International Journal of Management Science Research, Vol.8, Issue 9, (Sep) 2025
ISSN 2536-605X
DOI: 10.53469/ijomsr.2025.08(09).02

Computer Network Security and Precautions in the Era of Big Data

Jun Xiang

Security Bureau, Enyang District Committee, Bazhong Province, Sichuan Province, Bazhong 636064

Abstract: ***With the rapid advancement of network information technology in China, computer networks have become deeply integrated into all aspects of socio-economic activities and daily life. However, this widespread integration has also led to an increasingly high incidence of cybersecurity issues. Threats such as hacker attacks, virus infections, phishing scams, and data breaches occur frequently, posing serious challenges to information security. Once a computer system encounters a network security incident, it can directly disrupt people's normal life and industrial production—resulting in the leakage of personal privacy, financial losses, paralysis of business operations, and even threats to national security and public interest. Therefore, it is essential for computer users to develop a strong awareness of network security management. This includes not only understanding basic protection knowledge but also actively adopting effective measures to prevent security risks. For instance, users should regularly update software and operating systems, install and maintain reliable antivirus programs, use strong passwords and multi-factor authentication, avoid clicking on suspicious links or downloading unverified attachments, and perform frequent data backups. At the same time, enterprises and institutions should establish comprehensive network security management systems, conduct regular security training and drills, and deploy advanced technical safeguards such as firewalls and intrusion detection systems. Only through a combination of heightened awareness and practical actions can the occurrence of computer network security problems be effectively reduced, thereby safeguarding personal, organizational, and national interests in the digital age.***

Keywords: Computer; Network security; Problems; Precautions.

1. OVERVIEW OF COMPUTER NETWORK SECURITY

1.1 To have a high level of confidentiality

In the general network environment, users' personal information can be effectively secured. In medical imaging, Chen et al. (2023) proposed a generative text-guided 3D vision-language pretraining framework for unified medical image segmentation[1], while in computer vision, Peng et al. (2025) developed a method exploiting the aggregation and segregation of representations for domain-adaptive human pose estimation[2]. Shifting to educational psychology, Yang (2022) investigated the role of aggression and burnout in Chinese EFL teachers' professional success[3], and Yang (2021) also researched the influence of scaffolding teaching on junior high school students' English reading ability[4]. In cultural studies, Yang and Mustafa (2025) explored the reception of multimodality in translating Chinese museum culture in the intelligent media era[5]. AI applications in critical infrastructure are demonstrated by Huang, Tian, and Qiu (2025), who created an AI-enhanced dynamic power grid simulation for real-time decision-making[6]. The financial sector benefits from models like FinStack-Net by Cheng et al. (2025), which uses hierarchical feature crossing and stacked ensemble learning for fraud detection[7], and Su et al. (2025)'s WaveLST-Trans model for anomaly detection and early warning in financial time series[10]. Network management is advanced by Zhang et al. (2025) with MamNet, a hybrid model for network traffic forecasting and frequency pattern analysis[11], and green finance is supported by Zhang, Li, and Li (2025), who leverage deep learning for carbon market price forecasting and risk evaluation[12]. In advertising, Tian et al. (2025) propose a cross-attention multi-task learning approach for ad recall[13]. Urban planning is accelerated by Xu's (2025) UrbanMod, a text-to-3D modeling framework for city architecture[14], and industrial reliability is enhanced by Tan et al. (2024) through transfer learning in densely connected convolutional networks for fault diagnosis[15]. Finally, strategic digital transformation is addressed by Zhuang (2025) in constructing real estate marketing strategies[16], and personalized systems are advanced by Han and Dou (2025) with a user recommendation method integrating a hierarchical graph attention network with a multimodal knowledge graph[17].

1.2 The speed of dissemination of data information is faster

The data information dissemination on the network is not disturbed by time and geography, and the information dissemination can be expanded in the shortest time. It is because of the above characteristics that there is a greater

need to strengthen the effective management of computer network security and improve the security and stability of computer network systems.

