DOI: 10.53469/wjimt.2025.08(07).01

Threat Factors and Prevention Strategies for Computer Network Security

Okita Dan Odhiambo

Maharajadhiraj Uday Chand Women's College, Rajbati, Purba Barddhaman – 713104, West Bengal, India

Abstract: ***With the advent of the Internet era, computer network security technology is increasingly widely used. Strengthening the analysis of the impact factors of network security technology in the operation of computer systems and timely prevention and control of related risks in the context of actual practice can better ensure that computer network technology effectively performs its due functions. This paper first explores the importance of computer network security maintenance, analyzes some threat factors of computer network technology, and finally proposes specific preventive measures for how to strengthen computer network security management for your information.***

Keywords: Computer network security; Influence factors; Preventive strategies.

1. INTRODUCTION

At present, with the advent of the information age, computer technology and network technology have been widely used in different fields of society, which not only bring great convenience to people's lives, provide convenient means for learning, but also support enterprise security and production. In the application of computers, because the advantages and disadvantages of computer networks coexist, network workers must strengthen information encryption technology and information protection technology. In order to lay the foundation for network information security, network information security to solve the problem, this paper discusses the computer network information security factors and preventive measures. In the context of the "Internet Plus" twenty-first century, the Internet has become an indispensable and important tool in life, production and learning. Computer networks can be widely used in different industries, and the rapid development of science and technology has led to the increasing complexity of the network environment, and computer network security issues have become the most significant problems in their application. In order to rationally utilize the products developed in this new era, Therefore, it is necessary to strengthen the construction of computer network security and promote the development of information technology. Based on the current situation of network information security, this paper focuses on the analysis of the factors affecting computer network information security, and puts forward the pertinent preventive measures.

2. THE IMPORTANCE OF COMPUTER NETWORK SECURITY MAINTENANCE

With the rapid development of the Internet and information technology, the way people in all walks of life communicate information has become indispensable to the network and computers. Computer networks have gradually developed into a necessity in people's daily life, and people's dependence on computer networks is increasing. For example, network offices in universities, full network coverage in student dormitories, and online teaching, computer networks are increasingly demanding. However, with the rapid development of computer networks, the problem of network security is becoming more and more prominent. The importance of cybersecurity has become a social issue of concern to all. If network security is not guaranteed, the risk of disclosing, altering or destroying information, and the risk of stealing assets or secrets is likely to cause irreparable damage. So the importance of protecting computer network security is beyond question. Recent advances in AI span multiple domains, beginning with Wang (2025) who addresses recommendation systems with missing-not-at-random data through joint training of propensity and prediction models using targeted learning [1]. Concurrently, Ding et al. (2024) survey large language model applications in biosignal processing [2], while Restrepo et al. (2024) develop multimodal embedding alignment for healthcare in low-resource settings [3]. In NLP, Yang et al. (2025) propose a GAN-based text summarization model combining transductive and reinforcement learning [4]. Industrial applications include Xie and Chen's (2025) Maestro multi-agent system for manufacturing optimization [5]. Diagnostic and operational tools feature Zhu's (2025) TraceLM for temporal root-cause analysis using contextual language models [6], Zhang's (2025) CrossPlatformStack for high-availability deployment across services [7], and Hu's (2025) AdPercept for visual saliency modeling in 3D ad design [8]. Computer vision advances include Peng et al.'s (2024) domain-adaptive human pose estimation through representation aggregation-segregation [9]. Anomaly detection is advanced by Zhang et al.'s (2025) ML techniques for biomechanical big data [10] and Wang's (2025) knowledge graph-based clinical trial anomaly detection system [11]. Enterprise solutions encompass Qi's (2025) hybrid neural network for interpretable inventory forecasting [12], Fang's (2025) microservice-driven low-code platform for SME digital transformation [13], and Li's (2025) GIS-integrated U-Net for automated land encroachment detection [14]. Infrastructure innovation includes Lin's (2025) framework for generative AI in proactive incident management [15]. Sensor analytics feature Huang and Qiu's (2025) LSTM-based abnormal electricity detection in smart meters [16], while urban safety is enhanced by Li's (2025) AD-STGNN for adaptive fire vehicle dispatch [17].

3. COMPUTER NETWORK INFORMATION SECURITY THREATS

3.1 Computer virus attacks

Computer viruses are essentially a combination of computer instructions and computer program code. In the process of programming or inserting code and instructions, computer data and computer functions will also be affected, which will adversely affect the normal application of the computer. Network hackers will work with the goal of stealing important information in a computer or with the goal to damage important information. Relying on computer viruses, the computer targeted attacks, because the virus itself has a strong concealment, transmission perceptual, parasitic and triggering characteristics, it will greatly adversely affect the computer network information security, so starting from the computer virus, Rational preventive measures must be taken to reduce the likelihood of computer data and programs being attacked by viruses, to reduce the possibility of computer data being stolen or programs being lost, to maintain the normalization of computer network operations, and to reduce the probability of network paralysis problems [2].

