Cryptographic Mechanisms for Network Information Security

Ming Xiaofan Liu

Qingdao University of Technology, Qingdao, Shandong 266000

Abstract: ***With the advent of the information age, computer networks have become increasingly pervasive, and computer and network technologies are now widely applied across various industries. Consequently, ensuring the security of computer network information has emerged as a prominent topic of discussion in contemporary society. Issues such as password leakage, account security vulnerabilities, and the privacy of browsing information have caused considerable difficulties for users due to inadequate information security protection measures. To safeguard the integrity and confidentiality of information stored within computer networks, an increasing number of network hosts are adopting data encryption technology—a widely used information security technique that primarily enhances the security level of computer network information through data encryption. This article provides a detailed introduction to the specific applications of data encryption technology in protecting computer network security information across domains such as software systems, business operations, and network data. It also discusses important considerations during the application process, analyzing these applications with the goal of enhancing the effectiveness of data encryption technology in information security.***

Keywords: Data encryption technology; Computer; Network information security; Practical application.

1. INTRODUCTION

In recent years, network technology has developed rapidly, with access to every village, 5G networks, and 4K high-definition movies. The network infrastructure of our country is constantly improving, the network technology is constantly improving, the network communication function has been closely linked with people, the computer network has become the main component of society, people's food and clothing are inseparable from it, and the Internet has become an indispensable part of our lives. Nowadays, computer networks are used in various industries, such as information-based education, where schools use multimedia technology to teach and cultivate students' active learning abilities; You don't have to go to the hospital to queue up for medical treatment. You can make an appointment online first. You can also open your browser and enter your symptoms to pay 1 yuan, and a renowned doctor will help you diagnose. Medications can also be delivered directly to your doorstep; And now Alipay's online payment, taking the subway bus only needs to scan the QR code of the mobile phone; Internet and agriculture are also very trendy applications. They can save more time and labor by replacing the original manpower to manufacture electronic equipment. Computer network has become the most important tool for people to use in life, study and work.

But while enjoying the efficiency and convenience that computers have created for people, we have also discovered that there are still many threats to people's security information protection. For example, a series of issues such as telecommunications fraud, bank card theft, computer virus intrusion, data privacy recovery, illegal hacking, and computer system vulnerabilities are enough to make us vigilant when using computers. In order to ensure the safety of users and the sustainable and harmonious development of society, we must enhance the information security capabilities of computers through data encryption technology, resist more illegal human operations that may cause property losses, and safeguard the information security of network entities. Recent advances in deep learning have significantly impacted computer vision applications.

Zheng et al. [1] proposed DiffMesh, a motion-aware diffusion framework for human mesh recovery from videos, in 2025. Pinyoanuntapong et al. [2] introduced Gaitsada, a self-aligned domain adaptation method for mmWave gait recognition, in 2023. Peng et al. [3] developed a 3D vision-language Gaussian splatting approach for novel view synthesis and scene understanding in 2025. Zhao, Zhang, and Hu [4] designed a smart warehouse track identification method based on Res2Net-YOLACT+HSV in 2023. Shan, Xu, Xia, and Lin [5] rethought wine tasting for Chinese consumers using a service design approach enhanced by multimodal personalization in 2025. Wang et al. [6] proposed QA-ReID, a quality-aware query-adaptive convolution leveraging fused global and structural cues for clothes-changing person re-identification, in 2026. Narouei et al. [7] examined the effects of germicidal far-UVC on ozone and particulate matter in a conference room in 2025. Xiao et al. [8] designed an

ultrasmall Fe_3O_4-decorated polydopamine hybrid nanozyme for intensive wound disinfection in 2022. Ge and Wu [9] conducted an empirical study on the adoption of ChatGPT for bug fixing among professional developers in 2023. Li et al. [10] introduced MFT, a memory-aware fine-tuning of SAM2 for efficient long-sequence video object segmentation, in 2026. Yan et al. [11] presented PRISM, a pipeline for root-cause investigation via specialized multi-agents, in 2026. Finally, Hu, Zhang, and Sun [12] unveiled new directions in text sentiment analysis using multiscale deep neural networks in 2024.