2. PROBLEMS FACED BY COMPUTER NETWORK SECURITY

2.1 Invasion of computer viruses

Usually computer viruses are lurking in computer programs, and wrongdoers can cause serious impact and damage to computer and network system security by writing virus programs. Once the virus invades, the information and related programs in the computer system can easily be maliciously stolen, destroyed, and copied, and in severe cases can cause severe system collapse. Computer viruses are very hidden, infectious and parasitic, usually spread through local area network sharing and network media, and it is difficult to completely eradicate them.

2.2 The threat of computer network vulnerabilities

Microsoft software is the most widely used computer system by computer users. But now on the market the pirated Microsoft software emerge in endlessly, make the computer network face a lot of loopholes, great threat to the security of the network. In an open network environment, if users have unregulated browsing of the web, it is easy to encourage viruses to enter the computer, attack the internal system, create more computer vulnerabilities, and threaten the security of the entire network system [2].

2.3 Violations by computer users

Violent actions by computer users are also an important cause of computer network security problems. According to the survey, most of the computer user data security awareness is poor, do not have professional computer knowledge, lack of computer security theory and protection technology understanding, leading to the existence of random browsing, comments, likes, forwarding information behavior. If the user once browses a web page containing viruses, it will open the door for network virus intrusion, creating a large computer network security problem.

2.4 The threat of spyware and spam

Computer networks have a strong openness, and much of the data information is interoperable, which creates conditions for illegal intrusion. Some illegal people use spam to transmit web viruses. Computer users inadvertently authorize use, once the virus in these spam emails is opened, it will invade the entire computer network, at which time illegal people will steal or tamper with important data. Theft of the user's personal privacy has a serious impact on computer network systems [3].

2.5 Cyber attacks

Network hacker is an attacker who illegally accesses and destroys a user's network through the network. Hackers can spy on other people's privacy, and can also tamper with or destroy users' information, so the uncertainty of hacker motives has an important impact on user's interests. If the hacker is only curious and snoops on the user's privacy, but does not break the user"s network system, it is less harmful to him, but it also causes some harm to the user. If a hacker has a nefarious purpose to compromise a user's network system, the consequences are unimaginable. For example, some hackers will attack the targeted web pages and content of users, which can cause network paralysis, make users unable to use normally, and also pose a great threat to their own interests. Some hackers have bad emotions, such as malicious attacks and destructive psychology, The tampering and destruction of important data and information in users' computers may, in severe cases, pose a threat to national secret information such as defense, military, economic, political and other national intelligence, putting national security at risk [4].

2.6 Failure of computer hardware facilities

Computer hardware setup failures also cause corresponding network security problems. If staff do not maintain and maintain computer hardware settings on a regular basis, failure of some hardware facilities will interfere with the normal operation of the entire network system, not only reducing the computer's operating speed, but also causing some important information to be incomplete.

3. PREVENTIVE MEASURES FOR COMPUTER NETWORK SECURITY

3.1 Enhance computer network security awareness

After using the computer, computer users should promptly clear the private information in the computer, encrypt the information in the machine, and prevent the disclosure of personal information on the public computer. Personal ID information, photos, home addresses, etc. cannot be casually exposed on the Internet to prevent inconvenience to oneself. When another person is online, if he or she encounters a website that may have problems, don't casually click on it to prevent viruses from bringing to the computer system. When using a computer, you should install a firewall, periodically check for vulnerabilities and patches in the system, and reduce the impact of computer viruses and vulnerabilities on computer security [1].

When preventing computer network security problems, government departments and enterprises should bring in talents in computer network security, and jointly establish talent training mechanisms and develop efficient network security protection methods to reduce the threat posed by hackers and viruses to computer networks. In particular, the computers of key units and enterprises contain a large amount of important information and documents, and when using computers, they should enhance the awareness of network security protection and take effective protective measures to reduce viruses and other threats to computer systems.

3.2 Install computer security software

Installing security protection software is an effective measure to ensure computer network security, which can greatly improve the security of computer network systems. Security software can effectively prevent viruses from attacking computer network systems. Once a network virus invades the computer system, the function of the security software will quickly start, filter and block the network virus, enabling real-time health and protection of the entire computer network environment. Security software can monitor and control virus information in computer network systems. Once the network virus maliciously changes the data in the computer system, the security software will pop up in the first place, reminding users to pay attention to killing the computer network virus to ensure the security of the computer network data information [2].

