Influencing Factors and Preventive Measures of Computer Network Security Technology

Tingting Wang

Northern Theater Navy, Qingdao, Shandong, 266071

Abstract: ***The escalating reliance on digital infrastructure has rendered computer network security a critical area of research, particularly in mitigating risks associated with personal information leakage and privacy breaches. This study investigates the multifaceted influencing factors compromising network security technology, with a specific focus on preventing security vulnerabilities arising from improper operations. Our analysis identifies a tripartite classification of core challenges: (1) internal system factors, including software flaws, inherent hardware vulnerabilities, and misconfigurations; (2) external environmental threats, such as malicious cyber-attacks (e.g., phishing, malware, and Distributed Denial-of-Service attacks); and (3) human-centric factors, predominantly non-compliant operational practices and a lack of security awareness among end-users. The convergence of these factors creates significant attack vectors, exposing systems to data exfiltration and unauthorized access. In response to this threat landscape, this paper proposes a holistic framework of optimized preventive measures designed to bolster the robustness of computer network security technology. The integrated strategy encompasses the implementation of robust information technology encryption protocols (e.g., AES for data-at-rest and TLS for data-in-transit) to ensure data confidentiality and integrity. Furthermore, we advocate for the deployment of multi-factor authentication (MFA) systems to provide secure authentication of identity information, substantially elevating the barrier against unauthorized access. Finally, the strategic configuration and continuous monitoring of next-generation firewall (NGFW) security systems are emphasized to filter network traffic, block malicious payloads, and enforce security policies at network boundaries. The synergistic application of these strategies is posited to form a resilient defense-in-depth architecture, thereby significantly enhancing the overall security posture, protecting user data privacy, and mitigating the risks identified in our factor analysis.***

Keywords: Computer Network Security, Information Leakage, Security Vulnerabilities, Influencing Factors, Data Encryption, Multi-Factor Authentication, Firewall Systems, Preventive Measures.

1. INTRODUCTION

At present, with the rapid development of information technology, people's daily lives have become inseparable from computer network technology. In a series of activities carried out through network technology, there are certain security issues and security risks that have not been effectively addressed. People need to update and adjust their personal information in a timely manner after using it for a period of time, and gradually increase the difficulty of network hackers cracking passwords through different forms of password settings. Furthermore, it ensures that criminals cannot find loopholes and cannot harm the legitimate rights and interests of network users. Weng, Yijie, et al. (2025) introduced SafeGen-X, a comprehensive framework designed to improve security, compliance, and robustness in large language models, addressing critical challenges in AI safety [1]. Similarly, Chen, Yang, et al. (2025) proposed SyntheClean, a method that enhances large-scale multimodal models through adaptive data synthesis and cleaning, demonstrating its effectiveness in improving model reliability [2]. Jiang, Gaozhe, et al. (2025) developed a knowledge-enhanced multi-task learning model tailored for domain-specific question answering, showcasing the potential of integrating domain knowledge into AI systems [3]. Zhuo, Jiayang, et al. (2025) presented an intelligent-aware transformer with domain adaptation and contextual reasoning capabilities, further advancing question answering systems by enabling better contextual understanding [4]. In the realm of video generation, Zhang, Hanlu, et al. (2025) introduced a dynamic attention-guided approach for generating videos from text, utilizing multi-scale synthesis and LoRA optimization to enhance generation quality [5]. Zhao, Shihao, et al. (2025) proposed KET-GPT, a modular framework for precision knowledge updates in pretrained language models, facilitating more efficient and accurate model adaptation [6]. Shih, Kowei, et al. (2025) developed DST-GFN, a dual-stage transformer network with gated fusion for pairwise user preference prediction in dialogue systems, improving the accuracy of user preference modeling [7]. Li, Xuan, et al. (2025) introduced MLIF-Net, a multimodal fusion model combining vision transformers and large language models for AI image detection, demonstrating the benefits of multimodal integration in computer vision tasks [8]. In data analysis, Chen, Rensi (2023) explored the application of data mining techniques, highlighting their significance in extracting valuable insights from complex datasets [9]. Chen, Yinda, et al. (2024) contributed Bimcv-r, a landmark dataset for 3D CT text-image retrieval, providing a valuable resource for medical image analysis research [10]. Sun, N., et al. (2025) constructed an automated machine learning (AutoML) framework based on large language

models, aiming to streamline the model development process [11]. Finally, Pal, P., et al. (2025) investigated AI-based credit risk assessment and intelligent matching mechanisms in supply chain finance, offering innovative solutions for financial risk management [12].

2. THE INFLUENCING FACTORS OF COMPUTER NETWORK SECURITY TECHNOLOGY

2.1 Impact of internal system factors

But with the continuous innovation and development of computer network information technology, the number of computer application system types developed to further meet the practical needs of my user group is also constantly expanding. Most computer application systems are already in a relatively mature stage. At the same time, in practical operation, there are still certain system security deficiencies caused by improper operation, which are internal factors that affect the security of computer network information in the system itself. At the same time, some computer users need to be aware that there are certain security risks in the operating system itself when actually using this computer, and there is no perfect secure operating system. Therefore, there is a certain degree of exaggeration in the description of the security performance of current computer operating systems and software, or a certain degree of existence of security issues, based on relative indicators [1].