2. DATA ENCRYPTION TECHNOLOGY

2.1 What is data encryption technology

Data encryption technology is a computer technology that protects network data. It mainly uses encryption methods such as encryption keys or functions to convert text obtained in computer networks into meaningless ciphertext for propagation. When the receiving party sees the ciphertext content, they use decryption to restore the ciphertext to its original form. The development of data encryption technology is to ensure the security of information dissemination during the use of the network.

2.2 Classification of Data Encryption Technologies

(1) Node encryption

In the process of transmitting information, a special encryption site is used by the data transmitter to transmit data. There is a distance between the transmitting and receiving parties, and a node is designed for each distance. The amount of information transmitted in each distance is different, and real-time encryption is usually performed at the intermediate node with the largest amount of transmitted information.

(2) Link encryption

The principle of node decryption is similar to that of encrypting two adjacent nodes, as the encryption effect may vary depending on the distance range and location of each transmission. This encryption form can effectively improve the security of data during use. By using the method of transmitting ciphertext and server-side plaintext during data transmission, it can be hidden at the beginning and end. Because it is always in an encrypted state, it can also effectively resist virus intrusion, thereby reducing the danger index of computer operation.

(3) Double mutual encryption

Generally, the sender's port encrypts the data and then transports it to the receiver's port for decryption. Double encryption is end-to-end encryption, where encryption and decryption are performed simultaneously at the sender's and receiver's ports. This ensures that the information is fully encrypted during the transmission process, making the operation simple and the security of the information higher. It is also one of the most commonly used encryption methods currently.

2.3 Characteristics of Data Encryption Technology

(1) Data processing

This is the most essential feature, which is the processing of data. The data information received in computer networks that can be recognized by everyone is processed through specific algorithms, and then disseminated to only a few people who can decrypt and identify the original content using specific keys.

(2) Algorithm complexity

The encryption technology of conversion is a process of processing plaintext information, which requires precise algorithms for encryption. Different algorithms have different categories. Different types of algorithms correspond to different calculation methods, resulting in vastly different outcomes. The commonly used encryption calculation methods for computers nowadays include permutation table algorithm, cyclic displacement, replacement table algorithm, cyclic redundancy check algorithm, etc. The calculation method is relatively complex.

(3) Reduce the number of users in contact

Data confidentiality technology is achieved through double encryption transmission. The data sender encrypts the data information using a specific algorithm and then provides the key to the data receiver. After receiving the ciphertext, the data receiver decrypts it using the obtained key to obtain the ciphertext information. Specific keys correspond to specific ciphertexts, just like a key corresponds to a lock. Because data encryption involves the mutual transmission of specific keys between both parties, it can greatly reduce contact with other users during the transmission process, and greatly enhance information security.

3. PROBLEMS IN COMPUTER NETWORK INFORMATION SECURITY

After understanding the operating principles and characteristics of data encryption technology, let's take a look at what problems exist in computer network information security, in order to improve the effectiveness of later technology applications and make better breakthroughs.

3.1 System has vulnerabilities

There are certain loopholes in the use of computers. For example, when we browse a web page, we will have a history of the web page or browsing traces. Network hackers can invade the computing system through the Internet traces left by your computer network operations, find the system loopholes, and then take the opportunity to plant viruses, so that we can control the operating mode of the computer system and steal the internal stored information for our own use. Therefore, when using the Internet at ordinary times, we should be careful to click on any link, do not easily download unknown software or browse unknown websites, and at the same time, we should install anti-virus software to clean up and timely update protection.

3.2 Hacker Invasion

Hackers are also a great hidden danger in the process of computer security use. Hackers have become a profession that everyone criticizes in today's society. They are usually advanced computing level technicians who infiltrate computer systems to steal user information for their own benefit. A few days ago, there were reports in the news that a man caused dissatisfaction due to flight delays and hacked into the airline's network system, resulting in a few minutes of network paralysis and extremely heavy losses. This is an illegal and criminal act. So the existence of professional hackers poses a great threat to people's economy, security, and privacy.

