Woody International Publish Limited
An Multidisciplinary Academic Journal Publisher

Journal of Artificial Intelligence and Information, Volume 2, 2025
https://www.woodyinternational.com/

Threat Factors and Prevention Strategies for Computer Network Security

Lijie Bai

Liaoyuan Vocational and Technical College Jilin Liaoyuan 136200

Abstract: ***With the rapid development of Internet technology, computer network has become an indispensable part of modern society. Computer networks play a crucial role in personal life, business operations, and national management. However, with the popularization of network applications, network security issues have become increasingly prominent and have become an important factor restricting the development of computer networks. Therefore, strengthening research on network security technology during the operation of computer systems, analyzing influencing factors, and timely preventing and controlling related risks are of great significance for ensuring the effective application of computer network technology.***

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

Cited as: Bai, L. (2025). Threat Factors and Prevention Strategies for Computer Network Security. *Journal of Artificial Intelligence and Information*, *2*, 32–36. Retrieved from https://woodyinternational.com/index.php/jaii/article/view/146

1. Introduction

At present, with the advent of the information age, computer technology and network technology have been widely applied in different fields of society. They not only bring great convenience to people's lives and provide convenient means for learning, but also provide support for enterprise safety and production. In the process of applying computers, due to the coexistence of advantages and disadvantages of computer networks, network workers must strengthen information encryption technology and information protection technology to lay the foundation for network information security and solve network information security problems. This article discusses and analyzes the influencing factors and preventive measures of computer network information security. Under the background of the "Internet plus" in the twenty-first century, the network has become an indispensable tool in life, production and learning. Computer networks can be widely used in different industries. The rapid development of science and technology has led to the increasing complexity of the network environment. Computer network security has become the most important problem in its application. In order to make rational use of the product of the development of this new era, it is necessary to strengthen the construction of computer network security and constantly promote the development of information technology. This paper, starting from the current situation of network information security, focuses on the analysis of the influencing factors of computer network information security, and puts forward targeted preventive measures. The recent advancements in artificial intelligence and computing have led to various innovative applications. Xu et al. (2024) explored ways to enhance user experience and trust in advanced large language model (LLM)-based conversational agents [1]. Chen et al. (2020) applied deep learning techniques for grading printed mottle defects, while Chen et al. (2022) introduced a one-stage object referring method with gaze estimation[2][3]. Yan et al. (2024) researched image super-resolution reconstruction using convolutional neural networks[4]. Wu (2024) focused on semantic parsing for intelligent database query engines based on large language models[5]. Additionally, Zheng Ren presented two studies on role-oriented dialogue summarization, one on balancing role contributions and another on enhancing sequence-to-sequence models through adaptive feature weighting and dynamic statistical conditioning [6][7]. These contributions collectively demonstrate the diverse and expanding applications of AI and computing in various fields.

2. The Importance of Computer Network Security Maintenance

With the rapid development of the Internet and information technology, people in all walks of life can not spread information without the network and computers. Computer networks have gradually become a necessity in people's daily lives, and their dependence on computer networks is increasing day by day. The requirements for computer

networks such as online office in universities, full coverage of student dormitories, and online teaching are becoming increasingly high. However, with the rapid development of computer networks, network security issues have become increasingly prominent. The importance of cybersecurity has become a social issue that everyone is concerned about. If network security is not guaranteed, it can result in the leakage, alteration, or destruction of information, or the theft of assets or secrets, which could potentially cause irreparable losses. So the importance of ensuring computer network security is beyond doubt [8].

3. Threat factors of computer network information security

3.1 Computer virus attacks

Computer viruses are essentially a combination of computer instructions and computer program code. During the process of programming or inserting code and instructions, computer data and functions will also be affected to some extent, which will have adverse effects on the normal application of computers. Network hackers, with the goal of stealing important information from computers or damaging important information, rely on computer viruses to launch targeted attacks on computers. Due to the strong concealment, sensing, parasitism, and triggering characteristics of viruses, they can greatly affect the security of computer network information. Therefore, starting from computer viruses, reasonable preventive measures must be taken to reduce the possibility of computer data and programs being attacked by viruses, reduce the possibility of computer data being stolen or programs being lost, maintain the normal operation of computer networks, and reduce the probability of network paralysis [9].

3.2 Network Intrusion

The computer network being exploited by hackers for various illegal profits is called network intrusion. There are also various ways of network intrusion, such as eavesdropping, Trojan horse techniques, password methods, and concealment techniques. Hackers mainly attack information networks, such as government websites, financial institutions, and national key universities (with important scientific research projects). Hacker activities are frequent, using illegal interception, decryption, tampering, copying, and other forms to steal. Due to the existence of hackers, computer network information security will be seriously threatened, and national security interests will also be threatened, causing losses to public property [10].

