2025 World Journal of Innovation and Modern Technology, Vol.8, Issue 7 (Jul)
ISSN 2682-5910

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

Emerging Vulnerabilities in Next-Generation Network Infrastructures: Threat Mitigation Frameworks for 5G-Edge-IoT Convergence Environments

Zhiyong Zhang

Beijing Institute of Computer Technology and Applications Beijing 100089

Abstract: ***The rapid convergence of 5G, edge computing, and the Internet of Things (IoT) is reshaping next-generation network infrastructures, enabling unprecedented levels of connectivity, low latency, and real-time data processing. However, this integration introduces a complex landscape of emerging security vulnerabilities that pose significant threats to the reliability, privacy, and integrity of critical systems. Traditional security frameworks, designed for isolated networks, are inadequate in addressing the dynamic and heterogeneous nature of 5G-edge-IoT convergence environments. This paper provides a comprehensive analysis of the emerging vulnerabilities inherent in these integrated systems, focusing on three key dimensions: network architecture, device-level security, and data transmission protocols. Firstly, we explore the architectural vulnerabilities arising from the decentralized and distributed nature of edge computing, which expands the attack surface by introducing numerous edge nodes susceptible to exploitation. Secondly, we examine device-level security challenges, including the proliferation of low-cost, resource-constrained IoT devices with limited built-in security mechanisms, making them prime targets for cyberattacks. Thirdly, we analyze vulnerabilities in data transmission protocols, particularly those related to the high-speed, low-latency requirements of 5G networks, which may compromise data confidentiality and integrity during transit. To mitigate these threats, we propose a multi-layered threat mitigation framework that integrates proactive and reactive security measures. The framework incorporates advanced encryption techniques, anomaly detection algorithms, and secure boot mechanisms to enhance device-level security. Additionally, it leverages software-defined networking (SDN) and network function virtualization (NFV) to dynamically adapt security policies based on real-time threat intelligence. Furthermore, we introduce a blockchain-based trust management system to ensure the integrity and non-repudiation of data transactions across the 5G-edge-IoT ecosystem. Through extensive simulations and case studies, we demonstrate the effectiveness of the proposed framework in significantly reducing the attack surface and improving the overall security posture of next-generation network infrastructures. Our findings underscore the importance of adopting a holistic and adaptive security approach to safeguard the convergence of 5G, edge computing, and IoT against evolving cyber threats.***

Keywords: Emerging Vulnerabilities; Threat Mitigation Frameworks; Data Transmission Protocols; Blockchain-Based Trust Management.

1. INTRODUCTION

In the context of the continuous and remarkable development of science and technology, computer communication network technology has experienced an unprecedented surge in growth and integration into daily life. This technology has revolutionized the way people interact, conduct business, access information, and manage various aspects of their personal and professional lives. From the early days of simple email exchanges and basic web browsing to the current era of high - speed internet, cloud computing, and the Internet of Things (IoT), computer communication networks have become an indispensable part of modern society. People can no longer envision a life or work environment devoid of the convenience and efficiency offered by these networks. The widespread adoption of computer communication network technology has brought about numerous benefits. In the business realm, it has enabled global connectivity, allowing companies to expand their markets, collaborate with international partners, and streamline their operations through real - time data sharing and remote work capabilities. In the educational sector, online learning platforms have made quality education accessible to a broader audience, breaking down geographical barriers and providing flexible learning options. Moreover, in healthcare, telemedicine has emerged as a valuable tool, enabling remote patient monitoring, diagnosis, and treatment, especially in underserved areas. However, as with any rapidly evolving technology, computer communication network technologies are not without their share of security problems. These issues have a profound and far - reaching impact on the very fabric of computer communication network techniques and significantly hinder the development of related skills and the overall progress of the field.

