores how to maintain computer information security, aiming to promote the development of science and technology.***

Keywords: Era of artificial intelligence; Computer information security; Protection.

1. INTRODUCTION

With the development of science and technology, computer technology has been widely applied to various industries, promoting the development of the industry.However, at the same time, some insecure factors threaten the security of computer system usage.How to ensure the integrity of computer information and maintain the stability of computer systems has become a key research topic in the computer industry in the era of artificial intelligence.In the era of artificial intelligence, the development of various intelligent activities requires the participation of computer technology.Therefore, ensuring network security and information security is a key link in the development of the times.At present, China has realized the importance of information security and has formulated effective security management and protection measures based on the actual development situation.However, information security has the characteristics of multiplicity and complexity, which increases the difficulty of information security management.Therefore, it is necessary to analyze the current security issues and their adverse effects, in order to adjust the security management plan and lay the foundation for the stable development of science and technology. Wang et al. (2022) [1] constructed a comprehensive cell atlas of the immune microenvironment in gastrointestinal cancers, with a particular focus on dendritic cells and their roles in tumor immunity. Shifting to logistics and e-commerce, Wang (2025) [2] developed predictive modeling techniques to optimize sortation and delivery processes, while Yuan (2024) [3] explored the potential of GPT-4 for processing multimodal medical data in electronic health record systems. In the domain of e-commerce content generation, Song (2024) [4] investigated how AI-generated content (AIGC) and human-computer interaction design can enhance both efficiency and quality. Data integration and smart city technologies were advanced by Chen (2025) [5][6], who proposed a quantized framework for data quality in gig economy platforms and introduced geospatial neural networks for location intelligence applications. Legal aspects of enterprise naming rights were examined by Wang (2024) [7], whereas Gong et al. (2024) [8] optimized enterprise risk decision support systems using ensemble machine learning methods. In computer vision, Bohang et al. (2025) [9] improved image steganalysis through active learning and hyperparameter optimization techniques. Emerging technologies for sustainable development were showcased by Yao et al. (2025) [10], who developed a drone-3D printing linkage system for rapid construction of post-disaster shelters. Financial applications of AI were explored by Yang et al. (2025) [11] through CNN-based stock market sentiment analysis and by Ji et al. (2025) [12] in personalized retail go-to-market strategies. Yang et al. (2025) [13] further demonstrated the integration of large language models (LLMs) for cross-asset risk management in financial markets. In healthcare and cognitive science, Peng et al. (2025) [14] investigated IoT-enhanced exercise and cognitive training effects on executive function, while Yang (2025) [15] developed LLM-driven dynamic hedging strategies for derivatives markets. Medical AI applications were advanced by Yuan (2025) [16] through self-supervised learning for tumor classification and by Wang et al. (2025) [17] in automating legal compliance audits using explainable LLMs.

2. COMPUTER INFORMATION SECURITY ISSUES AND IMPACTS IN THE ERA OF ARTIFICIAL INTELLIGENCE

2.1 Complexity of network viruses and diversity of network attacks

In the context of the Internet, the rapid development of information technology has promoted the development of science and technology in the era of artificial intelligence.In this context, artificial intelligence and information security promote and influence each other.Human computer interaction has been widely applied, and in order to ensure the security of computer information, industry technicians have conducted in-depth research on data management, security protection, and so on.For artificial intelligence technology, with the deepening of research, the level of information security management has improved, but there are still security risks and issues, among which the most prominent are network viruses and network attacks, which exhibit complexity and diversity.The most common security issue in the era of the Internet is hacker attacks. Through analyzing the traditional methods of hacker attacks, there are three main intrusion paths. Taking the implantation of Trojan viruses as an example, this type of network attack accounts for the largest proportion and is the most common.The attack is mainly carried out by clicking on pages containing viruses. At this point, the Trojan virus has already invaded the system, and the virus's invasion affects the security and stability of the computer system.In addition, there are some viruses hidden in spam messages. If users click on the website at this time, their personal information will be leaked, causing financial losses to the users.Finally, it is through the download of software that viruses hide within the software. During the download process, viruses enter computer devices along with the software, affecting the normal operation of the computer.

2.2 Network Information Vulnerability

People are accustomed to storing data information in databases during the application of information technology.Due to the large amount of data, multiple subsystems will be set up under the database for ease of management.Generally speaking, the probability of information leakage in network databases is relatively low.However, in the process of information utilization and transfer, network hackers and criminals will attack the transmission system, which is prone to information leakage and loss.Meanwhile, during the process of information transmission and utilization, data information is highly susceptible to theft.There are certain limitations in information system management, as it can only provide alerts for shallow level risks and cannot identify complex security risks in a timely manner.