3.2 Network intrusion

A computer network that is exploited by hackers for illegal profit is a network intrusion. There are also a variety of ways to hack networks: there are listening methods, trojan horses, password methods, hidden technologies, and so on. Hackers mainly attack information networks, government websites, financial institutions, and the websites of key national universities (which have relatively important scientific research projects of the country). Hacker activities are frequent, and theft is carried out in the form of illegal interception, deciphering, tampering, copying and other forms. Because of the existence of hackers, computer network information security will suffer a serious threat, national security interests will also be threatened, to the masses of property losses.

3.3 Insufficient user safety awareness

The security awareness of computer users greatly affects the security of network information. Due to the lack of attention to information security issues, users can not correctly understand the anti-virus software and firewall programs, most of them think that this kind of software will greatly affect the performance of the computer process, Therefore, most people choose not to install antivirus software and firewalls. In the process, if users apply computers in public places and do not clean personal data and passwords after use, it will directly induce the occurrence of important information data leakage problems. From the overall perspective, the user security awareness can not be enhanced, which is the most important factor of computer information security threats.

3.4 Inadequate operating management system

In the computer network information security management process, the lack of appropriate human resources, because in the computer network for the cost of investment is not much, and the actual needs of users are also different. Then, as users make higher demands, the corresponding management changes. In this process, relevant managers need to be able to manage it, and the lack of professional managers and technicians will affect computer network security.

4. STRATEGIES FOR IMPROVING COMPUTER NETWORK SECURITY PREVENTION

4.1 Use of firewall technology

In the process of building a network security system, firewalls need to be used, and by utilizing firewalls, they can effectively block bad information and avoid computer poisoning. Therefore, in the process of improving the network security system, we should actively utilize firewall technology and be able to effectively combine it with computer systems to improve the security performance of the firewall. In the composition of a firewall, network and application gateways are very important elements, Through the effective application of application-level gateways, the security of computers transmitting and receiving data can be checked in a timely manner, and backups can be implemented with the help of the gateway, which is a technology that better ensures effective communication between servers and customers. At the same time, by applying an application-level gateway, you can also know the actual needs of the computer in a timely manner and access them according to specific needs [3]. Network firewalls are analyzed according to the data port and specific requirements to check the receipt and transmission of information.

4.2 Strengthening the control of computer network access rights

Strengthening the control of computer network access right is an effective way to improve the security of computer network information. Access right control mainly refers to the strategy of preventing illegal users through the strict authentication of computer network users. By distinguishing different identities, assigning them a unique account as a unified electronic identity, let them log on to the network using the unique unified electronic ID. Strengthening computer network access right control is one of the most direct and effective means, greatly increasing the security of computer network.

4.3 Continuous optimization of computer systems

The computer network security technology system itself is relatively complex, and it is necessary to comprehensively strengthen the optimization and upgrading of computer systems. To this end, it is necessary to continuously share and exchange technologies in the light of the real development needs of computer networks, fully draw on domestic and international experience in the upgrading, management and maintenance of computer network systems, and achieve comprehensive verification of user information by configuring encryption key software; Strengthen the optimization and configuration of conventional systems and conduct regular inspections of relevant risks to prevent possible problems in a timely manner. In addition, the optimization and configuration of computer hardware systems and software systems should be comprehensively strengthened, and mismatched relevant software or old devices should be replaced in a timely manner to better create a good operating environment.

4.4 Application of Network Information Encryption Technology

The utility of network information encryption technology application can reduce the leakage of information data in transmission or storage. At present, the information age has arrived, and the application of encryption can effectively guarantee the security of user information data. At present, with the application of key technology, hardware can be regarded as the core content of computer information security, which can prevent the network hacker from entering into the computer hardware system and the inside of the network system. The application of this technology in information interaction can rely on password matching to identify network attackers, reduce network security vulnerabilities and retroactive applications to realize network system attack situations. The application of key technology can encrypt information technology before information data is transmitted. After the information is transmitted to the corresponding target, a security algorithm is adopted, relying on public or private keys to unlock the password, which not only ensures the security of the information transmission, but also reduces the probability of information attacks and information interception problems [4].

