HiLL PUBLISHING

Cybersecurity and Information Assurance, 2026, 1(1), 20-23
https://www.hillpublisher.com/Journals/cia/
ISSN Online:

Research on the Application Value of Data Encryption Technology in Computer Network Security

Hui Si

Suzhou Polytechnic Institute of Agriculture, Suzhou 215008, Jiangsu, China.

How to cite this paper: Hui Si. (2026). Research on the Application Value of Data Encryption Technology in Computer Network Security. *Cybersecurity and Information Assurance*, 1(1), 20-23.
DOI: 10.26855/cia.2026.06.005

Received: November 22, 2025
Accepted: December 16, 2025
Published: January 27, 2026

***Corresponding author:** Hui Si, Suzhou Polytechnic Institute of Agriculture, Suzhou 215008, Jiangsu, China.

Abstract

Because the application of computer network technology has become more and more popular, and the threat of computer network security to human daily life and working environment is also growing, in order to more effectively maintain the security of computer network, we must pay attention to the scientific use of corresponding data encryption technology. There are many kinds of data encryption technologies. Only by selecting appropriate technical means and closely connecting with computer security issues can we effectively help to improve the overall security level of computer networks. This paper mainly introduces the problem of computer system security and its application value to data encryption technology from the theoretical level, and discusses the types of data encryption technology and its application in computer system security in detail, hoping to play a positive role in the practical application of technology by virtue of the application research of data encryption technology.

Keywords

Computer; Network

Introduction

To effectively improve the level of computer network security, it is essential to fully leverage the resource advantages of computer encryption technology. Only by closely linking encryption technology with the overall level of computer security and fully utilizing its advantages can the highest level of network security be achieved. Currently, there are increasingly more factors hindering computer network security. Therefore, to truly and effectively improve the quality of computer network security, we must start with the fundamental idea of technological innovation and pay attention to fully utilizing the application functions of computer encryption technology, thus laying the foundation for effective computer security protection.

1. Application of Computer System Security and Data Encryption Technology

Data theft is a significant security risk in computer networks, primarily manifested in the theft of data. Data management and protection are crucial aspects of computer network engineering and essential prerequisites for the application of various advanced technologies within computer networks. However, some criminals steal internet users' data through illegal means to achieve their illicit purposes, such as stealing online banking passwords, causing substantial losses to users. Data theft results in significant economic losses for individuals, companies, and enterprises alike.

Computer virus issues. Many factors contribute to computer security problems, but computer viruses are a

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

prominent one. To more effectively maintain computer network security, attention must be paid to protecting against computer viruses, thus laying a solid foundation for effective network security management. Only by perfecting these fundamental aspects can a crucial cornerstone for computer network security be truly established. The intrusive nature of computer viruses can cause considerable damage to computer networks. Due to their high degree of stealth and powerful attacks, computer viruses pose a significant threat to computer networks. Therefore, a direct attack on a computer or network system can lead to anything from information system loss to the complete system crash.

The issue of hacker attacks. In the real-world application of the internet, security threats also manifest at the level of computer hacker attacks. Hacking methods can be categorized as proactive or reactive. Proactive intrusion generally refers to targeted or planned intrusions, with the aim of stealing or threatening user information, causing significant economic losses to users. Reactive intrusion, on the other hand, typically involves obtaining data through data cracking, while the user's computer continues to function normally; this method generally poses less of a security risk. However, the harm that hacker intrusion methods cause to computer system security is considerable. Therefore, in order to effectively improve internet security, this security issue must be addressed and effectively managed.

System vulnerabilities are a significant issue. During the use of computer networks, inherent flaws in the network system itself can reduce network security and significantly improve overall network efficiency. Therefore, careful attention must be paid to the management and repair of network system vulnerabilities. Computer defects can also interfere with the security and stability of the network system. System vulnerabilities can lead to a decline in the computer's information reception function, directly interfering with normal computer use and reducing the user experience. Therefore, resolving this network security issue becomes even more crucial.

2. Types of Data Encryption Technologies and Their Applications in Computer Security

2.1 Types of Data Encryption Technologies

In the process of protecting computer security, the use of data encryption technology enhances the overall security of information data in computer systems. Different encryption technologies should be selected to fully leverage the advantages of information technology and effectively contribute to internet security. Data encryption technologies generally fall into two categories: symmetric encryption and asymmetric cryptography. The following will explain the types of data encryption technologies. Asymmetric encryption technology is a crucial type of data encryption. During the encryption process, the parties transmitting and receiving information can use various keys and methods to encrypt and decode the information. There is a choice between public and private keys, and the parties in data communication do not need to exchange keys in advance, greatly reducing the relative risk. The confidentiality and information security of various statistical information are thus guaranteed. Symmetric cryptography is also a critical part of data security encryption. This type of encryption method uses shared-key encryption. The party transmitting data must use the same key as the party receiving the data to encrypt and decode the data. The use of this technology also requires both parties to ensure the security of the key during information transmission, ensuring information security without leaking the encrypted content. This will have a positive impact on improving the overall security level of data.