3.3 Unknown virus

Computers often encounter unknown viruses during use, just like how people occasionally suffer from headaches, headaches, colds, and fever, which cannot be completely avoided. Common viruses include Trojan and Panda viruses. Once these viruses appear, they can damage the computer's operating system, causing system crashes and resulting in many encrypted files being destroyed or data information being leaked. Even if there is a built-in firewall or antivirus software on the computer, it cannot prevent the invasion of viruses.

3.4 Improper management

The lack of standardized network management is also a major issue in current computer network information security. Nowadays, when you open a webpage, various advertisements and junk information are everywhere. If you accidentally click on them, you will get infected with viruses. There are also many websites that are gambling pornography, which can seriously lead to many users being deceived, causing physical and mental damage to their property. Mild cases include computer black screens, system crashes, and data loss. This not only threatens the privacy and security of users, but also occupies a large amount of public resources, so computer network information managers need to increase their management efforts in network information security.

4. THE SPECIFIC APPLICATION OF DATA ENCRYPTION TECHNOLOGY IN ENSURING NETWORK INFORMATION SECURITY

At present, data encryption technology presents a diversified state of ensuring network information security in different application methods and scenarios. It is not singular but diverse. We can adopt different encryption methods for data processing according to different network types and application links to ensure the security of network information. What are the specific applications of data encryption technology in computer network information security?

4.1 Software Encryption

The main application of software encryption is our common computer antivirus software, such as 360 Security Cleanup Master, Lu Master, and Computer Manager. This type of software can not only remove viruses that appear in computer networks, but also prevent the installation of unknown programs and effectively protect the file information stored on the computer. In order to prevent virus invasion from causing antivirus software to fail and reduce the security of stored file data information, we usually test the security and effectiveness of antivirus software in advance, determine the security of protected information, and then encrypt the data.

4.2 System Encryption

In order to make it easier for users to operate computers, nowadays computers generally use Windows NT or Unix systems. The security performance of these systems is generally at the lowest C1 and C2 levels, because the storage function of the system itself is not strong, which can easily cause the leakage of user data information or the tampering of stored information during the operation process. Data encryption technology can set permissions for the operating system, which changes the system's operating instructions, and technically encrypts the database that stores information. Users need to obtain corresponding access permissions before accessing the system. This not only improves the security of the entire operating system, but also reduces the risk of system intrusion.

4.3 Network Encryption

Virtual private network is a communication method that can connect large enterprises or groups through reliable message transmission through server software. Traditional single keys are easily cracked, causing data file leakage. Therefore, many enterprises generally build local area networks to ensure information security by setting up network firewalls, encrypting the local area networks, and encrypting node ports to ensure the security of data transmission. Generally, enterprise routers have encryption functions for data encryption technology in the local area network. They encrypt all files, information, and data in real-time, and the receiving router decrypts and converts them into the original files, reducing the number of people in contact while avoiding the risk of file leakage and building a more secure network environment. At the same time, data encryption technology in the local area network can achieve security protection in different areas of the network, ensuring the smooth implementation of various enterprise businesses.

4.4 Data Encryption

The main application of data encryption technology in data confidentiality is network database encryption. Computer network databases are places where information is stored centrally. Due to the large amount of information, their security performance must also be at the highest level. In order to ensure the security of various information data in the database, in addition to encrypting the network database, it is also necessary to test and prevent the security of user data during computer use. When users perform computer operations, their data is stored, and encrypted network databases can analyze and detect this data. If there are any security risks, they will be automatically displayed to the user on the operating end, and the user will receive a reminder from the computer before taking security measures.

