Applied Science and Innovative Research
ISSN 2474-4972 (Print) ISSN 2474-4980 (Online)
Vol. 8, No. 2, 2024
www.scholink.org/ojs/index.php/asir

Original Paper

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

Hongzhi Huang

School of Computer and Software Engineering, Xihua University, Chengdu, Sichuan 610039, China

Received: May 4, 2024 Accepted: May 17, 2024 Online Published: May 22, 2024

doi:10.22158/asir.v8n2p80 URL: http://doi.org/10.22158/asir.v8n2p80

Abstract

With the rapid development of information technology, computer network communication has been widely used in various fields. However, the security issues of network communication have become increasingly prominent, and data is vulnerable to various attacks during transmission. Data encryption technology is a key technology for protecting information security. By converting plaintext information into non-mandatory ciphertext, the confidentiality and non-threatening nature of data are protected. This paper first introduces the basic principles and classification of data encryption technology, including real-time encryption, real-time encryption and hybrid encryption. It mainly analyzes the specific applications of data encryption technology in virtual private networks (VPNs), secure gateway security layers (SSL)/transport layer security (TLS), wireless network security, email encryption and cloud storage encryption. Finally, the development trends of emerging technologies such as quantum encryption, homomorphic encryption and blockchain encryption are discussed. By reasonably applying these encryption technologies, the security of computer network communication can be effectively improved.

Keywords

Data encryption technology, computer network communication, ultimate encryption, non-ultimate encryption, network security

1. Introduction

With the popularization of computer networks and the continuous advancement of information technology, network communication has penetrated into all aspects of social life and has become a part of the driver of modern society. However, while network communication brings convenience, it also faces severe security risks. In the process of data transmission in the network, there may be various attacks such as eavesdropping, tampering, and disguise, which seriously threaten the confidentiality,

integrity and authenticity of information. In order to protect the security of network communication, data encryption technology has emerged and has received widespread attention and research in practical applications.

Encryption technology converts plaintext information into encrypted text, which cannot be interpreted even if it is intercepted during transmission, thereby achieving information security. Encryption technology can be divided into the most encrypted and the most encrypted categories, each with its own non-novel encryption algorithm with fast calculation speed and suitable for encryption of large amounts of data, but the key management complexity is high; non-novel encryption algorithm has high security and relatively simple key management, but the calculation complexity is high and suitable for encryption of large amounts of data. In addition, hybrid encryption technology combines the advantages of extreme speed encryption and non-extreme speed encryption, and is widely evaluated in actual network communications.

This paper aims to explore the application of data encryption technology in network communication security. First, the basic principles and classification of data encryption technology are introduced, and its specific computer applications in different fields are analyzed. Finally, the development trend of data encryption technology is prospected. In-depth research can provide theoretical support and technical guidance for improving the security of network communication.

2. Basic Principles of Data Encryption Technology

Data encryption technology protects the confidentiality and integrity of information during transmission by converting plaintext information into invincible ciphertext. The encryption process involves two basic operations: encryption and decryption. Encryption is the process of converting plaintext into ciphertext, and decryption is the process of converting ciphertext into plaintext. Encryption and decryption usually rely on a certain encryption algorithm and key.

2.1 Innovative Encryption Algorithm

Novel encryption algorithm is a type of encryption technology that uses the same key for encryption and decryption. Common novel encryption algorithms include Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Advanced Encryption Standard (AES), etc. These algorithms perform well in processing speed and can perform encryption and decryption operations quickly, so they are widely used in scenarios that require efficient data processing. The implementation of novel encryption algorithms is relatively simple and suitable for resource-based environments. However, a major challenge of such algorithms is key management, especially in large-scale networks, ensuring the secure distribution environment and storage of keys is a complex task. If the key is leaked, the security of the entire encryption system will be threatened.