2.2 Application of Data Encryption Technology in Networks

Software encryption is a crucial computer encryption technology. It leverages software functionality to enhance computer security, thereby improving the overall security performance of the computer system and preventing unauthorized viruses from infiltrating and posing security threats. With the use of various antivirus and disease detection tools, computer users are protected by the overall defense capabilities of the computer system, improving the security of information used within the system. The main function of software encryption is to protect the information and internal data of antivirus programs and anti-virus software. Cloud computing platforms, with their high stability, can effectively protect the security of computer and internet information systems and can also perform security scans on system information, thus improving the overall security and stability of the computer system.

Key encryption. To ensure computer security, careful attention must be paid to the use of key encryption technology, as it is crucial for safeguarding computer security. The use of key encryption technology can also promote targeted data processing, thereby effectively enhancing the overall effectiveness of the password. Key encryption technology includes private and public encryption methods. For example, private encryption establishes a private connection between the data and the access party, and a unified key is distributed. Information about the data can

also be obtained using this unified key, ensuring information security. Public key encryption, on the other hand, is a method of securing the data access key through a separate password. If the data access party obtains the data key through a separate password, it will help ensure information security. Public encryption is more common and generally provides greater protection than private encryption. When maintaining the security of computer data, it is important to choose the correct encryption method.

Node information encryption. When maintaining computer system security, it is crucial to fully emphasize and leverage the confidentiality function of node information. The scientific application of internet node information encryption can further enhance data confidentiality, thereby ensuring the security of network information transmission between computer systems. Since data information passes through numerous internet nodes before reaching the target algorithm, and the presence of viruses or malicious intrusions on the internet severely compromises data security, the scientific application of node information encryption can significantly improve the ability to protect data security. Each node can decrypt or securely encrypt data, effectively preventing targeted attacks.

3. Strategies for Applying Data Encryption Technology in Computer Network Security

3.1 Applications in Computer Software

In the process of computer operation, if the hardware provides the support, the application software will implement it. The hardware determines the characteristics of the computer operating system, while the application software determines the characteristics of the operating system. This means that users mainly rely on system software to manage data in computer information systems. This makes computer technology and software a key target for hackers. First, user confidentiality is crucial. Only with a valid key in front of legitimate users can access and copy data with certain permissions. Second, data encryption systems can be used to develop necessary capabilities when software is attacked. Encryption technology allows for early detection and prevention of viruses, and antivirus systems can also remove these viruses, thus achieving absolute security protection for the entire computer system.

3.2 Important Applications in E-commerce

E-commerce has achieved historic progress thanks to the internet. It has redefined customer value, making customers crucial nodes in the global supply chain. In today's increasingly prosperous e-commerce sector in my country, information security is no longer just a matter of personal or corporate interests, but also a matter of national economic and social development. Ensuring the confidentiality of data information can guarantee the smooth operation of e-commerce. Currently, data encryption technologies used in all aspects of secure information network exchange have become the primary means of protecting the rights and interests of information stakeholders.

3.3 Applications in Local Area Networks

The ultimate value of technological development lies in serving the development of applications. Currently, data encryption technology is also evolving with the continuous changes in user application formats, developing increasingly suitable information technologies to serve application development. At the company level, many medium and large companies have proactively established local area networks (LANs) to facilitate centralized management of small and medium-sized enterprises and to enable faster and more convenient content management such as video conferencing, data processing, and uploading. While LANs have improved enterprise management to some extent, they have also significantly posed a threat to important data in company operations. Therefore, the application of data encryption technology within LANs becomes crucial. The effective use of data encryption technology within LANs can provide better protection for computer data security, creating the necessary foundation for the healthy development of the company.

Conclusion

In conclusion, to ensure computer security, attention must be paid to the use of data encryption methods. By selecting various types of data encryption methods, a robust foundation for computer system security management can be established. The data encryption techniques mentioned above, such as software encryption or attribute-based encryption, can all lay a solid foundation for maintaining the security of modern computers.

References

Cheng, H. Y. (2021). Application of data encryption technology in computer network security. *Software*, *42*(11), 62-64.

Dong, Y. (2022). Analysis of the application value of data encryption technology in computer network security. *Data Communication World*, (05), 112-114.

Guo, C. (2021). A brief analysis of the application of data encryption technology in computer network information security. *China New Communications*, *23*(21), 131-133.

He, L. M. (2021). Application of data encryption technology in computer network security. *Computer Programming Skills and Maintenance*, (10), 155-157.

Li, Y. (2020). Research on the application value of data encryption technology in computer network security. *Information and Computer (Theoretical Edition)*, *32*(06), 187-189.

Yu, S. K. (2020). Application of data encryption technology in computer network communication security. *Network Security Technology and Application*, (09), 24-25.

Zhao, Y. (2018). Research on the application value of data encryption technology in computer network security. *Network Security Technology and Application*, (12), 32-33.

Zhou, P. (2021). The application value of data encryption technology in computer network security. *Software*, *42*(10), 168-170.