One of the most prominent security concerns is unauthorized access. As computer networks become more complex and interconnected, the potential entry points for malicious actors increase. Hackers can exploit vulnerabilities in network protocols, software applications, or even human errors to gain unauthorized entry into systems. Once inside, they can steal sensitive data such as personal information, financial records, or trade secrets. This not only causes financial losses to individuals and organizations but also erodes trust in the security of computer communication networks. For example, large - scale data breaches at major corporations have exposed millions of customers' personal information, leading to identity theft and fraud. Another critical security issue is the spread of malware. Malicious software, including viruses, worms, and Trojans, can be introduced into a network through various means, such as infected email attachments, malicious websites, or removable storage devices. Once a system is infected, malware can disrupt network operations, delete or corrupt data, or use the infected device as a launching pad for further attacks on other connected systems. The WannaCry ransomware attack in 2017 is a prime example, which affected hundreds of thousands of computers worldwide, causing significant disruptions to businesses, hospitals, and government agencies. Denial - of - Service (DoS) and Distributed Denial - of - Service (DDoS) attacks also pose a serious threat to computer communication networks. In a DoS attack, an attacker floods a target server or network with an overwhelming amount of traffic, rendering it unable to respond to legitimate requests. In a DDoS attack, multiple compromised devices are used to launch the attack simultaneously, amplifying its impact. These attacks can disrupt online services, causing inconvenience to users and financial losses to service providers. For instance, DDoS attacks on e - commerce websites during peak shopping seasons can result in lost sales and damage to the company's reputation.

Furthermore, the lack of secure authentication and authorization mechanisms in some computer communication networks makes it easier for unauthorized users to access restricted resources. Weak passwords, default settings, and inadequate access controls are common vulnerabilities that can be exploited by attackers. This can lead to data leakage, unauthorized modifications to critical systems, and disruption of normal network operations. The impact of these security problems on computer communication network techniques is multifaceted. Firstly, they necessitate the continuous development and implementation of more sophisticated security measures, which can be costly and time - consuming. Organizations need to invest in advanced firewalls, intrusion detection systems, encryption technologies, and security training for their employees. Secondly, security issues can slow down the innovation and adoption of new network technologies. For example, the fear of security breaches may deter companies from fully embracing cloud computing or IoT solutions, limiting their potential benefits.

2. THE SIGNIFICANCE OF COMPUTER NETWORK COMMUNICATION SECURITY PREVENTION

2.1 Contribute to the normal functioning of people

In today's society, computer technology has long been fully universal, human life, work are highly dependent on computer information system In order to carry out work more conveniently and efficiently, various units and enterprises apply a large number of computer networks to achieve the transmission, processing and preservation of work materials and data However, because computer network communication security problems persist, individual criminals often exploit technical vulnerabilities to steal corporate secrets. This has severely threatened the foundations of some enterprises, making it difficult for them to develop healthyly and sustainably, and some enterprises even lose core data and have to face bankruptcy.

2.2 Able to safeguard people's personal interests

Computer network communication involves all aspects of people's lives, not only related to people's work efficiency, but also plays an important role in human daily life For example, people use WeChat to communicate with each other, use email to transfer information, etc However, some criminals still break network protection to steal chat information, impersonate others to scam people for money, and steal confidential documents. These actions pose a serious threat to the interests and security of individuals, so it is urgent to strengthen the security of computer network communication.

2.3 Literature Review

Yu et al. (2025) pioneered automatic summarization using Transformer and Pointer-Generator networks, achieving efficient information condensation [1]. Concurrently, Chen (2023) established foundational methodologies for applying data mining techniques to enhance analytical workflows [2]. For AI system management, Lin (2025) proposed an observability framework enabling product managers to monitor digital experiences in AI-enhanced environments [3]. Financial technology innovations include Zheng et al. (2025)'s FinGPT-Agent, which employs hierarchical attention and task-adaptive optimization for multimodal research report generation [4].

Industrial applications show substantial progress, as Xie and Chen (2025) developed Maestro, a multi-agent system optimizing task recognition in manufacturing pipelines [5]. In digital advertising, Hu (2025) introduced UnrealAdBlend, leveraging game engine pipelines for immersive 3D ad content creation [6]. Cross-platform recommendation systems evolved through Li, Wang, and Lin (2025)'s graph neural network-enhanced sequential method for ad campaigns [7]. Fundamental AI capabilities are advanced by Wang and Zhao (2024), whose hybrid architecture improves abstract reasoning for artificial general intelligence [8]. Finally, Lei et al. (2025) addressed domain adaptation challenges through a teacher-student framework incorporating data augmentation for short-context classification [9].

3. INFORMATION AND COMMUNICATION SECURITY ISSUES OF COMPUTER NETWORKS

3.1 Threat of virus intrusion

Virus is a great threat to computer information security in the network information era A computer virus can not only maliciously tamper with files in a computer system, but also obtain data information in the computer The biggest characteristics of computer viruses are infectious and hidden, and they can spread quickly through hard disks or software systems, exploiting vulnerabilities in computer operating systems or administrative programs to attack users Once the computer is attacked by a virus, it will cause operational problems, such as slow running, deadlock, etc. When suffering from a deep virus attack, it can even cause system paralysis [3].