3.3 Insufficient user security 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 cannot correctly understand antivirus software and firewall programs. Most people believe that such software will greatly affect the process performance of computer operation, so they choose not to install antivirus software and firewalls. In this process, if users use computers in public places and do not clean their personal information or passwords after use, it will directly trigger the occurrence of important information leakage problems. From an overall perspective, the inability to enhance user security awareness is the most significant factor threatening computer information security [11].

3.4 Insufficient operation management system

In the process of computer network information security management, there is a lack of corresponding human resources because there is not much investment in costs under the computer network, and the actual needs of users are also different. So when users demand higher standards, the corresponding management will also change. In this process, it is necessary for relevant management personnel to be able to manage it. Once there is a lack of professional management and technical personnel, it will affect computer network security [12].

4. Strategies for Enhancing Computer Network Security Prevention

4.1 Application of Firewall Technology

In the process of building a network security system, firewalls are needed to effectively block malicious information and prevent computer poisoning through the use of firewalls. Therefore, in the process of improving network security systems, firewall technology should be actively utilized and effectively integrated with computer systems to enhance the security performance of firewalls. In the composition of firewalls, network level and application level gateways are very important. By effectively applying application level gateways, the security of

computer transmission and reception data can be checked in a timely manner, and backups can be implemented with the help of gateways. This technology ensures better effective communication between servers and customers. At the same time, through the application of application level gateways, it is possible to timely understand the actual needs of computers and access them according to specific requirements [13]. A network firewall analyzes and checks the reception and transmission of information based on data ports and specific requirements.

4.2 Strengthen the control of computer network access permissions

Strengthening the control of computer network access permissions is an effective way to improve the security of computer network information usage. Access control mainly refers to the strategy of strictly authenticating the identity of computer network users to prevent unauthorized users from accessing. By distinguishing different identities and assigning them a unique account as a unified electronic identity, they can log in to the network using a unique unified electronic identity. Strengthening the control of computer network access permissions is the most direct and effective means, greatly increasing the security of computer networks [14].

4.3 Continuously strengthen computer system optimization

The design of computer network security technology systems is relatively complex, and it is necessary to comprehensively strengthen the optimization and upgrading of computer systems. To this end, it is necessary to combine the needs of the development of computer networks, continuously share and exchange technologies, fully draw on the experience of upgrading, managing, and maintaining computer network systems at home and abroad, and achieve comprehensive verification of user information through configuring encryption key software and other methods; Strengthen the optimization configuration of conventional systems, conduct regular risk assessments, and promptly prevent potential issues. In addition, it is necessary to comprehensively strengthen the optimization configuration of computer hardware and software systems, timely replace mismatched related software or old components, in order to better create a good operating environment.

4.4 Application of Network Information Encryption Technology

The application of network information encryption technology can reduce the leakage of information data during transmission or storage. With the advent of the information age, the security of user information data can be effectively guaranteed through the application of encryption technology. Currently, the application of key technology can make hardware the core content of computer information security protection, which has a preventive effect on network hackers entering computer hardware systems and preventing them from entering the interior of network systems. The application of this technology in information exchange can rely on password pairing to identify network attackers, reducing the occurrence of network security vulnerabilities and reverse applications by criminals to achieve network system attacks. The application of key technology can encrypt information technology before data transmission. After the information is transmitted to the corresponding target, security algorithms can be used to decrypt the password using public or private keys. This not only ensures the security of information transmission, but also reduces the probability of information attacks and interception problems.

4.5 Learn advanced technology

The development of computer network security requires the assistance of relevant professionals. Therefore, in the research process of computer network security technology, a high-quality security management team should be built, which not only needs to strengthen the research on technology, but also continuously learn advanced technology in it, so as to better improve the level of computer network technology. Computer security managers can use the method of designing problems to determine the identity of users when they need to obtain corresponding information, thereby enabling users to obtain the information they want in a timely manner. We should also strengthen network monitoring and evaluation, and have a professional management team evaluate network equipment. Regular inspections of network equipment are also important methods to ensure network security.