4.5 Identity authentication

In the past few decades, the ID card has been the unique identifier for everyone's identity recognition, with extremely strong attributes. In today's digital age, there are many authentication methods to confirm a user's identity. Identity authentication is currently one of the most widely used data encryption technologies, and there are two main categories of identity authentication technology: identity authentication and network identity authentication. There are differences and similarities between the two.

4.6 Network Identity Authentication

Users need to provide their identity information for authentication when logging into the network in order to obtain the corresponding access permissions. There are three modes: dynamic password, USBKey, and OCL mode.

(1) Dynamic password

Dynamic passwords have high security and are widely used, mainly relying on the time difference between servers and clients for verification. This can be seen everywhere in daily life, such as binding bank cards, registering apps, setting passwords, and so on. Only dynamic verification codes include voice dynamic codes and digital dynamic codes. As long as the client and server passwords match, the verification login can be completed successfully.

(2) OCL mode

OCL is an object constraint language that applies constraints to specified model elements. It is a new type of identity authentication technology solution mainly used for secure system operation authentication of personal accounts in online banking, with many verification modes. For example, using dynamic passwords and manual passwords, or combining mobile verification codes and passwords, maximizes the security of traders' funds.

(3) USBKey

USBKey is a hardware device with a USB interface that has storage space and a built-in smart chip. The user private key embedded in USBKey is locked using data confidentiality technology, and the encryption lock is mainly used for software cracking and copying to prevent software piracy, with a high level of security.

4.7 Identity authentication

(1) Utilize information known to users

Because we provide our identity information to the system during computer operations, our identity information is present in network data. For example, when logging into QQ, Taobao, or WeChat, you will be asked which of the following is not your WeChat friend, or to set a security question. Only when you answer the question correctly can you complete the verification.

(2) Utilize what users possess

Due to the storage of information data, computer networks have already mastered our data. For example, when logging into various apps, you need a dynamic verification code to receive information. At the same time, you can drag the icon to a designated location for verification, and select objects on the screen in order. Moreover, the program QR code is also a unique item owned by users.

(3) Utilize identity features

This is easy to explain. Nowadays, mobile phones use facial recognition or fingerprint recognition, and data confidentiality technology is also used in facial recognition technology, fingerprint recognition technology, and DNA testing technology, all of which utilize the unique identity characteristics of users for detection.

5. ISSUES AND SOLUTIONS TO BE NOTED IN THE USE OF DATA ENCRYPTION TECHNOLOGY

5.1 Insufficient user security awareness

In the era of efficient development of the internet, many people do not have sufficient knowledge about the use of computers and only understand some basic operations. Due to the limited knowledge reserve, it is also difficult to discover the hidden dangers of computer information security, resulting in security threats to their own data information. So we should provide training on network knowledge and security in schools, and at the same time, carry out more promotional activities and lectures on telecommunications network fraud in communities and enterprises. We warn everyone not to easily click on unfamiliar links to guard against Trojan viruses, and to use computer networks with high security performance as much as possible. At the same time, when downloading apps, pay attention to security reminders. When using secure payments, be sure to pay attention to dynamic passwords

and not leak them. At the same time, when applying for user permissions for unknown software web pages, be sure to read carefully.

5.2 Use without scientific norms

There is still a lot of room for development in data encryption technology, and it is not omnipotent. It cannot solve all the hidden dangers that threaten computer network information security. Therefore, when choosing data encryption technology, users must find professional personnel to purchase it through legitimate channels and use it scientifically and standardly. Therefore, in order to address the issue of scientific application, users need to choose safe and reliable antivirus software when using computers, and regularly disinfect the antivirus software to ensure that the computer can be quickly identified by antivirus software when security risks such as viruses, vulnerabilities, and hacker intrusions occur during use.