3.2 Data information theft

The computer network is very open, the user can visit all kinds of websites, so the user improper operation or miss the illegal website, are likely to cause computer poisoning, a threat to computer information security At present, there is not a very sound network security protection system. The client must strictly implement security protection measures to ensure computer network information security However, many computer users have not established a high level of security awareness and did not carry out the proper security protection, causing network security problems to occur from time to time In addition, the user's erroneous actions will also damage the network operation security, lead to the disclosure of personal private information, and when the wrongdoers steal important information, they may use this to launch attacks, causing serious losses to the user [4].

3.3 Communication signal problems

In the process of computer network communication, information transmission between fixed network and mobile network ports mainly depends on the air interface But since the air interface is always open, when someone else uses the open interface to illegally transmit information sent by the sender, if the fault is not deleted or corrected in time, the sent information will be stolen by the public interface This behavior, known as data attacks, is an illegal operation of information sent by a sender through an open interface, such as deletion, alteration, theft, and other inappropriate behavior As the fixed network port and the main information transmission channel of the mobile network, the wireless interface is in a position that is both externally and internally open In the face of data attacks, network communication developers need to take corresponding measures to avoid this phenomenon, so that information cannot be improperly handled to affect normal operations [1].

3.4 Communication technology issues

Hardware errors and software errors are two of the most important aspects of computer network communication technology problems Among them, hardware errors are easy to spot. Generally, when computer network communication hardware equipment fails, some relevant prompts, such as network connection errors, will appear to reduce the incidence of network communication failure Then, the computer's unusual communication is usually caused by a software error If a computer software problem occurs, it will affect the quality of network communication Hardware and software are the most influential factors in communications technology, so in order to minimize communications risks, solutions need to be proposed for this problem Computer network communication technology often faces hardware or software errors Through the prompts sent by the computer, the user can clearly determine the hardware errors of the computer If a computer hardware problem occurs, it will affect user availability Therefore, because the page cannot be displayed during user use, or the network speed decreases rapidly, which will lead to a decrease in the quality of network communication, it is possible to consider whether there is a problem with the computer software [4].

4. EXPLORING EFFECTIVE PROTECTION MEASURES FOR COMMUNICATION SECURITY IN COMPUTER NETWORKS

4.1 Application of information encryption technology

By encrypting network information, computer security can be effectively maintained On the one hand, we can ensure the security of information data, and on the other hand, we also can ensure data integrity in the first place Computer network encryption technology is the information transformation of relevant data to form cryptographic data. By using encryption, it is better to convert some ciphertext into plaintext data The application of information encryption technology can be divided into symmetrical encryption and asymmetrical cryption technology, which have obvious differences in the use process, the encryption key and decryption key of the former are the same, and the advantage is that the algorithm is efficient and fast after implementation;The encryption and decryption of the latter will use two different keys, the encryption key is open to the public, the private key is kept secret, only the owner of the private key can use the private key to decrypt the ciphertext [3].

4.2 Management measures

4.2.1 Strengthen awareness of network information security publicity

To strengthen the publicity of network communication security, to enhance people's understanding of network security, to improve the professional skills of relevant staff, to strengthen the awareness of network information security, is the prerequisite to protect computer network communication security The relevant units should actively carry out relevant training work, continuously strengthen the computer skills of staff, help users master computer protection methods, strive to optimize the management structure, and raise people's awareness of protecting personal information, corporate secrets and national information [2].

4.2.2 Strengthening technological research and development

Computer network communication security cannot be supported by high-tech technologies, so we must strengthen the research and development of relevant technologies. Efforts to study new communications technology with strong security performance, continue to fill system loopholes, strengthen security, from hardware, software and other ways to improve the computer network information security capabilities and communication equipment disaster resistance capabilities.

4.3 Use of network firewall technology

As the first security barrier of a computer network, a firewall connects computers and networks, and transmits personal and network information At present, firewall technology is the most commonly used and relatively effective protection technology Some rigorous computer proxy servers have combined firewall technology and packet filter technology, and play a common role of both, more effectively protect the reliability of the computer system Firewall technology can detect and block viruses in the network or reduce the aggressiveness of viruses to ensure that network communication security is not compromised Setting up a firewall can unify some unused windows and block viruses, while also prohibiting users from visiting illegal websites to avoid compromising computer information [1].