2.2 Non-substitution Encryption Algorithm

Symmetric asymmetric encryption algorithms, also known as symmetric encryption algorithms, use symmetric keys: symmetric and private keys. Symmetric keys are used to encrypt data, while

symmetric keys are used to decrypt data. Common asymmetric encryption algorithms include RSA (Rivest-Shamir-Adleman) algorithm and Elliptic Curve Cryptography (ECC) algorithm. A significant disadvantage of non-temporary encryption algorithms is the anonymity of key management. Since different keys are used for encryption and decryption, the public key can be distributed publicly, while the private key must be kept strictly confidential, which greatly reduces the security risks that may occur during the key distribution process. However, compared with temporary encryption algorithms, the encryption and decryption process of non-temporary encryption algorithms is slower and more computationally complex, and is usually used in situations where high security is required, such as digital signatures and key exchange. In practical applications, cheap encryption and non-cheap encryption are generally used in combination to balance security and efficiency.

3. Classification of Data Encryption Technology

According to the way the encryption key is used, data encryption technology can be divided into the following categories:

3.1 Ultimate Encryption

Temporary encryption algorithms use the same key for encryption and decryption. Common speed encryption algorithms include DES, 3DES, AES, etc. Temporary encryption algorithms are characterized by fast calculation and are suitable for encrypting large data. Its implementation process is relatively simple, with high computational efficiency and the ability to process large amounts of data. Therefore, it is widely used in scenarios that require data processing. However, the main problem facing fast encryption is the distribution and management of keys, especially in the field of network communications, where how to securely transmit encryption keys is an important challenge. If the key is stolen or leaked during transmission, the security of the entire encryption system will be seriously threatened. Therefore, in practical applications, cryptocurrencies usually need to be equipped with other encryption technologies to ensure the safe and secure distribution and storage of keys.

3.2 Non-charged Encryption

Common non-encryption algorithms are RSA and ECC. Non-encryption encryption algorithms are characterized by high security and relatively simple key management. Since encryption and decryption use different keys, public keys can be publicly distributed, while private keys need to be kept strictly confidential, which greatly reduces the security risks that may occur during key distribution. However, compared with encryption algorithms, asymmetric encryption algorithms have slower encryption and decryption processes and higher computational complexity. Asymmetric encryption is often used in scenarios such as encryption key exchange and digital signatures, where high security is a factor that needs to be considered. In practical applications, asymmetric encryption is often used for asymmetric encryption keys to achieve secure key exchange.

3.3 Hybrid Encryption

The encryption technology combines the advantages of temporary encryption and non-hybrid

encryption. The usual practice is to use a non-temporary encryption algorithm to encrypt the temporary encryption key, and then use the temporary encryption algorithm to encrypt the actual data. This method ensures that the data is encrypted. Specifically, during the data transmission process, the data key is first encrypted with the receiver's key, and then the encrypted key is used together with the data encrypted with the key. The receiver uses its private key to decrypt the private key, and then uses the private key to decrypt. This hybrid encryption method makes full use of the efficiency of the private key and the security of the non-private key. It is one of the most secure and commonly used encryption technologies. It is widely used in e-commerce evaluation, online banking and other scenarios that require highly secure data transmission.

4. Application of Data Encryption Technology in Computer Network Communication

4.1 Virtual Private Network (VPN)

Virtual Private Network (VPN) is a technology that enables secure communication between remote users and the company's internal network by establishing an encrypted channel on a public network (such as the Internet). VPN uses various encryption protocols (such as IPsec, SSL/TLS) to ensure the confidentiality and ownership of data and prevent data from being stolen or tampered with during transmission. Through VPN, remote users can securely access internal company resources as if they were in the company's internal network. In addition, VPN also provides authentication and access control functions to ensure that only authorized users can connect to the network. VPN technology comprehensively covers scenarios such as corporate remote office and internal network interconnection of multinational companies, effectively protecting the security of sensitive information.

4.2 Secure Sockets Layer Gateway (SSL)/Transport Layer Security (TLS)

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are encryption protocols used to provide secure communication in computer networks. The SSL/TLS protocol encrypts data at the transport layer to ensure the security of data during network transmission. Their main functions include data encryption, data integrity verification and authentication. SSL/TLS fully evaluates the HTTPS protocol to protect the privacy and data security of users on the Internet. Through SSL/TLS, the communication between users and websites is encrypted to prevent sensitive information (such as credit card numbers and passwords) from being stolen during transmission. In addition, SSL/TLS also verifies the true identity of the website through digital certificates, preventing users from accessing fake websites, and improving the security of Internet transactions.