2.3 Universality of Computer Network Security Vulnerabilities

At present, computer vulnerabilities mainly manifest in the following aspects: software, hardware, and system security. These vulnerabilities provide opportunities for criminals, who often start from these aspects to invade and damage computer systems.Vulnerabilities in computer systems not only have a negative impact on the system itself, but also endanger other software and hardware.There are various types of hardware and software in computer systems, and different software versions can also increase the probability of system vulnerabilities.In the era of intelligence, information technology is widely applied in various fields of life, and people are gradually increasing their attention to information systems and security.At the same time, industry technical personnel actively participate in information security management work, aiming to handle security issues that arise in information systems through professional skill training, and ensure that they are properly resolved.However, the current industry technology and staff still use traditional security management methods to ensure the security of data information, lacking technological innovation and unable to meet the requirements of modern information system security management.This leads to frequent information security issues, affecting the stable operation of computer systems and endangering personal information security.

3. COMPUTER INFORMATION SECURITY AND PROTECTION STRATEGIES IN THE ERA OF ARTIFICIAL INTELLIGENCE

3.1 Introducing information technology to control computer information security

In the era of artificial intelligence, strengthening the management of information security can promote the development of information technology, reduce the occurrence of information leakage and information loss.Therefore, in order to ensure the quality of work, it is necessary to introduce specialized technical means to

comprehensively control and protect information security. Only in this way can the healthy and stable operation of the network system be guaranteed, and the frequency of information security accidents be reduced.At the national level, it is necessary for all levels of government in China to recognize the importance of information security management, give full play to the guiding role of government departments to provide strong support for information security management, establish special funds to provide funding for information security technology research and development, inspect and analyze information technology equipment on the market, and introduce effective information technology and means to improve the effectiveness of information security management;

Secondly, it is necessary to innovate and reform the current data encryption technology, and introduce new technologies to protect data memory, ensuring the security of data transmission process and avoiding attacks on information systems during data transmission.

Thirdly, digital signature technology can be used to encrypt files, and double encryption can reduce the probability of information being tampered with.Digital signature technology mainly utilizes the asymmetry of computer information to ensure information security.In the application process of this technology, users often store important files and information under specific accounts and set up special passwords to ensure information security.Through experiments, setting passwords in the form of numbers, letters, and symbols minimizes the chance of being cracked.In addition, it is necessary to regularly set passwords so that files can be securely stored.

The fourth requirement is for technical personnel to learn current intelligent algorithms and apply them to existing information systems to improve information security. In specific work, artificial intelligence recognition technology can be actively used to identify potential risks in the operation of computer systems, evaluate their level of danger, and detect their illegal behavior. Through the system's detection and organization of dangerous behavior, it can be automatically submitted to the network security regulatory department, improving the efficiency and quality of the security regulatory department's work.

Finally, it is necessary to build an information monitoring platform to monitor and evaluate all operations within the system.Based on the collected information, present a rigorous monitoring report to ensure the stability of information security.

3.2 Build a security awareness system and strengthen the protection of information systems

The main role of artificial intelligence systems in the field of computer information security is to recognize user instructions, collect and manage data information within the system, and use specific algorithms to evaluate network behavior, clarify dangerous behaviors, and assist management personnel in identifying and warning of risks and security threats in the system, making it easier for management personnel to take effective measures to deal with problems in a timely manner.For example, some illegal individuals use users' online behavior to steal personal privacy and commit fraud, or sell users' phone numbers and personal information, daring to promote and commit online fraud.These behaviors hinder the development of a harmonious society and, in more serious cases, threaten national security, causing certain economic losses.Therefore, in response to this situation, industry technicians need to realize the importance of network information security, actively introduce diverse technological means, and apply them to specific security management work, in order to build a security perception system, monitor and manage potential threats and security risks in the network, and improve the effectiveness of security protection.By utilizing visualization technology to analyze and explore security incidents, it facilitates users to form a correct understanding of network security events and provides them with security information [7].

3.3 Develop laws and regulations to improve the legal level of network security

In order to reduce the occurrence of computer information security incidents and improve the quality and level of information security protection, it is necessary to give full play to the guiding role of government departments, combine the characteristics of current computer security incidents and information security management technology, and formulate targeted laws and regulations.Before formulating laws and regulations, it is necessary to conduct in-depth research on the types and risks of computer information security accidents in various industries, in order to formulate legal provisions and enhance legislative effectiveness.In the past, China did not attach great importance to network security and failed to formulate professional laws and regulations.In the context of artificial intelligence, it is necessary to introduce a cybersecurity law to ensure that there are laws to abide by and that current illegal activities are restrained, providing support for the secure development of information technology.Relevant departments need to enhance their ideological stance, using the Party's ideology as the basis

for the formulation of laws and regulations, ensuring the rationality and scientificity of the formulation of laws and regulations, and thus realizing the value of laws and regulations.In the specific work, it is necessary for China's security departments to analyze the adverse consequences caused by current network security incidents, so as to consider network security work from multiple perspectives and formulate security maintenance measures.In addition, it is necessary to strengthen the sense of responsibility, clarify the responsibilities and obligations of personnel in each department, and facilitate the identification of relevant responsible persons as soon as possible after a cybersecurity incident occurs.Establish a reward and punishment system to enhance the sense of responsibility of staff, so that they can fulfill their duties and take on their responsibilities.Finally, it is necessary to improve personal protection systems, network security systems, etc., to reduce the occurrence of network security incidents from the source.Standardize and constrain online behavior, and protect personal information security [8].