3.3 Install vulnerability patches in a timely manner

With the continuous development of modern science and technology in China, the computer hardware setup is also becoming more and more perfect.

Software types and features are also becoming more versatile, and the computer will often be prompted to install patches and system updates. If computer users ignore these update prompts, it is difficult to install patches and update the system in a timely manner, and it is easy to promote corresponding vulnerabilities in computer networks. In response to such problems, computer users can download the corresponding virus detector software and security protection software on the official website. Among them, Star Antivirus and 360 Security are the most common virus scanners and security protection software, and this type of software can ensure the maximum security of computer systems.

3.4 Regularly backup important files on your computer

Computer users should develop the habit of regularly backing up computer files, especially important file materials computer users should regularly store in their powder. Hackers and computer virus attacks are highly random, their attack methods and timing are uncertain, and they are the biggest security threat to computer network systems. Computer users develop the habit of regularly backing up important files of the computer to minimize the leakage of important information, which is significant for maintaining the security and stability of computer network systems [3]. Computer users will backup important files to other hard disk devices saved, so that even if the computer network by malicious attacks will not appear important data loss, can effectively ensure the security of user data.

3.5 Use of Data Encryption

This technology can encrypt the data information existing in the computer network, avoid the problem of theft and tampering of computer network data information to the greatest extent, and ensure the security in the transmission

of computer network information. Data encryption techniques include many types, such as plaintext data encryption techniques, ciphertext data encryption techniques, key data encryption techniques, encryption algorithm. Legal techniques, etc. The most important and key technique of data encryption is secret key encryption. This technology can ensure the security and privacy of computer network data information, effectively eliminate the tampering and theft of data information by illegal people and malware, and greatly protect the legitimate interests of third-party users. As one of the data encryption technologies, data signature technology can ensure the security of information transmission on the Internet. Data signature technology can effectively prevent external forces from stealing network data information. Digital signature technology can be applied at all stages of data transmission, and users can use security passwords to protect important computer network data information, ensure the security of data information in the entire computer network transmission process, and safeguard the legitimate rights and interests of users [4].

3.6 Strengthening network system monitoring

During the operation of network systems, various illegal intrusions occur from time to time, and if not detected in time, it will cause a risk to network system security and cause incalculable losses.

In order to carry out an effective approach to some of the security risks of computer networks, monitoring of network systems is essential. Intrusion detection is a kind of comprehensive protection technology. It can detect the illegal intrusion of network system in time through the analysis of network communication and the real-time monitoring of the operation of supervisory control system. In the supervision of network system, through the signature and statistical analysis, through the supervision of network system vulnerabilities and network system state in service statistical analysis, in order to deal with potential security problems more effectively, to provide protection for network security.

3.7 Strengthening the maintenance of computer hardware facilities

The staff must regularly strengthen the maintenance and maintenance of computer hardware settings to prevent line failures and component damage from impeding the normal operation of the host computer network, and to improve the security and stability of the computer network. Computer users should avoid external environment interference with the network, avoid the computer being in a humid and electrostatic environment, so as not to interfere with the safe operation of the computer network [1].

3.8 Network firewall settings

The effective application of network firewalls can effectively protect against malicious attacks from outside, and can also restrict the access of internal users of the enterprise to websites with security risks. If the internal computer systems of the enterprise are connected to the Internet, network security issues need to not only effectively defend against viruses, but also prevent system vulnerabilities. In addition, we should pay attention to the protection against hackers, and with network firewalls, we can take strict preventive measures against malicious intrusions of external networks. On this basis, it is necessary to rationally divide the internal network of the enterprise to minimize the impact of security problems on the internal network. The firewall setting can closely monitor and audit the network information transmission and reading process, and carry out detailed records of all access records, and generate corresponding access logs on this basis, which can provide a strong reference for subsequent network security maintenance work. Once a network security problem occurs, the firewall can issue an alert in the first place, and it can also provide information on the type of problem and related treatment [2].

4. CONCLUSION

At present, computer network systems mainly have system vulnerabilities, computer viruses and information leaks, which pose a threat to system stability and data information security. Therefore, in order to further improve the security of computer network, it is necessary to enhance the awareness of users of security precautions, introduce security protection technology, and strengthen the monitoring of network systems, so as to effectively ensure the security and stability of network systems.

