International Journal of Management Science Research, Vol.8, Issue 7, (Jul) 2025
ISSN 2536-605X
DOI: 10.53469/ijomsr.2025.08(07).03

Computer Network and Information Security System Establishment and Technical Research

Guodong Chen*

Guangdong Vocational College of Science and Trade, Guangzhou, Guangdong 510430
*Email: 2145324770@qq.com

Abstract: ***In today's era, computer application technology has entered thousands of homes, which not only improves people's efficiency in work, but also meets people' needs in daily life, realizing the widespread popularization and effective application of network technology. Along with the computer network technology application thorough, its information security management exposes many questions, seriously threatens the network application technology security. Therefore, it is urgent for us to take effective measures to improve the information security system to ensure the security of computer network information. Based on this, this paper discusses the establishment of computer network and information security system and the key technology for reference.***

Keywords: Computer network; Information security system; Established; Technology.

1. CHARACTERISTICS ANALYSIS OF COMPUTER NETWORKS

Computer networks are characterized by the following three points:

(1) Data can be transmitted and transported quickly

When the network is connected, data can be transmitted quickly, no matter how far away the distance is.

(2) The Internet has realized the sharing of information resources

In the computer network, the information resources are not limited by the time and space, anyone who uses the network can get the information resources he needs.

(3) Computer networks are now moving towards higher performance

Computer networks provide users with high-quality and convenient services as well as advanced science, technology and knowledge, which also promotes the development of computer networks, which provide users with a variety of services under advanced equipment. Jiang et al. (2025) introduced Investment Advisory Robotics 2.0, leveraging deep neural networks to provide personalized financial guidance, showcasing the potential of AI in finance [1]. Wang (2025) proposed a method for joint training of propensity and prediction models via targeted learning, addressing the challenge of recommendation systems dealing with data missing not at random [2]. Ding and Wu (2024) conducted a systematic review on self-supervised learning for biomedical signal processing, focusing on ECG and PPG signals, which contributes significantly to the healthcare domain [3]. Restrepo et al. (2024) explored multimodal deep learning in low-resource settings, employing a vector embedding alignment approach for healthcare applications, highlighting the importance of adaptable AI solutions [4]. Xie and Chen (2025) developed InVis, an interactive neural visualization system for human-centered data interpretation, enhancing the accessibility and interpretability of complex data [5]. Their subsequent work, CoreViz, introduced a context-aware reasoning and visualization engine for business intelligence dashboards, further advancing data visualization techniques [6]. Zhu (2025) proposed TraceLM, a framework for temporal root-cause analysis using contextual embedding language models, providing insights into temporal data patterns [7]. Zhang (2025) introduced CrossPlatformStack, enabling high availability and safe deployment for products across meta services, addressing scalability and reliability challenges [8]. Hu (2025) presented GenPlayAds, a procedural playable 3D ad creation system via generative models, showcasing the creative potential of AI in advertising [9]. Wang and Shih (2024) proposed a hybrid multi-modal recommendation system integrating MMOE and XGBoost, enhancing personalization and accuracy in recommendation tasks [10]. Fu et al. (2025) explored adversarial prompt optimization in LLMs, presenting HijackNet's approach to improving robustness and defense evasion capabilities [11]. Zheng et al. (2025) introduced FinGPT-Agent, an advanced framework for multimodal research report generation, incorporating task-adaptive optimization and hierarchical attention mechanisms [12]. Weng et al.