6. CONCLUSION

In this article, we learned about the specific application of data encryption technology in computer network information security, and also discovered the problems that exist in its use. As an important means of ensuring network information security, data encryption technology deserves the attention of people from all walks of life. The use of data encryption technology not only purifies the environment of complete network information, but also greatly improves the efficiency of computer use, enabling efficient development of enterprise economy and making people's lives more convenient, achieving global and village connectivity, and bringing people closer together. Data encryption technology ensures the rapid development of technology. Nowadays, facial recognition, fingerprint recognition, and more high-tech have entered people's lives. We can shop on our phones, make payments on our phones, use QR codes for transportation, swipe our ID cards to take high-speed trains, use apps for medical treatment, use 5G communication to play videos online, and use autonomous driving in cars. The internet has made our lives more colorful. So we need to scientifically choose to use data confidentiality technology to ensure our own network information security.

REFERENCES

[1] Zheng, Ce, et al. "Diffmesh: A motion-aware diffusion framework for human mesh recovery from videos." 2025 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV). IEEE, 2025.
[2] Pinyoanuntapong, Ekkasit, et al. "Gaitsada: Self-aligned domain adaptation for mmwave gait recognition." 2023 IEEE 20th International Conference on Mobile Ad Hoc and Smart Systems (MASS). IEEE, 2023.
[3] Peng, Q., Planche, B., Gao, Z., Zheng, M., Choudhuri, A., Chen, T., Chen, C. and Wu, Z., 3D Vision-Language Gaussian Splatting. In The Thirteenth International Conference on Learning Representations.
[4] Zhao, X., Zhang, L., & Hu, Z. (2023). Smart warehouse track identification based on Res2Net-YOLACT+HSV. Innovation & Technology Advances, 1(1), 7–11. https://doi.org/10.61187/ita.v1i1.2
[5] Shan, X., Xu, Y., Xia, T., & Lin, Y. S. (2025, October). Rethinking Wine Tasting for Chinese Consumers: A Service Design Approach Enhanced by Multimodal Personalization. In 2025 International Conference on Content-Based Multimedia Indexing (CBMI) (pp. 1-5). IEEE.
[6] Wang, Y., Jiang, K., Zhang, T., Tian, K., & Jiang, G. (2026). QA-ReID: Quality-Aware Query-Adaptive Convolution Leveraging Fused Global and Structural Cues for Clothes-Changing ReID. arXiv preprint arXiv:2601.19133.
[7] Narouei, F. H., Tang, Z., Wang, S. I., Hashmi, R. H., Welch, D., Sethuraman, S., ... & McNeill, V. F. (2025). Effects of germicidal far-UVC on ozone and particulate matter in a conference room. Plos one, 20(8), e0328224.
[8] Xiao, J., Hai, L., Li, Y., Li, H., Gong, M., Wang, Z., ... & He, D. (2022). An Ultrasmall Fe3O4 ‐ Decorated Polydopamine Hybrid Nanozyme Enables Continuous Conversion of Oxygen into Toxic Hydroxyl Radical via GSH ‐ Depleted Cascade Redox Reactions for Intensive Wound Disinfection. Small, 18(9), 2105465.
[9] Ge, H., & Wu, Y. (2023). An Empirical Study of Adoption of ChatGPT for Bug Fixing among Professional Developers. Innovation & Technology Advances, 1(1), 21–29. https://doi.org/10.61187/ita.v1i1.19
[10] Li, G., Yuan, H., Chen, S., Hu, Q., Wang, J., & Jiang, K. (2026). MFT: Memory-Aware Fine-Tuning of SAM2 for Efficient Long-Sequence Video Object Segmentation. IEEE Signal Processing Letters.

[11] Yan, W., Wu, Y., Liang, P., Yuan, M., Liu, J., Yang, J., & Li, X. (2026, March). PRISM: Pipeline for Root-cause Investigation via Specialized Multi-agents. In 2026 International Conference on Generative Artificial Intelligence and Information Security (GAIIS) (pp. 709-712). IEEE.
[12] Hu, H., Zhang, J., & Sun, Y. (2024). The Multiscale Deep Neural Networks: Unveiling New Directions in Text Sentiment Analysis. Innovation & Technology Advances, 2(2), 34–45. https://doi.org/10.61187/ita.v2i2.65