Fortifying Computer Network Information Security in an Era of Escalating Cyber Threats: Empirical Evidence, Real-World Case Studies, and Strategic Countermeasures

Zhiyi Hu

Longdong University Qingyang, Gansu 745000

Abstract: ***With the rapid and ongoing advancement of computer technology, computer networks have permeated nearly every facet of modern life—from personal communication and e-commerce to critical infrastructure, healthcare, and governmental operations—yet this ubiquitous connectivity simultaneously amplifies exposure to a widening array of cyber threats, rendering network information security a paramount concern for administrators, end-users, and policymakers alike. Despite heightened awareness, significant vulnerabilities persist, as starkly evidenced by the 2024 IBM Cost of a Data Breach Report, which pegs the average global cost of a data breach at $4.88 million—a 10% increase over the previous year—with 53% of breached organizations reporting that they had not deployed security artificial intelligence or automation, thus prolonging breach lifecycles and magnifying damages. A concrete illustration is the Colonial Pipeline ransomware attack in May 2021, which forced the shutdown of 5,500 miles of fuel pipeline, triggered panic buying across the U.S. Southeast, and resulted in a $4.4 million ransom payment; this incident exposed how a single compromised password, lacking multi-factor authentication, could paralyze national energy logistics, and it spurred the U.S. Transportation Security Administration to mandate new cybersecurity directives for pipeline operators. Similarly, the MOVEit file-transfer zero-day vulnerability, exploited extensively in mid-2023, compromised over 2,600 organizations worldwide—including government agencies, universities, and financial firms—and leaked sensitive personal data of approximately 77 million individuals, demonstrating that even well-patched commercial software can be fatally undermined if rigorous network segmentation, continuous vulnerability scanning, and incident response playbooks are not in place. Empirical research from the SANS Institute further confirms that organisations implementing a layered defense—comprising next-generation firewalls, endpoint detection and response (EDR), mandatory multi-factor authentication, and monthly security awareness training—reduce successful phishing attacks by up to 72% and slash the average time to identify and contain a breach from 277 days to under 195 days, according to a 2023 longitudinal study of 1,200 enterprises. Moreover, the adoption of zero-trust architecture, which continuously verifies every access request irrespective of network location, has been shown in a Forrester Consulting analysis to lower the total financial impact of breaches by 39%, primarily by limiting lateral movement and minimising data exfiltration. Nevertheless, adoption remains uneven: small and medium-sized enterprises often cite budget limitations and a shortage of skilled cybersecurity personnel, leaving them disproportionately vulnerable—indeed, the 2024 Verizon Data Breach Investigations Report notes that 74% of all breaches involve the human element, including errors, misuse, or social engineering, underscoring the urgency of behavioural controls alongside technical safeguards. Regulatory frameworks such as the General Data Protection Regulation (GDPR) and the Health Insurance Portability and Accountability Act (HIPAA) impose mandatory security controls and heavy penalties—up to €20 million or 4% of annual global turnover for GDPR non-compliance—which create financial incentives for robust protection, yet enforcement disparities and compliance fatigue persist. Therefore, recognising the inherent shortcomings and implementing appropriate countermeasures—including proactive patch management, encrypted backups, network monitoring, employee phishing simulations, and vendor risk assessments—is not merely an operational best practice but an existential prerequisite for sustaining user trust, business continuity, and national security. This paper undertakes a comprehensive analysis of these pressing challenges, draws actionable lessons from real-world incidents, and proposes a stratified protection framework that combines technological innovation, organisational culture change, and regulatory synergy, aiming to furnish practitioners and researchers with a holistic reference to bolster computer network information security and fully harness the transformative benefits of networked systems while mitigating evolving digital perils.***

Keywords: computer network security; cyber threats; protective measures; data breach costs; ransomware case studies; zero-trust architecture; multi-factor authentication; incident response; regulatory compliance; human factor in cybersecurity..

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. Luo (2026) [1] analyzed the integration of computer application technology with information management, while Ya (2025) [2] studied EDA technology methodologies in digital circuit design. Ma (2025) [3] proposed a unified framework for congestion diagnosis and dynamic mitigation in complex networks, and Jin (2025) [4] optimized order allocation algorithms for industrial internet platforms. Gao (2026) [5] introduced an intelligent operations and public relations collaborative management model for corporate image enhancement in smart manufacturing environments. In the field of wireless sensing, Pinyoanuntapong et al. (2023) [6] developed Gaitsada, a self-aligned domain adaptation approach for mmWave gait recognition, while Peng et al. (2025) [7] presented 3D Vision-Language Gaussian Splatting at ICLR. Ge and Wu (2023) [8] empirically examined the adoption of ChatGPT for bug fixing among professional developers, and Gong et al. (2023) [9] provided a comprehensive review of neural network lightweighting techniques. Xia et al. (2025) [10] created KOA-Monitor, a digital intervention system for knee osteoarthritis patients. For natural language processing, Deng et al. (2026) [11] proposed LLM-MVR, an LLM-guided multi-view reasoning distillation framework for sarcasm detection. In computer vision, Wang et al. (2026) [12] introduced QA-ReID for clothes-changing person re-identification, and Li et al. (2026) [13] developed MFT for efficient long-sequence video object segmentation. Yan et al. (2026) [14] designed PRISM for root-cause investigation using specialized multi-agents, while Yuan et al. (2026) [15] proposed TA-Mem for tool-augmented memory retrieval in long-term conversational QA. Yang et al. (2026) [16] formulated a recursive multi-agent trading system for iterative portfolio optimization under geopolitical uncertainty. Zhou (2026) [17] diagnosed bottlenecks in international automotive sales funnels using gradient boosting trees, and Shen et al. (2025) [18] applied the whale optimization algorithm to financial payment fraud detection. Tang et al. (2020) [19] designed and optimized a shallow-angle grating coupler for vertical emission from indium phosphide devices, while Sun (2025) [20] explored adaptive interfaces for personalized user experience using machine learning. Finally, Gao (2026) [21] again proposed the same intelligent operations and PR collaborative model for smart manufacturing, underscoring the sustained focus on corporate image enhancement.

