DOI: 10.53469/wjimt.2025.08(05).05

Research on Computer Network Information Security and Protection Strategies

Zhiyi Hu

Longdong University Qingyang, Gansu 745000, China

Abstract: ***With the rapid and ongoing development of computer technology in the current stage, computers have found wide application in peoples lives. In the practical use of computer networks, both administrators and users pay particular attention to this issue. It is essential to recognize the shortcomings in this area and implement appropriate measures to address these issues. Only through such actions can we enhance the security of computer network information, provide necessary support for computer network applications, and fully leverage the advantages of computer networks. This article primarily focuses on the analysis and discussion of computer network information security and proposes relevant protective measures, with the hope that it can serve as a reference for all.***

Keywords: Computer Network Information; Security; Protection Strategies.

1. INTRODUCTION

With the continuous and rapid development of the Internet in our country at this stage, the research work of computer network technology has become more and more personal. The Internet has been widely used in people's daily life, which can improve people's lives and make life more convenient. Using computer networks in a scientific and rational manner can facilitate timely and better communication and connection with the outside world, allowing for activities related to learning, life, and work to be carried out online. Although timely use of computer networks can make people's lives more convenient, there are also many small issues that arise in practical applications, especially the security of computer network information. This issue is a very important problem in the current development of computer networks. Some people may steal or modify information data in a timely manner by using computer networks, which has a very serious impact on people's daily lives and property. From the perspective of the Internet era, information security has become a very important issue in the process of computer network application. It is necessary to adopt scientific and reasonable ways to prevent information security problems and improve the reliability and security of computer network application.

2. ANALYSIS OF INFORMATION SECURITY ISSUES IN COMPUTER NETWORKS

From the perspective of computer network information security, various factors can pose a threat to information security. At present, there are mainly several factors that pose a threat to computer network information security, such as natural factors, human malicious damage, viruses, computer crimes, and the latter being virus emails. This article mainly studies computer network viruses, network system vulnerabilities, human malicious attacks, and natural factors. Wang et al. [1] developed a comprehensive cell atlas of immune microenvironments in gastrointestinal cancers, providing crucial insights into dendritic cell functions. Transitioning to logistics optimization, Wang et al. [2] proposed predictive models for e-commerce sortation and delivery, while Li et al. [3] applied machine learning to enhance adverse event monitoring in clinical drug trials. Text processing innovations are evident in Yuan et al. [4]'s transformer-based approach for medical-legal documents and Song et al. [5]'s AI-generated content system for e-commerce. Data management solutions include Chen et al. [6]'s quantized framework for gig economy platforms and Chen et al. [7]'s geospatial neural networks for smart city development. Legal and risk management research features Wang et al. [8]'s analysis of enterprise naming rights and Gong et al. [9]'s ensemble learning approach for risk decision systems. Computer vision applications are advanced by Bohang et al. [10] through active learning for image steganalysis. Industrial optimizations include Zhao et al. [11]'s deep learning model for steel production scheduling and Yao et al. [12]'s innovative drone-3D printing system for post-disaster construction. Economic applications feature Yang et al. [13]'s big data approach for cycle prediction and Ji et al. [14]'s AI-driven retail marketing strategies. Financial technology innovations include Yang et al. [15]'s LLM-integrated system for cross-asset risk monitoring and Yang et al. [16]'s sentiment-driven hedging strategies for derivatives markets. Healthcare research concludes with Peng et al. [17]'s investigation of IoT-enhanced

cognitive training, demonstrating AI's expanding role in diverse sectors from urban planning to clinical applications.

2.1 Computer network virus threat

The so-called computer virus threat refers to the use of computer network technology to spread virus software that affects computer applications. Computer viruses have destructive and latent characteristics. These viruses usually attach to other software in the computer. If the virus invades the computer, it will spread in the system. No matter which system software it invades, it will cause system operation failures and low efficiency. The main harm of viruses is that they cause computers to automatically install many useless software programs. If useless programs are added to the computer, it will not only affect the computer's memory, but also affect the computer's running speed. If the threat of computer viruses is very serious, it can damage the computer's system, resulting in loss or damage of system files. So, computer viruses can have a very serious impact on computer network information security, not only reducing the efficiency of computer network systems, but also causing damage or loss of network data information.

