HiLL PUBLISHING

Cybersecurity and Information Assurance, 2026, 1(1), 15-19
https://www.hillpublisher.com/Journals/cia/
ISSN Online:

Application of Computer Network Security Technology Based on Big Data Era

Kai Li

Guangxi Zhuang Autonomous Region Information Security Evaluation Center Nanning, Nanning 530201, Guangxi, China.

How to cite this paper: Kai Li. (2026). Application of Computer Network Security Technology Based on Big Data Era. *Cybersecurity and Information Assurance*, 1(1), 15-19.
DOI: 10.26855/cia.2026.06.004

Received: November 22, 2025
Accepted: December 16, 2025
Published: January 23, 2026

***Corresponding author:** Kai Li, Guangxi Zhuang Autonomous Region Information Security Evaluation Center Nanning, Nanning 530201, Guangxi, China.

Abstract

In the era of big data, people's dependence on computer networks continues to increase, and the exchange and sharing of information and data through computer networks has become the norm in all walks of life. However, while the application of computer network brings great convenience to people's work and life, it also inevitably produces corresponding network security problems. How to apply computer network security technology well to ensure network security has become an issue that must be fully paid attention to at this stage. question. This paper takes the computer network security issues in the era of big data as the starting point for analysis, through the research on its characteristics and influencing factors, and on this basis, explores the practical application of computer network security technology, hoping to provide some reference for the development of related work.

Keywords

Big data; Computer; Network security technology; Security issues

Currently, information technology is increasingly permeating all aspects of human life, and the ever-increasing demand for computer network usage has spurred a massive amount of electronic information, becoming an important medium for people to work efficiently. This trend has ushered in the era of big data. At the same time, with the continued popularization of computer networks, computer network security issues have gradually attracted widespread attention. Malicious attacks, hacker intrusions, and computer viruses from the internet constantly threaten computer network information security. Computer network security technology refers to a series of protective measures built around computer data processing systems to prevent attacks and damage from both hardware and software levels. Only by scientifically applying computer network security technology can a sound computer network environment be effectively created, providing strong guarantees for normal production and life. Based on this, this paper conducts an in-depth analysis of typical computer network security issues in the era of big data and analyzes the specific applications of related technologies, hoping to benefit relevant practices.

1. Characteristic Analysis of Computer Network Security Issues in the Big Data Era

In the era of big data, the scale of data generated in people's daily lives and work is unprecedented, and utilizing data resources through computer networks has become commonplace. However, as people's reliance on computer networks increases, corresponding computer network security issues also arise. If these issues are not prevented or addressed with targeted solutions, they can easily have a significant negative impact on normal production and life, and in severe cases, even cause huge economic losses. Therefore, it is necessary to pay full attention to computer network security issues in the era of big data, clarify their characteristics and influencing factors, and thus lay a solid foundation for developing targeted solutions.

Note: The article was originally published in *Advances in International Computer Science*, and this is an authorized translation of it.

1.1 High degree of concealment

Currently, people face massive amounts of information and data every day, and this scale continues to grow, putting significant pressure on computer network data processing. Consequently, many cyberattacks lurk within this environment, making it difficult to identify threats in a timely manner. Furthermore, some cyberattacks have long latency periods, resulting in high levels of concealment of computer network security vulnerabilities. Victims often only discover the security issues after a failure has occurred.

1.2 Significant Harm

Currently, electronic office work has developed significantly across various industries, and the storage and transmission of information through computer networks is very common. This has further amplified the harm caused by computer network attacks. For example, attacks against companies can easily cause huge economic losses, while attacks on personal computers can easily steal personal privacy data and threaten personal information security.

1.3 Strong diffusion properties

In the era of big data, it has become commonplace for people to communicate, exchange, and share information and data through computer networks. Furthermore, with the increasing complexity of economic development, the connections between different industries and between people are becoming more diversified. This creates favorable conditions for the spread of computer network security threats. If security response plans are not perfect, they can easily lead to a chain reaction.

