10.70711/aitr.v2i6.5748

# Exploration of the Application of Data Encryption Technology in Computer Network Communication Engineering

**Weizhi Sun, Chaojun Zou**

**Changsha Normal University, Changsha 410200, Hunan**

***Abstract:*** With the rapid development of information technology, computer network communication engineering has been widely applied in various fields. However, the complexity of the network environment and the security threats it poses make data confidentiality and integrity important issues. This article explores the key role of data encryption technology in computer network communication, analyzes different encryption methods and their practical applications, aiming to provide effective solutions for improving network communication security and promote the development of related technologies.

***Keywords:*** Data encryption; Computer network; Communication engineering

In modern society, computer networks have become an important medium for information transmission and communication. However, the security issues of data in the process of network communication are becoming increasingly serious, and incidents such as network attacks, data breaches, and privacy violations are not uncommon. To address these issues, data encryption technology has emerged. Encryption technology can not only protect the security of data during transmission, but also ensure the confidentiality and integrity of information. This article introduces several commonly used data encryption techniques and their applications in computer network communication engineering, aiming to provide reference for improving the security of computer networks.

## 1. Common data encryption techniques

### 1.1 Link Encryption Technology

Link encryption technology is a technique that encrypts transmitted data at the data communication link layer, typically running at the second layer of the OSI model, the data link layer. This means that it encrypts data packets before they enter the network, protecting the secure transmission of data. Link encryption is transparent to users and applications, and users do not need to change existing applications or communication protocols to enjoy the security brought by encryption, which provides convenience for network deployment and use. In link encryption technology, multiple encryption algorithms can be selected, such as symmetric encryption (AES, DES) and asymmetric encryption (RSA, ECDSA), and users can choose the appropriate algorithm according to their own needs. Link encryption technology is currently widely used in virtual private networks (VPNs), wireless local area networks (such as WPA/WPA2), and enterprise network connections to ensure the secure transmission of data in insecure network environments.

### 1.2 Node encryption technology

Node encryption is a means of encrypting data for specific nodes (such as user terminals, servers, IoT devices, etc.) in a computer network. Its main goal is to protect the confidentiality and integrity of data throughout its entire lifecycle of generation, storage, and transmission. Before the data is sent, the source node encrypts the data using encryption algorithms. The encrypted data is sent to the target node, and even if the data is intercepted during transmission, the attacker cannot decrypt the data. After receiving the encrypted data, the target node decrypts it using the corresponding key and restores it to plaintext data for processing. Node encryption technology can be applied in various scenarios [1]. For example, in cloud services, user data can be encrypted on the client side to ensure the security of the data during storage and transmission to the cloud platform; When sensitive data is transmitted between mobile devices and desktop computers, using node encryption can protect user privacy. In addition, IoT devices (such as smart homes, industrial equipment, etc.) can also ensure that their transmitted data is not maliciously intercepted through node encryption technology.

### 1.3 End to end encryption

End to end encryption is a communication method that ensures the security of information throughout the entire process of sending and receiving through encryption techniques. Even if intercepted during data transmission, third parties (including service providers) cannot access

or decrypt the information. The sender encrypts the message using encryption algorithms before sending it, including symmetric encryption (such as AES) and asymmetric encryption (such as RSA). In the case of using asymmetric encryption algorithms, the sender encrypts the message using the receiver's public key, and the information is sent over the network. Any third party that intercepts the message cannot decrypt it. After receiving the encrypted message, the receiver decrypts it using its private key and restores it to plaintext data. End to end encryption technology is widely used in communication applications to protect users' chat records and call content from theft. End to end encryption is also applied in email services such as ProtonMail to ensure that users' email content is encrypted during both sending and receiving processes. Currently, major technology companies and organizations are exploring and developing standards for end-to-end encryption to enhance interoperability and security. With the development of quantum computing and other emerging technologies, new end-to-end encryption schemes may emerge in the future to enhance security and efficiency.