(2025) developed SafeGen-X, a comprehensive framework aimed at enhancing security, compliance, and robustness in large language models [13]. Chen et al. (2025) introduced SyntheClean, a method for enhancing large-scale multimodal models through adaptive data synthesis and cleaning [14]. Jiang et al. (2025) developed a knowledge-enhanced multi-task learning model for domain-specific question answering, demonstrating the effectiveness of integrating external knowledge sources [15]. Zhuo et al. (2025) proposed an intelligent-aware Transformer with domain adaptation and contextual reasoning capabilities for question answering tasks [16]. Zhang et al. (2025) explored dynamic attention-guided video generation from text, utilizing multi-scale synthesis and LoRA optimization techniques [17]. Zhao et al. (2025) introduced KET-GPT, a modular framework for precision knowledge updates in pretrained language models [18]. Shih et al. (2025) developed DST-GFN, a dual-stage Transformer network with gated fusion for pairwise user preference prediction in dialogue systems [19]. Li et al. (2025) proposed MLIF-Net, a multimodal fusion approach combining vision transformers and large language models for AI image detection [20]. Chen et al. (2024) introduced Bimcv-r, a landmark dataset for 3D CT text-image retrieval, providing a valuable resource for medical image analysis [21]. Sun et al. (2025) focused on constructing an Automated Machine Learning (AutoML) framework based on large language models, aiming to streamline the machine learning pipeline [22]. Pal et al. (2025) proposed an AI-based credit risk assessment and intelligent matching mechanism in supply chain finance, enhancing financial decision-making processes [23]. These studies collectively contribute to the advancement of AI technologies across various domains, highlighting the diversity and depth of current research efforts.

2. SECURITY ISSUES IN COMPUTER NETWORKS

2.1 Virus invasion

The destructive nature of computer viruses is obvious to all, and viruses affect computers mainly by hackers installing instructions or related program code in computer programs that can destroy computer data. Viruses can make wanton actions on files in the computer, such as copying or deleting, which can have a deep or shallow impact on the normal operation of computer hardware and software, and pose a serious threat to computer data security [2].

2.2 Intrusion of Trojan horses and malicious programs

The intrusion of Trojans and malicious programs has become one of the most common problems in the operation of computer networks at this stage. Often, this is mainly caused by some computer users who are unwittingly or unwitting enough to visit unhealthy websites. These websites will cause the computer to suffer the Trojan horse and the malicious program invasion, has affected the network system the normal and the stable operation directly, also forms the enormous threat to the information security, but also indirectly causes the user privacy to issue the information to leak, when serious also can cause the financial aspect the loss.

2.3 The problem of network openness and resource sharing

Although the rapid development of network technology has brought great convenience to human everyday life, work and learning, However, due to the openness of the Internet and the sharing of information resources, so that some criminals can be more convenient to steal some private information, and even the information out of the sale, in this case of illegal disclosure directly to people's normal life and work carried out. There are also some lawless elements through the sharing of network system to carry out attacks on computer systems, or cause damage to the network behavior [3].

2.4 Risks arising from incorrect user operation

Because some users lack security protection awareness and good operating habits when using computers, they still click on informal websites, knowing the risks, and enter their real personal information into their computers, thereby leaving some criminals with lucrative opportunities. Some customers also credulous others, will own account to others to use, these are likely to lead to their own network information resources under threat.

3. COMPUTER NETWORK AND INFORMATION SECURITY SYSTEM

3.1 System physical environment

At the beginning of the establishment of computer network and information system, it is necessary to use effective system standards for the installation of the computer room. For the physical environment and the specific layout of the facilities, managers need to establish the optimal layout scheme based on the combination of standardization and specification. First, establish computer network rooms on the appropriate floors to avoid hazardous building facilities. Second, install access control system and real-time supervisory control system to improve the effect of computer room management. In addition, it is necessary to install specialized air conditioners in the machine room centrally to ensure that the temperature and humidity are moderate and to reduce safety problems. Third, install effective fire prevention facilities in the computer control center to ensure the integrity of the overall structure while establishing a fire prevention emergency plan [4].

3.2 Operating environment of the system

The key of information system safety is the human element. For the information construction of enterprises and public service units, the first step is to establish a perfect administration system. Advanced technology to support computer network and information security system, according to the specific circumstances of enterprises and public service units, from the perspective of organization, management and technology to protect the security of network system. The running environment of the network information system includes the network communication environment, whether the network communication process can realize the safe transmission of the data, whether the data is complete and whether the data is usable after the transmission.