2. Types of Computer Network Security Issues and Their Influencing Factors in the Big Data Era

2.1 Main Types of Computer Network Security Issues in the Big Data Era

The era of big data has promoted the continuous improvement of information data utilization across society, leading to a diversified development of computer network security issues and increasingly complex types of security threats. Specifically, these threats mainly fall into the following categories:

2.1.1 Virus attack

Currently, computer viruses are undoubtedly one of the main factors affecting computer network information security. Unlike other attacks that threaten information security, computer viruses are man-made and spread through channels people encounter daily, such as emails, news, and software. Furthermore, most computer viruses possess self-replicating program code, making them highly stealthy and capable of rapidly infecting a large number of computers in a short period, causing significant damage. Once a computer is infected with a computer virus, it can easily become paralyzed. In more serious cases, the virus can spread to other users' computers under malicious program manipulation, threatening users' secure access to and use of network information. Since the beginning of the new century, computer network information security incidents caused by computer viruses have frequently appeared in the news, causing varying degrees of loss to people's work and lives. This has objectively promoted the development of computer network information security technology. In the era of big data, computer software development technology has made tremendous progress, leading to profound changes in the network environment. Computer viruses are showing an increasingly complex and diversified trend, with frequent mutations. With the current trend of data sharing, once a virus infiltrates a computer system, it can access various data files, thereby threatening computer network security.

2.1.2 Data theft

Currently, data and information have become a crucial production resource, especially for most enterprises. However, driven by profit, some malicious attackers use Trojan programs to attack corporate computer servers, stealing corporate data resources for profit, which can easily lead to significant economic losses for enterprises. Furthermore, attacks targeting personal computer networks aim to steal personal information, and information leaks can also have varying degrees of impact on users. Both of these impacts hinder the harmonious and stable operation of society and are detrimental to achieving social benefits.

2.1.3 DDoS attack

The specific implementation process of a DDoS attack is as follows: By rapidly generating a massive number of concurrent processes in a short period of time, these processes occupy a large amount of normal network communication resources, making it difficult for computer servers to carry out data processing and other services. This, in turn, greatly increases the response time for user logic business requests, ultimately causing abnormal operation of the computer server.

2.1.4 Software vulnerabilities

The increasing complexity of social development has led to the increasingly specialized functions of computers, thereby driving the vigorous development of various software applications. Currently, software providing corresponding services is constantly emerging, and its types and functions are continuously expanding. While this has significantly facilitated people's daily work and life, it has also brought new network information security problems. Software developers often set certain access permissions during development to facilitate future updates and upgrades. However, if these permission settings are cracked by hackers, they can maliciously modify them to obtain relevant users' personal information data, and even more seriously, the core data of the software may be stolen.

2.2 Factors Influencing Computer Network Security in the Big Data Era

2.2.1 Internal influencing factors

The main internal factors affecting computer network security are: First, vulnerabilities in the TCL protocol. Current computer networks are generally built on the TCL protocol. While the TCL protocol's design could only support a limited scale of interconnection in the past, the number of computers needing to share communication has surged in the era of big data. This has highlighted the imperfections of the TCL protocol, and its vulnerabilities provide the basis for network attacks. Second, vulnerabilities inherent in the computer system itself. Currently, the development and application of computer software systems are developing rapidly, with increasingly faster updates and iterations. This also brings corresponding challenges to computer network security. Insufficient attention to security factors in some software designs may create hidden dangers for network security.

2.2.2 External influencing factors

In the era of big data, external factors affecting computer network security can be divided into two types: First, the threat of attacks and intrusions from hackers. By exploiting vulnerabilities in computer networks, hackers can enter user systems to steal or destroy data. Second, the non-standard use of personal computer networks. Many computer users do not have a strong awareness of security precautions, resulting in varying degrees of non-standard behavior when operating computers or ignoring relevant security prompts, leaving significant hidden dangers for computer security defense.

3. An Exploration of the Application of Computer Network Security Technology in the Big Data Era

3.1 Data Encryption Technology

Among various computer network security defense technologies, data encryption technology is undoubtedly of paramount importance. This technology primarily encrypts transmitted information to effectively prevent data loss and tampering. Generally speaking, data encryption technology can be divided into two types: symmetric encryption and asymmetric encryption. The former is simpler and more convenient to use, employing cryptographic techniques to encrypt information and thus hide it, effectively protecting information security. The latter often involves more advanced technical applications, and the encryption and decryption processes are more complex, resulting in slower speeds. Furthermore, asymmetric encryption technology also consumes more system resources of the computer network.