3.4 Strengthen the construction of information technology talent team and improve information security protection capabilities

If we want to achieve the expected information security protection effect, we need to attach importance to the construction of the information technology talent team, ensure that they can correctly apply advanced information management technology to regulate and constrain network behavior in their work, and ensure information security.Therefore, it is necessary to increase the efforts of talent introduction, and professional colleges need to adjust their talent training plans in combination with the current information security incidents, in order to provide a continuous supply of talents to society.Enterprises regularly provide visiting and internship opportunities for students from professional colleges, enabling them to grasp the current talent requirements of society and develop towards their ideal direction.Furthermore, it is important to recognize the significance of specialized training.In practical work, actively organize various professional trainings to enable them to master advanced network security management techniques.By continuously learning and practicing, we aim to improve the professional competence and comprehensive application ability of technical personnel, and ensure information security.In addition, incorporating professional competence assessment into performance evaluation and improving the work enthusiasm of technical personnel through regular assessments.The content involved in network information security protection work is relatively complex, and it is necessary to increase the salary level of technical personnel so that they can improve their work enthusiasm, actively participate in technology research and innovation, and safeguard the development of the industry.

4. CONCLUSION

Under the background of artificial intelligence, the application scope of information technology is constantly expanding.Although information technology has brought some convenience to people's lives, the inherent vulnerabilities in network systems pose a threat to the integrity of information security.In the specific implementation of work, it is necessary for the country to be aware of the adverse effects caused by the occurrence of current cybersecurity incidents, so as to analyze and study these issues, formulate reasonable solutions, and effectively solve the exposed problems.Actively introduce advanced security measures and technologies, implement them in specific work, and establish an information security protection platform.Governments at all levels need to play a macro guiding role, providing theoretical basis for information security management through strengthening legislative supervision, establishing security management regulations, and other forms.Finally, it is necessary to improve the literacy and abilities of professional and technical personnel, build specialized management teams, enable computers to operate normally, and promote the orderly implementation of computer activities.

REFERENCES

[1] 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.
[2] Wang, J. (2025). Predictive Modeling for Sortation and Delivery Optimization in E-Commerce Logistics.
[3] Yuan, J. (2024). Exploiting gpt-4 for multimodal medical data processing in electronic health record systems. Preprints, December.
[4] Song, X. (2024). Leveraging aigc and human-computer interaction design to enhance efficiency and quality in e-commerce content generation.
[5] Chen, J. (2025). Data Quality Quantized Framework: Ensuring Large-Scale Data Integration in Gig Economy Platforms.
[6] Chen, J. (2025). Geospatial Neural Networks: Enhancing Smart City through Location Intelligence.

[7] Wang, H. (2024). The Restriction and Balance of Prior Rights on the Right of Enterprise Name.
[8] 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).
[9] 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
[10] Yao, T., Jian, X., He, J., & Meng, Q. (2025). Drone-3D Printing Linkage for Rapid Construction of Sustainable Post-Disaster Temporary Shelters.
[11] Yang, W., Lin, Y., Xue, H., & Wang, J. (2025). Research on Stock Market Sentiment Analysis and Prediction Method Based on Convolutional Neural Network.
[12] Ji, F., Zheng, X., Xue, H., & Wang, J. (2025). A Study on the Application of Artificial Intelligence in Personalized Go-to-Market Strategy in Retail Industry.
[13] Yang, J., Tang, Y., Li, Y., Zhang, L., & Zhang, H. (2025). Cross-Asset Risk Management: Integrating LLMs for Real-Time Monitoring of Equity, Fixed Income, and Currency Markets. arXiv preprint arXiv:2504.04292.
[14] Peng, Y., Zhang, G., & Pang, H. (2025). Exploring the effects of IoT-enhanced exercise and cognitive training on executive function in middle-aged adults. Alexandria Engineering Journal, 120, 106-115.
[15] Yang, Jie, et al. "Dynamic Hedging Strategies in Derivatives Markets with LLM-Driven Sentiment and News Analytics." arXiv preprint arXiv:2504.04295 (2025).
[16] Yuan, J. (2025). Self-Supervised Multimodal Learning for Tumor Classification in Chest Radiography. Authorea Preprints.
[17] Wang, J., Yuan, J., Liu, J., & Evans, L. (2025). Simple Legal Compliance: Automating Regulatory Audits with Explainable LLMs.