Places that attach great importance to computer network and information system. The places of routers and central servers are marked with obvious signs, which can include door numbers or other prominent graphic signs such as "The machine room is heavy, please do not enter," and "Fireworks are strictly prohibited."

The network equipment, network communication lines and control devices in the central machine room are backed up accordingly. Backup communication lines are used, as well as backup core switching equipment or servers.

Computer and network information system communication take measures to ensure the integrity of the data, data transmission in the network by adding a certain amount of redundant information, in favor of the network transmission may occur in the data to change or delete the operation.

3.3 Software and data environment of the system

Software is the key component of computer network and information system. When software has bugs, information security will be threatened. Therefore, the following four points need to be achieved in routine software and data environment maintenance: One, in addition to selecting the appropriate operating system, the system needs to be patched; The second is to use a physical and logical isolation to ensure the security of the software and data environment; Third, the computer network and information system data to take protective measures; Fourth, backup management of computer network data is performed to prevent exceptions. The data in the information system can not be recovered.

4. STRATEGY OF ESTABLISHING COMPUTER NETWORK AND INFORMATION SECURITY SYSTEM

4.1 Strengthen the supervision of network access

The supervision of computer network access is the premise to ensure computer network and information security, which can effectively prevent computer users from using computer network resources beyond the permission. Strengthening the regulation of computer network access to prevent the malicious use of computer network resources by illegal users, In addition to basic shared information, other Internet information can be regulated from the source of computer network access by means such as access account verification, access password verification, and access IP address verification. Improve the relevant technical means to realize the security of computer network properties, directory security and other aspects of computer network security.

4.2 Do a good job of network vulnerability protection

Some computer network and information security incidents occur due to the computer network technology itself caused by vulnerabilities, such as the proliferation of computer viruses is due to the computer network technology

can achieve timely sharing of information, it is necessary to do a good job of the corresponding technical vulnerability protection. First, do a good job of detecting and isolating computer network viruses, detect computer network virus in a timely manner, and update network virus killing system in a prompt manner. Second, we should do our best to protect the regional network, and establish and update the firewall system in a timely manner to effectively protect the regional networks.

4.3 Establish and improve the supervision mechanism of computer networks and information security

"No rules, no radius," the lack of appropriate regulatory mechanisms and regulatory policies, computer networks and information security incidents can not be more fundamentally put an end to. In essence, some of the greater impact of computer networks and information security incidents are caused by human factors, and only improve the relevant supervision and management mechanisms, so that perpetrators are afraid to bear the consequences of undermining network security can reduce the recurrence of network security incidents[5].

5. KEY TECHNOLOGY OF COMPUTER NETWORK AND INFORMATION SECURITY SYSTEM

5.1 Password setting technology

Cryptography is one of the technologies commonly used in computer networks to ensure the security of computer information and data. Network communication is safely carried out by encryption algorithm changes of data information, preventing data information from being used by illegal molecules, thus enabling the safe transmission of network information data. By using cryptographic technology, network data information exists in another form, and at the same time adds an extra layer of protection to network data information, so that network data information cannot be easily cracked after it is stolen. In general, cryptography has the following three functions: one can ensure that the data is verified as non-reliable; The second is to ensure that data is not easily stolen; Third, ensure complete validation of data.

5.2 Access control technology

Access control technology is mainly regulated by client-side protection measures, which are composed of network permissions division and human network access control. Under the implementation of this technology, it can effectively restrict the inappropriate behavior of users during network access, reduce the probability of the network being attacked en route to access, and form a certain degree of protection of the network. Moreover, under strict access control technologies and specifications, only authorized users and devices can access and browse it. The more common network access control technology is firewall and VLAN technology.

5.3 Intrusion Detection Technology

Intrusion detection technology has been developed on the basis of consideration of network system security and on the premise that corresponding rules are established. Behaviors in a network are classified as intrusive when they violate set rules, and network intrusion detection techniques can be used over a certain period.