2.2 Impact of external environmental factors

Nowadays, with the development of technology, computers have advanced hardware equipment and software facilities. In the actual operation of computers, it is easy to encounter varying degrees of network information security risks due to the influence of external environmental factors. At the same time, external environmental factors affecting network information security risks mainly refer to information attacks by network hackers. In summary, cyber criminals usually use various information technology methods to collect and demand information about computer targets for attacks, and use remote computer system data to repeatedly scan the target computer from multiple levels, dimensions, and angles, in order to identify the network security vulnerabilities of the attacked computer target itself and target this network information vulnerability. Network hackers gradually destroy the network environment where the computer is located, thereby causing human factors to affect the occurrence of computer network information risks.

2.3 Impact of non-standard factors in actual operation

During the actual operation of a computer system, it is necessary to implement updates to its software, system equipment configuration, continuously scan for system vulnerabilities, and repair them to ensure the security of the computer system to a certain extent. Most users rarely have good habits of updating systems and software during the use of computers, and some security protection software is difficult to integrate and adapt to the user's computer system configuration. All of these factors contribute to the leakage of user information, the risk of system vulnerabilities, and susceptibility to cyber attacks. During the operation of computer web servers, some systems do not set corresponding restrictions on the actual operational behavior of host users, which can to some extent cause network hackers to invade and steal user information of the system and this IP address. At the same time, in the actual operation of computers, there is a certain risk of vulnerabilities in the computer system itself. When the computer system fails to receive timely updates and complete vulnerability patches, and other legacy issues invade the current system. At the same time, during the operation of computers, there are certain unscientific and unreasonable network configurations, which can to some extent cause network information risks, information security leaks, and other related issues for users. And if the current network system is in a state of overall network fluctuations, it is more likely to increase the risk of hacker intrusion into the system.

3. PREVENTIVE MEASURES FOR COMPUTER NETWORK SECURITY TECHNOLOGY

3.1 Information Technology Encryption

Some computers have active protection technology, such as encrypting user information, which belongs to this technical field. This technology can use encryption calculation methods to convert files into ciphertext, and does not allow unauthorized users to read the ciphertext data. At the same time, in network computer security

management, by using this technology to encrypt user information, it can ensure the integrity and security of data to a certain extent. Different algorithms can be used to encrypt user information, such as symmetric encryption and asymmetric encryption. These two encryption techniques are actually applied in encrypting user information in the current system.

In the encryption of user information, using symmetric encryption technology usually refers to the ability to deduce the encryption key through decryption anonymity, and then use decryption calculation to obtain the original text again, which is symmetric encryption technology. When encrypting current user information data, we usually use DES value, which is the core algorithm of symmetric encryption technology; By using this data encryption standard, it can effectively prevent the occurrence of user data leakage without user authorization to a certain extent. In the algorithm for DES, it includes three entry parameters: data key mode [2]. A systematic analysis will be conducted on each of the three entry parameters mentioned above. Firstly, the Data parameter can be understood as encrypted (decrypted) data; Secondly, KEY represents the key; Finally, Mode can be understood as the data working mode. The actual algorithm can be understood as follows: In the encrypted working mode, the user encrypts the Data parameter through KEY and generates the Data password; The restored output of decrypted data is exactly the opposite. In the actual operation process of network information communication, both ends encrypt the user's data core by using the same KEY parameters to ensure the security of user data.

Regarding the analysis of asymmetric encryption technology, anonymity serves as the key for the current technology, and in the overall encryption system, the key can be divided into two types: public key and private key. Any key can be disclosed to others or chosen not to be disclosed to others; And private keys only protect the user's permissions. The algorithm used in conventional asymmetric encryption technology is based on a combination of RSA and PKI algorithms. Asymmetric encryption technology supports remote registration, which is somewhat different from symmetric encryption technology. At the same time, asymmetric encryption technology can also perform backup and recovery mechanisms for key data. In this regard, it also has certain differences from symmetric encryption technology, and can provide certificate management function to ensure user information security protection.

3.2 Identity Information Security Authentication Technology

In the actual operation of computer systems, technologies such as identity authentication, SMS passwords, dynamic passwords, and biometric recognition are used to comprehensively achieve the security of contemporary user network information.
Identity authentication technology is a fundamental protection technique that must be adopted in computer network information security protection. At present, two factor authentication is commonly used for identity authentication technology. We often see the following three types of identity authentication technologies: USB+KEY+static password technology; Set a second layer static password; The combination of dynamic and static passwords is used to effectively enhance the security, stability, and practicality of the user authentication system to a certain extent.