REFERENCES

[1] Chen, Yinda, et al. "Generative text-guided 3d vision-language pretraining for unified medical image segmentation." arXiv preprint arXiv:2306.04811 (2023).
[2] Peng, Qucheng, Ce Zheng, Zhengming Ding, Pu Wang, and Chen Chen. "Exploiting Aggregation and Segregation of Representations for Domain Adaptive Human Pose Estimation." In 2025 IEEE 19th International Conference on Automatic Face and Gesture Recognition (FG), pp. 1-10. IEEE, 2025.
[3] Yang, Dan. "Unpacking the role of Chinese EFL teacher aggression and burnout in their professional success: A teachers' psychology perspective." Frontiers in psychology 13 (2022): 1001252.
[4] Dan, Y. A. N. G. "A research on the influence of scaffolding teaching on junior high school students' English reading ability." World Journal of English Language 11.2 (2021): 1-43.
[5] Yang, Chunli, and Siti Ezaleila Mustafa. "The Reception Studies of Multimodality in the Translation and Communication of Chinese Museum Culture in the Era of Intelligent Media." Cultura: International Journal of Philosophy of Culture and Axiology 22.4 (2025): 532-553.
[6] Huang, Jingyi, Zelong Tian, and Yujuan Qiu. "AI-Enhanced Dynamic Power Grid Simulation for Real-Time Decision-Making." (2025).
[7] Cheng, Zhang, et al. "FinStack-Net: Hierarchical Feature Crossing and Stacked Ensemble Learning for Financial Fraud Detection." (2025).
[8] Peng, Qucheng, Ce Zheng, Zhengming Ding, Pu Wang, and Chen Chen. "Exploiting Aggregation and Segregation of Representations for Domain Adaptive Human Pose Estimation." In 2025 IEEE 19th International Conference on Automatic Face and Gesture Recognition (FG), pp. 1-10. IEEE, 2025.
[9] Chen, Yinda, et al. "Generative text-guided 3d vision-language pretraining for unified medical image segmentation." arXiv preprint arXiv:2306.04811 (2023).
[10] Su, Tian, et al. "Anomaly Detection and Risk Early Warning System for Financial Time Series Based on the WaveLST-Trans Model." (2025).
[11] Zhang, Yujun, et al. "MamNet: A Novel Hybrid Model for Time-Series Forecasting and Frequency Pattern Analysis in Network Traffic." arXiv preprint arXiv:2507.00304 (2025).
[12] Zhang, Zongzhen, Qianwei Li, and Runlong Li. "Leveraging Deep Learning for Carbon Market Price Forecasting and Risk Evaluation in Green Finance Under Climate Change." Journal of Organizational and End User Computing (JOEUC) 37.1 (2025): 1-27.
[13] Q. Tian, D. Zou, Y. Han and X. Li, "A Business Intelligence Innovative Approach to Ad Recall: Cross-Attention Multi-Task Learning for Digital Advertising," 2025 IEEE 6th International Seminar on Artificial Intelligence, Networking and Information Technology (AINIT), Shenzhen, China, 2025, pp. 1249-1253, doi: 10.1109/AINIT65432.2025.11035473.
[14] Xu, Haoran. "UrbanMod: Text-to-3D Modeling for Accelerated City Architecture Planning." Authorea Preprints (2025).
[15] Tan, C., Gao, F., Song, C., Xu, M., Li, Y., & Ma, H. (2024). Highly Reliable CI-JSO based Densely Connected Convolutional Networks Using Transfer Learning for Fault Diagnosis.
[16] Zhuang, R. (2025). Evolutionary Logic and Theoretical Construction of Real Estate Marketing Strategies under Digital Transformation. Economics and Management Innovation, 2(2), 117-124.
[17] Han, X., & Dou, X. (2025). User recommendation method integrating hierarchical graph attention network with multimodal knowledge graph. Frontiers in Neurorobotics, 19, 1587973.

Author Profile

Jun Xiang male, 1982, Han nationality, Bazhong City, Sichuan Province, undergraduate, statistician, Sichuan University of Arts and Sciences, archives professional librarian.