5.4 Anti-virus and firewall technologies

One of the most commonly used virus protection techniques is the installation of antivirus software. There are two forms of antivirus software used on computer networks at present, namely, standalone antivirus software and network antivirus software. The focus of network antivirus software is on the network, and when viruses attack the network system, they can be killed in a timely manner. It is worth noting that antivirus software is not a panacea, and some new viruses can make it ineffective, so it is also necessary to back up important files of the system and encrypt critical information. A firewall is a network protection software that prevents the network from being compromised by the outside world. A computer with firewall software is equivalent to having a more protective wall that allows it to operate in a relatively secure environment.

6. CONCLUSION

In summary, with the deepening of people's understanding of the computer network, it has gone deep into our daily life and work, and information security is not only related to the vital interests of ordinary users, but also related to the security of the country and society. Therefore, in order to enable network technology and technology to serve the general public more securely, provide users with a secure network operation environment and ensure the orderly conduct of the network, and realize the efficient transmission of network data and information, the situation of strengthening computer network security system construction can no longer be allowed.

REFERENCES

[1] Jiang, G., Yang, J., Zhao, S., Chen, H., Zhong, Y., & Gong, C. (2025). Investment Advisory Robotics 2.0: Leveraging Deep Neural Networks for Personalized Financial Guidance. Preprints. https://doi.org/10.20944/preprints202504.1735.v1

[2] 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.

[3] Ding, C.; Wu, C. Self-Supervised Learning for Biomedical Signal Processing: A Systematic Review on ECG and PPG Signals. medRxiv 2024.

[4] D. Restrepo, C. Wu, S.A. Cajas, L.F. Nakayama, L.A. Celi, D.M. López. Multimodal deep learning for low-resource settings: A vector embedding alignment approach for healthcare applications. (2024), 10.1101/2024.06.03.24308401

[5] Xie, Minhui, and Shujian Chen. "InVis: Interactive Neural Visualization System for Human-Centered Data Interpretation." Authorea Preprints (2025).

[6] Xie, Minhui, and Shujian Chen. "CoreViz: Context-Aware Reasoning and Visualization Engine for Business Intelligence Dashboards." Authorea Preprints (2025).

[7] Zhu, Bingxin. "TraceLM: Temporal Root-Cause Analysis with Contextual Embedding Language Models." (2025).

[8] Zhang, Yuhan. "CrossPlatformStack: Enabling High Availability and Safe Deployment for Products Across Meta Services." (2025).

[9] Hu, Xiao. "GenPlayAds: Procedural Playable 3D Ad Creation via Generative Model." (2025).

[10] Wang, Yang, and Kowei Shih. "Hybrid multi-modal recommendation system: Integrating mmoe and xgboost for enhanced personalization and accuracy." 2024 4th International Conference on Artificial Intelligence, Robotics, and Communication (ICAIRC). IEEE, 2024.

[11] Fu, Lei, et al. "Adversarial Prompt Optimization in LLMs: HijackNet's Approach to Robustness and Defense Evasion." 2025 4th International Symposium on Computer Applications and Information Technology (ISCAIT). IEEE, 2025.

[12] Zheng, Haoran, et al. "FinGPT-Agent: An Advanced Framework for Multimodal Research Report Generation with Task-Adaptive Optimization and Hierarchical Attention." (2025).

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.
[21] 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.
[22] Sun, N., Yu, Z., Jiang, N., & Wang, Y. (2025). Construction of Automated Machine Learning (AutoML) Framework Based on Large LanguageModels.
[23] 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.

Author Profile

Chen Guodong Born: 1985.7, Ethnic: Han, Gender: Male, Place of origin: Guangdong, Organization: Guangdong Vocational College of Science and Trade, Title: Intermediate Network Engineer, Education: Undergraduate, Zip Code: 510430, Research interest: Computer Science and Technology.