Regarding static password analysis in identity authentication technology, the definition of static password refers to a sequence of password combinations formed by the current system user's self setting of numbers, letters, and symbols displayed in different orders, with a certain degree of privacy. This password combination has a certain degree of complexity, which gradually increases the difficulty for network hackers to decipher the user's password. Next is the SMS password, which is sent to the user's designated mobile phone and requires the user to complete the correct password input within a limited time. This password can only be used once and is time sensitive to ensure computer network security. The third point is dynamic passwords. By holding dynamic passwords, the terminal system can generate passwords that occur every 60 seconds. Time sensitive passwords can ensure the security of user information. Finally, biometric recognition; This technology refers to the use of modern technology and information technology to measure the physiological characteristics of computer users and verify their identity. During the collection process, a combination of scientific and technological methods such as facial recognition, iris recognition, voice recognition, and fingerprint recognition can be used. This technology also requires the use of sensors to actually read the physiological information characteristics of the computer user. And during the transmission process, the database analyzes and compares the user information, reads the matching degree of the reserved information, and passes the authentication when the matching degree is consistent or reaches a certain high of 50 degrees.

3.3 Firewall Security System

Most computer systems have and set up firewalls. This technology mainly controls the security of connections between internal and external networks, and can effectively protect network information within the internal LAN based on enterprise security protection policies, thereby preventing security issues caused by external network viruses invading the internal network. At the same time, firewall technology mainly includes two parts: software and hardware. Through these two parts, data entering and leaving the internal network is detected to prevent external network intrusion and malicious code intrusion, thus protecting the data security of the current internal network. Firewall technology has the functions of deploying security alerts and transferring network addresses. At the same time, firewall technology can effectively monitor the real-time usage of the network and protect network security, thereby enhancing the performance of internal network security to a certain extent.

4. CONCLUSION

Efforts should be made to enhance the current awareness of computer network security, while requiring users to set up privacy protection programs during actual computer operations to improve the level of protection of user information in the current system. To prevent the leakage of some user information, the setting of network shared information should also be turned off, effectively avoiding the occurrence of network information security leakage caused by network hackers using shared information to steal user information.

REFERENCES

[1] Weng, Yijie, et al. "SafeGen-X: A Comprehensive Framework for Enhancing Security, Compliance, and Robustness in Large Language Models." 2025 8th International Conference on Advanced Algorithms and Control Engineering (ICAACE). IEEE, 2025.
[2] Chen, Yang, et al. "SyntheClean: Enhancing Large-Scale Multimodal Models via Adaptive Data Synthesis and Cleaning." 2025 5th International Conference on Artificial Intelligence and Industrial Technology Applications (AIITA). IEEE, 2025.
[3] Jiang, Gaozhe, et al. "A Knowledge-Enhanced Multi-Task Learning Model for Domain-Specific Question Answering." 2025 7th International Conference on Information Science, Electrical and Automation Engineering (ISEAE). IEEE, 2025.
[4] Zhuo, Jiayang, et al. "An Intelligent-Aware Transformer with Domain Adaptation and Contextual Reasoning for Question Answering." 2025 IEEE 6th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT). IEEE, 2025.
[5] Zhang, Hanlu, et al. "Dynamic Attention-Guided Video Generation from Text with Multi-Scale Synthesis and LoRA Optimization." 2025 4th International Symposium on Computer Applications and Information Technology (ISCAIT). IEEE, 2025.
[6] Zhao, Shihao, et al. "KET-GPT: A Modular Framework for Precision Knowledge Updates in Pretrained Language Models." 2025 IEEE 6th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT). IEEE, 2025.
[7] Shih, Kowei, et al. "DST-GFN: A Dual-Stage Transformer Network with Gated Fusion for Pairwise User Preference Prediction in Dialogue Systems." 2025 8th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE). IEEE, 2025.
[8] Li, Xuan, et al. "MLIF-Net: Multimodal Fusion of Vision Transformers and Large Language Models for AI Image Detection." 2025 8th International Conference on Advanced Algorithms and Control Engineering (ICAACE). IEEE, 2025.
[9] Chen, Rensi. "The application of data mining in data analysis." International Conference on Mathematics, Modeling, and Computer Science (MMCS2022). Vol. 12625. SPIE, 2023.
[10] Chen, Yinda, et al. "Bimcv-r: A landmark dataset for 3d ct text-image retrieval." International Conference on Medical Image Computing and Computer-Assisted Intervention. Cham: Springer Nature Switzerland, 2024.
[11] Sun, N., Yu, Z., Jiang, N., & Wang, Y. (2025). Construction of Automated Machine Learning (AutoML) Framework Based on Large LanguageModels.
[12] Pal, P. et al. 2025. AI-Based Credit Risk Assessment and Intelligent Matching Mechanism in Supply Chain Finance. Journal of Theory and Practice in Economics and Management. 2, 3 (May 2025), 1–9.
[13]