4.6 Enhance the security awareness of network users

Firstly, for various threats to network security, it is necessary to strengthen users' awareness of network security, and most importantly, their awareness of protecting their personal privacy information. Relevant units should

strengthen the popularization of network security knowledge, and within the unit, employees can be alerted to "phishing" websites and website links that inexplicably pop up on websites. Typical templates for fraudulent and fake websites can be listed to enhance the awareness of relevant personnel towards fake websites. In this way, employees can avoid falling into the trap of unknown websites and software. Units should regularly promote network security knowledge and encourage employees to develop the habit of using antivirus software for scanning when downloading software, in order to prevent computer networks from being infected by viruses.

4.7 Improve management mechanisms

Information security management is the comprehensive integration of software and hardware facilities, information managers, and data users with information security protection functions through scientific organizational mechanisms, regulations, and control measures, to ensure that the organization can achieve predetermined information security goals and ensure the availability of information security and privacy. Specifically, information security management includes two aspects: management measures and security methods. Information security management must fully consider the value of technology in terms of systems and means. Only through the combination of systems, means, technology, and other aspects can comprehensive integration be achieved and the best security management effect be achieved.

5. Conclusion

In summary, computer networks have gradually become a necessity in people's daily lives, and their dependence on computer networks is increasing day by day. With the deepening development of computer networks, network security issues have become an important concern for people today. From the current situation of computer network security in China, there are many problems in computer network security, which pose significant risks and may cause irreparable losses to human society. To ensure the maximum security of computer networks, it is necessary to take preventive measures against the existing problems.

REFERENCES

[1] Xu, Y., Gao, W., Wang, Y., Shan , X., & Lin, Y.-S. (2024). Enhancing user experience and trust in advanced LLM-based conversational agents. Computing and Artificial Intelligence, 2(2), 1467. https://doi.org/10.59400/cai.v2i2.1467

[2] Chen, J., Lin, Q., & Allebach, J. P. (2020). Deep learning for printed mottle defect grading. Electronic Imaging, 32, 1-9.

[3] Chen, J., Zhang, X., Wu, Y., Ghosh, S., Natarajan, P., Chang, S. F., & Allebach, J. (2022). One-stage object referring with gaze estimation. In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (pp. 5021-5030).

[4] Yan, H., Wang, Z., Xu, Z., Wang, Z., Wu, Z., & Lyu, R. (2024, July). Research on image super-resolution reconstruction mechanism based on convolutional neural network. In Proceedings of the 2024 4th International Conference on Artificial Intelligence, Automation and High Performance Computing (pp. 142-146).

[5] Wu, Z. (2024). Large Language Model Based Semantic Parsing for Intelligent Database Query Engine. Journal of Computer and Communications, 12(10), 1-13.

[6] Zheng Ren, "Balancing role contributions: a novel approach for role-oriented dialogue summarization," Proc. SPIE 13259, International Conference on Automation Control, Algorithm, and Intelligent Bionics (ACAIB 2024), 1325920 (4 September 2024); https://doi.org/10.1117/12.3039616

[7] Z. Ren, "Enhancing Seq2Seq Models for Role-Oriented Dialogue Summary Generation Through Adaptive Feature Weighting and Dynamic Statistical Conditioninge," 2024 6th International Conference on Communications, Information System and Computer Engineering (CISCE), Guangzhou, China, 2024, pp. 497-501, doi: 10.1109/CISCE62493.2024.10653360.

[8] Guangqian Zhou Preventive Measures for Computer Network Security in the Era of Big Data [J]. Information and Computers (Theoretical Edition), 2019, 31 (24): 189-190193

[9] Lifan Zheng, Gang Li Related factors and prevention strategies affecting computer network security technology [J]. China New Communications, 2019, 21 (9): 135

[10] Qing Xie The influencing factors and prevention strategies of computer network security technology [J]. Network Security Technology and Application, 2021 (2): 161-163

[11] Li Zhang Research on Computer Network Security Issues and Countermeasures Based on Internet of Things Technology [J]. Information and Computer (Theoretical Edition), 2020, 32 (13): 203-204

[12] Guan, C., Mou, J., & Jiang, Z. (2020). Artificial intelligence innovation in education: A twenty-year data-driven historical analysis. *International Journal of Innovation Studies*, *4*(4), 134-147.
[13] Tiwari, P. C., Pal, R., Chaudhary, M. J., & Nath, R. (2023). Artificial intelligence revolutionizing drug development: Exploring opportunities and challenges. *Drug Development Research*, *84*(8), 1652-1663.
[14] Khalifa, M., & Albadawy, M. (2024). Artificial Intelligence for Clinical Prediction: Exploring Key Domains and Essential Functions. *Computer Methods and Programs in Biomedicine Update*, 100148