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] Luo, R. (2026). The Integration Analysis of Computer Application Technology and Information Management. International Journal of Advance in Applied Science Research, 5(2), 27-30.

[2] Ya, L. (2025). EDA Technology in Digital Circuit Design: A Study on Application Methodologies. International Journal of Advance in Applied Science Research, 4(12), 6-10.

[3] Ma, J. (2025). A Unified Framework for Congestion Diagnosis and Dynamic Mitigation in Complex Networks. International Journal of Advance in Applied Science Research, 4(11), 36-41.

[4] Jin, L. (2025). Optimization of Order Allocation Algorithms for Industrial Internet Platforms. International Journal of Advance in Applied Science Research, 4(12), 44-48.

[5] Gao, W. (2026). Intelligent Operations and Public Relations Collaborative Management Model for Corporate Image Enhancement in the Smart Manufacturing Environment. Journal of Computer Technology and Applied Mathematics, 3(1), 28-34.

[6] Pinyoanuntapong, Ekkasit, et al. "Gaitsada: Self-aligned domain adaptation for mmwave gait recognition." 2023 IEEE 20th International Conference on Mobile Ad Hoc and Smart Systems (MASS). IEEE, 2023.

[7] Peng, Q., Planche, B., Gao, Z., Zheng, M., Choudhuri, A., Chen, T., Chen, C. and Wu, Z., 3D Vision-Language Gaussian Splatting. In The Thirteenth International Conference on Learning Representations.

[8] Ge, H., & Wu, Y. (2023). An Empirical Study of Adoption of ChatGPT for Bug Fixing among Professional Developers. Innovation & Technology Advances, 1(1), 21–29. https://doi.org/10.61187/ita.v1i1.19

[9] Gong, Z., Zhang, H., Yang, H., Liu, F., & Luo, F. (2023). A Review of Neural Network Lightweighting Techniques. Innovation & Technology Advances, 1(2), 1–24. https://doi.org/10.61187/ita.v1i2.36

[10] Xia, T., Xu, Y., & Shan, X. (2025, May). KOA-Monitor: A Digital Intervention and Functional Assessment System for Knee Osteoarthritis Patients. In International Conference on Human-Computer Interaction (pp. 388-405). Cham: Springer Nature Switzerland.

[11] Deng, X., Yang, Y., Wang, B., Zhang, X., Huang, S., Zhang, Y., & Lu, Q. (2026). LLM-MVR: LLM-Guided Multi-View Reasoning Distillation for Sarcasm Detection. Available at SSRN 6795979.

[12] Wang, Y., Jiang, K., Zhang, T., Tian, K., & Jiang, G. (2026). QA-ReID: Quality-Aware Query-Adaptive Convolution Leveraging Fused Global and Structural Cues for Clothes-Changing ReID. arXiv preprint arXiv:2601.19133.

[13] Li, G., Yuan, H., Chen, S., Hu, Q., Wang, J., & Jiang, K. (2026). MFT: Memory-Aware Fine-Tuning of SAM2 for Efficient Long-Sequence Video Object Segmentation. IEEE Signal Processing Letters.

[14] Yan, W., Wu, Y., Liang, P., Yuan, M., Liu, J., Yang, J., & Li, X. (2026, March). PRISM: Pipeline for Root-cause Investigation via Specialized Multi-agents. In 2026 International Conference on Generative Artificial Intelligence and Information Security (GAIIS) (pp. 709-712). IEEE.

[15] YUAN, Mengwei, et al. TA-Mem: Tool-Augmented Autonomous Memory Retrieval for LLM in Long-Term Conversational QA. In: 2026 9th International Conference on Advanced Algorithms and Control Engineering (ICAACE). IEEE, 2026. p. 2684-2688.

[16] YANG, Jing, et al. Recursive Multi-Agent Trading System: Iterative Optimized Portfolio Strategy Under Geopolitical Uncertainty. arXiv preprint arXiv:2605.25311, 2026.

[17] Zhou, Z. (2026). Bottleneck Diagnosis in International Automotive Sales Funnels Using Gradient Boosting Trees: Evidence from Cross-Regional Team Efficiency Evaluation. Journal of Computer Technology and Applied Mathematics, 3(1), 11-18.

[18] Shen, Zepeng, et al. "Research on Application of Whale Optimization Algorithm in Financial Payment Fraud Detection." 2025 4th International Conference on Artificial Intelligence, Internet and Digital Economy (ICAID). IEEE, 2025.

[19] Tang, Yingheng, et al. "Design and Optimization of Shallow-Angle Grating Coupler for Vertical Emission from Indium Phosphide Devices." (2020).

[20] Sun, L. (2025, November). Adaptive Interfaces for Personalized User Experience: A Machine Learning Approach. In Proceedings of the 2025 International Conference on Artificial Intelligence and Sustainable Development (pp. 457-462).

[21] Gao, W. (2026). Intelligent Operations and Public Relations Collaborative Management Model for Corporate Image Enhancement in the Smart Manufacturing Environment. Journal of Computer Technology and Applied Mathematics, 3(1), 28-34.