## 2. The Application of Encryption Technology in Computer Network Communication Engineering

### 2.1 Data transmission

The application of encryption technology in computer data transmission is extensive and important, mainly used to protect the confidentiality, integrity, and authenticity of data. By using encryption technology to convert data into an unreadable form, it ensures that even if the data is intercepted during transmission, it cannot be understood. In data transmission, two main algorithms are used: symmetric encryption and asymmetric encryption, based on encryption protocols such as TLS, VPN, SSH, etc. TLS is a transport layer security protocol, which is mainly used to protect HTTP traffic on the Internet. It is the basis of modern Web security and ensures the security of data between the client and the server. VPN is a virtual private network that establishes encrypted channels on public networks to protect data transmission and ensure secure connections between remote users and enterprise networks. SSH is a secure shell protocol used to securely access remote computers and ensure the secure transmission of data and commands through encryption. In addition to protecting the confidentiality of data, encryption technology is often combined with hash algorithms to ensure the integrity of data during transmission. Hash algorithms (such as SHA-256) can detect whether data has been tampered with by generating a hash value of the data, and comparing the sent and received hash values during transmission to confirm whether the data is complete and lossless.

### 2.2 Data storage

Encryption technology can effectively protect sensitive data stored in computers, servers, and mobile devices, preventing unauthorized access and data leakage. By converting data into an unreadable format, only users holding the correct key can decrypt it. Full disk encryption is the process of encrypting the entire hard drive to ensure that all data stored on the disk remains encrypted in the event of system shutdown or unauthorized access. Partition encryption is the selective encryption of certain partitions or files while keeping other data unencrypted. In database management systems, data encryption is used to protect sensitive information in the database, and its implementation methods mainly include column level encryption and transparent data encryption. Column level encryption is the process of encrypting specific columns, such as user passwords and credit card numbers, to ensure that only authorized users can access this information. Transparent data encryption is encryption performed at the database level to protect the security of data files and log files, and is commonly used in SQL Server, Oracle Database, and other applications.

### 2.3 Email encryption

The main purpose of email encryption is to protect information from unauthorized access, ensure that only the sender and recipient can view the content of the email, and prevent information from being intercepted or tampered with during transmission. There are two commonly used email encryption protocols, one is PGP, which allows users to encrypt and digitally sign email content, ensuring the confidentiality and integrity of the email. The user needs to generate a pair of public and private keys [5]. The second is S/MIME, which protects emails through digital certificates and asymmetric encryption. Users obtain digital certificates from trusted certificate authorities to prove their identity and encrypt email content. Many companies use S/MIME or PGP to encrypt internal and external email communications in order to protect sensitive information such as customer data and trade secrets. Ordinary users can also use tools such as PGP and GnuPG to encrypt emails, ensuring personal privacy and security. Email encryption is typically combined with digital signatures to ensure the integrity and authenticity of the email. The sender generates a digital signature on the email content using their private key, and the receiver can use the sender's public key to verify the signature, confirming that the email has not been tampered with and that the sender is genuine and reliable.

## 3. Conclusion

With the rapid development of information technology and the increasingly complex network environment, data security issues have become more prominent, and the application of data encryption technology has become particularly important. The application of various encryption technologies, algorithms, and protocols provides comprehensive security guarantees for network communication. The widespread ap-

plication of data encryption technology has greatly improved the level of network security, whether in instant messaging, email, file transfer, or in fields such as cloud computing and the Internet of Things. In the future continuous development and innovation, data encryption technology will continue to provide strong support for the security and development of computer network communication engineering, helping to build a more secure and reliable network environment.

## References

[1] Yang Xin Application Analysis of Data Encryption Technology in Computer Network Communication Security [J] Network Security Technology and Applications, 2023, (08): 31-32

[2] Gu Siyi The Application of Data Encryption Technology in Computer Network Communication Security [J] Modern Industrial Economy and Informatization, 2023, 13 (02): 145-147

[3] He Feng Research on the Practical Application of Data Encryption Technology in Computer Network Security [J] Computer Knowledge and Technology, 2021, 17 (36): 67-69

[4] Zhang Bin Exploration of Security Vulnerabilities and Encryption Techniques in Computer Information Technology Data [J] Wireless Internet Technology, 2021, 18 (23): 94-95

[5] Hao Lin Exploration of the Application of Data Encryption Technology in Computer Network Security [J] Journal of Shanxi Energy University, 2021, 34 (05): 100-102

**About the author:** Weizhi Sun, Master's degree, research direction: Computer Technology, Computer Networks

**Fund:** This article is supported by the scientific research project "Research on Multivariate Time Series Prediction Based on Complex Network Methods and Graph Neural Networks" of the Education Department of Hunan Province (Project No. 22C1469).