4.5 Learning advanced technology

The development of computer network security requires the help of corresponding professionals. Therefore, in the process of computer network security technology research, a high-quality security management team should be built, which should not only strengthen the research on technology, but also continuously learn advanced technology in this process, so as to better improve the level of computer network technology. Computer security managers can adopt a design problem approach, which can determine the identity of users when they need to obtain corresponding information, and allow users to obtain the information they want in a timely manner. Network monitoring and evaluation should also be strengthened, and professional management teams should evaluate network equipment, and network equipment should be inspected regularly, which is also an important way to ensure network security.

4.6 Enhancing the security awareness of Internet users

First, for various phenomena that threaten network security, users' network security awareness needs to be strengthened, most importantly the protection of users' personal privacy messages. The relevant units strengthen the popularization of cybersecurity knowledge, and within the unit, employees can be vigilant about "phishing" websites and website links that pop up inexplicably on the website, and can list typical fraud and fake websites and other website templates to enhance the awareness of relevant personnel about fake websites. In this way, employees can avoid the "trap" of unexplained websites and software. The unit should regularly promote network security knowledge, and make employees develop the habit of scanning using antivirus software first when downloading software to avoid computer networks being infected by viruses.

4.7 Improving management mechanisms

Information security management is based on scientific organizational mechanism, rules and regulations, and control measures. Some of the existence of information security protection software and hardware facilities, management of information, data users, etc., to fully integrate to ensure that the organization can achieve the preset information security goals, to ensure the security of information, privacy available. Specifically, information security management includes two elements: management measures and security methods. Information security management must think about the value of technology in the aspects of system and means. Only through the combination of system, means and technology, can we achieve a comprehensive integration, can we achieve the best security management.

5. CONCLUSION

In summary, computer networks have gradually developed into a necessity for people's daily life, and people's dependence on computer networks is increasing. With the deep development of computer networks, network security issues have become an important issue of concern at present. From the current state of computer network security in China, there are many problems in computer network security, and the existence of these problems makes computer network security face great dangers, which may cause irreparable damage to human society. In order to maximize the security of computer networks, it is necessary to take preventive measures against their existing problems.

REFERENCES

[1] 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.
[2] Ding, Cheng, et al. "A Survey of LLMs on Biosignal Applications." Authorea Preprints (2024).
[3] Restrepo, David, et al. "Multimodal Deep Learning for Low-Resource Settings: A Vector Embedding Alignment Approach for Healthcare Applications." medRxiv (2024): 2024-06.
[4] Yang, Jing, et al. "A generative adversarial network-based extractive text summarization using transductive and reinforcement learning." IEEE Access (2025).
[5] Xie, Minhui, and Shujian Chen. "Maestro: Multi-Agent Enhanced System for Task Recognition and Optimization in Manufacturing Lines." Authorea Preprints (2025).
[6] Zhu, Bingxin. "TraceLM: Temporal Root-Cause Analysis with Contextual Embedding Language Models." (2025).
[7] Zhang, Yuhan. "CrossPlatformStack: Enabling High Availability and Safe Deployment for Products Across Meta Services." (2025).
[8] Hu, Xiao. "AdPercept: Visual Saliency and Attention Modeling in Ad 3D Design." (2025).
[9] Peng, Qucheng, et al. "Exploiting Aggregation and Segregation of Representations for Domain Adaptive Human Pose Estimation." arXiv preprint arXiv:2412.20538 (2024).
[10] Zhang, Shengyuan, et al. "Research on machine learning-based anomaly detection techniques in biomechanical big data environments." Molecular & Cellular Biomechanics 22.3 (2025): 669-669.
[11] Wang, Y. (2025, May). Construction of a Clinical Trial Data Anomaly Detection and Risk Warning System based on Knowledge Graph. In Forum on Research and Innovation Management (Vol. 3, No. 6).

[12] Qi, R. (2025). Interpretable Slow-Moving Inventory Forecasting: A Hybrid Neural Network Approach with Interactive Visualization.

[13] Fang, Z. (2025). Microservice-Driven Modular Low-Code Platform for Accelerating SME Digital Transformation.

[14] Li, B. (2025). GIS-Integrated Semi-Supervised U-Net for Automated Spatiotemporal Detection and Visualization of Land Encroachment in Protected Areas Using Remote Sensing Imagery.

[15] Lin, Tingting. "The Role of Generative AI in Proactive Incident Management: Transforming Infrastructure Operations."

[16] Huang, Jingyi, and Yujuan Qiu. "LSTM‑Based Time Series Detection of Abnormal Electricity Usage in Smart Meters." (2025).

[17] Li, Binghui. "AD-STGNN: Adaptive Diffusion Spatiotemporal GNN for Dynamic Urban Fire Vehicle Dispatch and Emergency." (2025).