3.2 Authentication Technology

Authentication technology primarily addresses network security issues related to the forgery and tampering of information parameters. It verifies parameters during information transmission, specifically employing identity authentication and message authentication technologies. Identity authentication technology leverages the principles and

methods of password and biometric authentication to verify the identity of computer system users. Message authentication technology targets the specific content of the message, as well as its source and destination, message sequence number, and operation time. Taking the practical application of message authentication technology as an example, when transmitting information over a computer network, the sender can add an authentication code, encrypt necessary content, and then send it to the receiver. The receiver decrypts or authenticates the received content using a predefined algorithm to obtain the corresponding authentication code. By comparing this code with the authentication code added by the sender, the receiver can determine the security and integrity of the information data. If the two codes do not match, the receiver rejects the information data.

3.3 Firewall Technology

Firewall technology involves both computer hardware and software. Deployed at the network boundary, it rapidly activates when a network security threat is detected during information communication and sharing between the internal and external networks. It plays a crucial role in security filtering and isolation, and its application is significant for effectively controlling the spread of computer network faults. Specifically, the key to firewall technology lies in access control. By assessing the security of information access and transmission, it promptly blocks illegal activities. For example, when hackers illegally access the computer network, the firewall can record this activity and compare it with other network access records to determine if it deviates from normal access rules, issuing an alert and restricting access. In the era of big data, firewall technology has become increasingly sophisticated and mature. Upgrading computers to higher levels of protection ensures a stable network environment and prevents economic losses due to network security issues.

3.4 Intrusion Detection Technology

Intrusion detection technology refers to the periodic detection of network applications and data packets by computer software to identify and handle malicious use of computer network resources. If a virus intrusion is detected in the computer system, the detection system will promptly alert the user, who can then perform a scan and removal based on the alert. In addition, if the computer network is under malicious attack by hackers, the detection system will quickly intercept the attack by cutting off the connection, thereby ensuring the safe use of the computer network. At present, the application of intrusion detection technology in practice mainly involves monitoring and analyzing computer network user data. Based on this, by clarifying the structural characteristics and shortcomings of the computer network system, a comprehensive understanding of the computer network security status can be achieved, and a corresponding computer system security assessment report can be generated (Tian & Shi, 2016; Duan, 2015; Xiong, 2015), thus providing a detailed and reliable basis for the formulation of targeted security strategies.

3.5 Development Trends of Computer Network Security Technology in the Big Data Era

The era of big data has brought a series of challenges to the application of traditional computer network security technologies. Network security threats are becoming increasingly complex, attack methods are becoming more covert, and the severity of harm is continuously expanding. Continuing with traditional methods is clearly not very adaptable. Therefore, it is necessary to introduce more advanced data defense and data identification technologies, such as artificial intelligence, neural networks, and genetic algorithms, to promote the intelligence of computer network security defense systems. In addition, the popularization of computer network security technology applications will also become a major development trend, effectively improving the computer security defense technology application level of every computer user, thereby eliminating some unnecessary negative impacts of network security threats on users' production and lives.

4. Conclusion

In the era of big data, it has become increasingly common for people to rely on computer networks for work and life. This increasing dependence makes computer network security technology increasingly important, which is crucial for maintaining the normal operation of computer networks and fully leveraging their benefits to production and daily life (Liu, 2016; Gao, 2015; Yang, 2017). Therefore, it is necessary to pay full attention to computer network security issues, and based on a comprehensive understanding of their characteristics and influencing factors, select targeted security protection technologies to safeguard the normal use of computer networks. Of course, the application of

computer network security technology still needs continuous improvement in practice, especially in terms of technological updates and iterations, to effectively enhance users' computer network experience, create a good computer network environment, and promote economic development.

References

Duan, L. (2015). Computer network security prevention measures under the background of big data. *Business*, (48), 1.

Gao, L. (2015). Exploring Computer Network Security and Prevention Measures in the Big Data Era. *Talent and Wisdom*, (23), 2.

Liu, Y. (2016). Research on Computer Network Security Prevention in the Big Data Era. *Digital Communications World*, (010), 169.

Tian, Y., & Shi, Q. (2016). A Preliminary Discussion on Computer Network Security and Preventive Measures in the Big Data Era. *Computer Programming Skills and Maintenance*, (10), 3.

Xiong, H. (2015). Computer network security prevention measures under the background of big data. *Computer CD Software and Applications*, *18*(2), 2.

Yang, J. (2017). A brief analysis of computer network security prevention in the era of big data. *Communications World*, (22), 2.