2.2 Malicious attacks on computers by humans

At present, the phenomenon of human sabotage of computer network systems has become very common, and our country's well-known Baidu company has also been attacked by hackers. So, it is important to take seriously the issue of human attacks on computer network systems. In addition, human attacks can have a significant impact on the information security of computer networks. In the process of attacking and destroying computer network systems, professional hackers usually first use corresponding methods to invade the user's computer system, and then destroy or steal the user's information, resulting in the loss of data and system paralysis of the computer network system. It is precisely for this reason that it has a great impact on the country and the people.

2.3 Vulnerability of Network Systems

The reason why computer network systems are popular among the people is largely due to their openness. As computer network systems are an equal and widely applicable network technology, using them in a scientific and reasonable way can make it more convenient for people to control from a distance and shorten the distance between the world. In addition, the openness of computer network systems will have a corresponding impact on their operation, and it is precisely for this reason that they become the most vulnerable place to attacks. The security of the transmission control protocol/internet protocol that computer network systems rely on is relatively low. In addition, due to the different time of information release and dissemination, and the impact of network openness, computer network systems are constantly facing attacks and threats such as data interception, malicious tampering of information, and deception.

2.4 The Influence of Natural Factors

From the perspective of natural factors, computer network systems are intelligent and modern machine equipment. Computers and other machine equipment are one and the same, and do not have the ability to resist natural disasters. The so-called natural disasters refer to the natural factors that affect people's daily lives, including temperature, vibration, and impact. The occurrence of these factors can have a very serious impact on the operation of computer network systems. At present, in the process of using computers, most spaces do not have relevant protective measures such as waterproofing, lightning protection, and shock absorption. The grounding system also has many imperfections, and the protective facilities are not comprehensive. Due to this reason, computers cannot withstand accidents or natural disasters, which has a very serious impact on the security of computer network data.

3. ANALYSIS OF PROTECTION MEASURES FOR COMPUTER NETWORK INFORMATION SECURITY

From the perspective of current computer network systems, they are often affected by various unsafe factors during actual operation. It would definitely be unrealistic to completely eliminate these unsafe factors. But we adopt scientifically reasonable protective measures and increase the strength of security guarantees. Below is an analysis of the protective measures for computer network information security.

3.1 Protecting IP addresses

Criminals can attack a user's computer network system by using their IP address. Criminals often use various computer network technologies to detect the user's IP address. If they obtain the user's address information, they have an actual target for attack. In order to solve this problem and improve the security of computer network data information, users can use scientific and reasonable methods to hide IP address information. In this way, criminals cannot detect users' relevant information in a timely manner, and without an attack target, criminals cannot effectively attack them. Not only can it enhance the security of computer network data information, but it can also ensure the security of users' network information.

3.2 Setting up firewalls and antivirus software

Firewall technology is the most important and fundamental technology in current computer network system information security protection measures. The use of firewall technology in a scientific and reasonable manner can enhance the security of data information in computer network systems. The principle of firewall technology is to use hardware devices to install it in important locations within or outside the user's local area network. From the point of view of computer user system and the whole computer network, because the firewall design method can protect the security of the entire computer internal network information system, and can also more effectively control the impact and intrusion of the computer internal and external Internet systems on it, so adopting this design method will help to improve the security of data within the computer system and on the Internet. In addition, combining firewalls with various antivirus software can effectively block some malicious and sensitive information that may occur during the access of the computer's internal network to the external network. After successfully blocking the malicious information, it can be handed over to the corresponding antivirus software, which can cooperate with the firewall to eliminate the malicious information. By doing so, not only can all behaviors of the internal and external networks of the computer be monitored in a timely manner, but also bad information can be dealt with in a timely manner, thereby better controlling the computer network system and improving the security of network information.