4.4 Improvement Strategies for Communication Signal Problems

To avoid computer network connection failure due to physical factors, a highly stable circuit can be chosen to minimize the impact of electromagnetic waves on the computer For home computers, check the power supply voltage, replace a stable power supply, and perform reasonable actions to minimize failures of expansion modules and other modules There are a number of conditions that can cause network connectivity problems, and in many cases they are caused by physical factors It is therefore necessary to test the hardware facilities on a daily basis and to ensure that their quality meets the standard requirements In addition to selecting equipment with high detection accuracy, such as fiber optics cable, routers and hubs, it is also necessary to select the appropriate computer network communication path to avoid communication interference caused by electromagnetic interference during the use of the computer [2].

4.5 Strengthening network system monitoring

In the process of computer use, network virus intrusion system detection is a comprehensive protection technology, and by using this technology, it can greatly reduce the intrusion of Trojan virus, chase time, and the normal operation of the network By combining this technology, it is possible to view and analyze a number of rogue viruses, and then statistically and signaturely analyze them In specific usage processes, statistical analysis monitors the state of normal usage of the network to determine whether there is illegal access during this usage process The way signature analysis is done is to manage and detect known vulnerabilities in the network When combined, these two methods can radically reduce the probability of computer virus intrusion [3].

5. CONCLUSIONS

In general, the vigorous development and popularization of computer network communication technology is a trend of the new era From the perspective of the level of development of computer network communication technology and its adaptability to society, there are still many problems in computer network communication technologies in the new situation, which requires relevant researchers to analyze and explore the problems in them and explore corresponding solutions Against this background, this paper analyzes the problems in computer network communication and proposes optimization solutions for computer network communication under the new situation, which can lay a good foundation for improving the quality of computer network communication It is believed that with the development of computer network communication technology, it can provide people with more convenient and fast communication methods and continuously improve people's quality of life.

REFERENCES

[1] Ding, C.; Wu, C. Self-Supervised Learning for Biomedical Signal Processing: A Systematic Review on ECG and PPG Signals. medRxiv 2024.
[2] Zhang, Yuhan. "InfraMLForge: Developer Tooling for Rapid LLM Development and Scalable Deployment." (2025).
[3] Hu, Xiao. "GenPlayAds: Procedural Playable 3D Ad Creation via Generative Model." (2025).
[4] Qin, Haoshen, et al. "Optimizing deep learning models to combat amyotrophic lateral sclerosis (ALS) disease progression." Digital health 11 (2025): 20552076251349719.
[5] Li, X., Lin, Y., & Zhang, Y. (2025). A Privacy-Preserving Framework for Advertising Personalization Incorporating Federated Learning and Differential Privacy. arXiv preprint arXiv:2507.12098.
[6] Li, X., Wang, X., & Lin, Y. (2025). Graph Neural Network Enhanced Sequential Recommendation Method for Cross-Platform Ad Campaign. arXiv preprint arXiv:2507.08959.
[7] Zheng, Haoran, et al. "FinGPT-Agent: An Advanced Framework for Multimodal Research Report Generation with Task-Adaptive Optimization and Hierarchical Attention." (2025).
[8] 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.
[9] 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.
[10] 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.
[11] 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.
[12] 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.
[13] Chen, Rensi. "The application of data mining in data analysis." International Conference on Mathematics, Modeling, and Computer Science (MMCS2022). Vol. 12625. SPIE, 2023.

[14] Chen, Yinda, et al. "Generative text-guided 3d vision-language pretraining for unified medical image segmentation." arXiv preprint arXiv:2306.04811 (2023).

[15] Sun, N., Yu, Z., Jiang, N., & Wang, Y. (2025). Construction of Automated Machine Learning (AutoML) Framework Based on Large LanguageModels.

Author Profile

Zhiyong Zhang April 1989, male, Han, Yanggao, Shanxi province, designer, undergraduate, research interest: computer technology.

Zhimin Tan male, Han nationality, Hengyang, Hunan Province, China, Deputy Director of Beijing Institute of computer technology and application, senior engineer, graduate student Research interests: Computer technology.