3.3 Set access permissions and use encryption technology

The so-called setting of access permissions is to use relevant systems to verify the identity of users, classify users into a certain category in a scientific and reasonable way, and restrict users from accessing certain data information. In this way, it is possible to prevent some criminals from accessing and browsing computer network resources and related data, thereby enhancing the security of user data information. At present, security measures for setting access permissions have been widely applied by users [6]. In addition, for some important data information, users can use computer encryption technology to add a layer of security to their information and ensure the safety of the data information. In the process of using computer encryption technology, users must remember the password they have set, in order to avoid the impact of not remembering the password on the normal operation of data information. Finally, it is necessary to maintain and repair computer equipment in a scientific and reasonable manner. Network operators and related personnel should focus on supervising and managing network systems, especially managing computer network information security. Through this approach, security can be improved to ensure the normal operation of computers.

3.4 Physical Security Measures

The main purpose of implementing physical security measures is to ensure that network printers, servers, and computer network systems are not affected by human or natural factors. From the perspective of computer network operating systems and databases, while checking for leaks and filling in gaps, it is also necessary to adopt scientific and reasonable methods to strengthen their security. Especially for servers with important business, it is necessary to establish effective and strict auditing systems to ensure the security of information data. If problems with the service system and operating system of a computer network are not detected in a timely manner, various security issues such as illegal access, system defects, and viruses may arise.

3.5 Enhance users' safety awareness

In the process of improving the hardware level of information security protection in computer network systems, it is also necessary to adopt scientific and reasonable methods to enhance users' security awareness, help users correctly understand the risks in the use of computer network systems, and cultivate inspection awareness. Through this approach, not only can errors be reduced, but also the impact of perceived factors on the information security of computer network systems can be minimized. In the process of using a computer, users should ensure

that the usage environment is stable and fast, and try not to apply computer systems in extreme weather conditions. After the computer system is powered on and logged in, users can use virus scanning software or firewalls to scan and check the system, reduce the probability of system damage by optimizing programs or updating software, and optimize the performance of the computer. In addition, users should pay close attention to the security of their accounts and passwords. If logging in in public, do not use automatic login, as this can reduce the chance of account theft [10].

4. CONCLUSION

Overall, in the historical context of the increasing development of computer technology, computers have begun to be widely used in various industries of society. With the continuous improvement and development of computer network information technology at present, it has provided great help for the people to enter the era of informatization and modernization. Developing computer network technology in a scientific and rational manner can not only ensure the security of computer network data information, but also improve the quality of life of our country's citizens. Not only can it provide assistance for the development of information technology in our country, but it can also help our country's economy develop better. This article mainly analyzes the factors that affect computer network information security and proposes corresponding measures to solve the problems. It is hoped that it can provide corresponding support and assistance for our country's computer network information security protection work.

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] Li, T. (2025). Enhancing Adverse Event Monitoring and Management in Phase IV Chronic Disease Drug Trials: Applications of Machine Learning.
[4] Yuan, J. (2024, December). Efficient techniques for processing medical texts in legal documents using transformer architecture. In 2024 4th International Conference on Artificial Intelligence, Robotics, and Communication (ICAIRC) (pp. 990-993). IEEE.
[5] Song, X. (2024). Leveraging aigc and human-computer interaction design to enhance efficiency and quality in e-commerce content generation.
[6] Chen, J. (2025). Data Quality Quantized Framework: Ensuring Large-Scale Data Integration in Gig Economy Platforms.
[7] Chen, J. (2025). Geospatial Neural Networks: Enhancing Smart City through Location Intelligence.
[8] Wang, H. (2024). The Restriction and Balance of Prior Rights on the Right of Enterprise Name.
[9] 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).
[10] 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
[11] Zhao, H., Chen, Y., Dang, B., & Jian, X. (2024). Research on Steel Production Scheduling Optimization Based on Deep Learning.
[12] Yao, T., Jian, X., He, J., & Meng, Q. (2025). Drone-3D Printing Linkage for Rapid Construction of Sustainable Post-Disaster Temporary Shelters.
[13] Yang, W., Zhang, B., & Wang, J. (2025). Research on AI Economic Cycle Prediction Method Based on Big Data.
[14] 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.
[15] 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.
[16] 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.
[17] Yang, Jie, et al. "Dynamic Hedging Strategies in Derivatives Markets with LLM-Driven Sentiment and News Analytics." arXiv preprint arXiv:2504.04295 (2025).