4.3 Wireless Network Security

Due to its openness, wireless networks are vulnerable to various attacks, such as eavesdropping and unauthorized access. In order to protect the data transmission security of wireless networks, a variety of wireless security protocols are adopted, including WEP (Wired Equivalent Privacy), WPA (Wi-Fi), and HTTPS. These protocols use encryption technology to protect data transmission in wireless networks and prevent illegal user intrusion and data eavesdropping. WEP uses the RC4 encryption algorithm, but

due to its weak security, it has gradually been replaced by WPA and WPA2. WPA uses TKIP (Temporal Key Integrity Protocol) and MIC (Message Integrity Check) technology to enhance the security of data transmission. WPA2 further adopts the stronger AES (Advanced Encryption Standard) encryption algorithm, which greatly improves the security of wireless networks. Security has become the most commonly used wireless security protocol. The application of wireless network security technology ensures data privacy and system security in wireless communication environments.

4.4 Email Encryption

Email encryption technology ensures the confidentiality and integrity of emails during transmission by encrypting the content of emails. Common email encryption technologies include PGP (Pretty Good Privacy) and S/MIME (Secure/Multi Purpose Internet Mail Extensions) PGP provides email encryption and digital signature functions by combining temporary encryption and non-temporary encryption, ensuring that only designated recipients can read the email content and verifying the authenticity and integrity of the email. Based on the S/MIME infrastructure (PKI), it provides similar encryption and signature functions and is widely evaluated in enterprise-level email systems. Through email encryption technology, users can prevent emails from being eavesdropped or tampered with during transmission and protect the security of sensitive information.

4.5 Cloud Storage Encryption

With the popularity of cloud computing, more and more companies and individuals store data in the cloud. Cloud storage encryption technology protects the confidentiality and security of data by encrypting data stored in the cloud, preventing data leakage and illegal access. Cloud storage encryption can be performed during data transmission or during data storage. Transmission encryption usually uses SSL/TLS protocol to ensure that data will not be intercepted during transmission. Storage encryption uses privacy encryption and non-privacy encryption technology to encrypt data, and only authorized users can decrypt and access it. Through cloud storage encryption, users can ensure that data stored in the cloud cannot be read and used even if it is obtained by unauthorized third parties, effectively protecting the privacy and security of the data.

5. Development Trend of Data Encryption Technology

5.1 Quantum Encryption

The emergence of quantum encryption technology is a cutting-edge solution to the threat of quantum computing to traditional encryption algorithms. Quantum encryption uses the principles of quantum mechanics, especially quantum entanglement and quantum superposition, to achieve unconditionally secure communication. Quantum key distribution (QKD) is the core of quantum encryption technology, which enables secure transmission of information by distributing encryption keys between two remote locations. The security of QKD is based on physical logic rather than computational complexity, which means that even with unlimited computing power, attackers cannot decipher the key.

A quantum key distribution system usually consists of two main parts: a transmitter (Alice) and a

receiver (Bob). Alice generates and sends a series of quantum states, and Bob measures these quantum states and compares and corrects the data with Alice through a classical communication channel. Due to the special properties of quantum states, any eavesdropping behavior will introduce noise and be detected, thereby ensuring the secure transmission of keys.

Currently, QKD has been verified in some experiments and preliminary commercial applications. For example, China launched the world's first quantum communication satellite "Mozi" in 2016, successfully realizing quantum key distribution between satellites and ground. In addition, some scientific research institutions and companies in Europe are also actively exploring quantum communication technology and have carried out multiple pilot projects. However, although QKD can provide unconditional security in theory, its large-scale popularization still faces technical and cost challenges.

On the one hand, the high manufacturing and maintenance costs of quantum communication equipment limit its widespread application in practice. On the other hand, the transmission distance and speed of quantum key distribution are also limited by existing fiber-optic communication technology. In the future, with the advancement of technology and the reduction of costs, quantum encryption is expected to become an important tool for protecting the security of sensitive information, especially in fields with high security requirements such as military and finance.

In addition, the development of quantum computers has also prompted scientists to explore new quantum encryption methods, such as encryption algorithms based on lattice theory. These algorithms can not only resist quantum computing attacks, but also provide higher security and efficiency. In short, the development of quantum encryption technology will have a profound impact on the field of information security and provide an important solution to future security threats.

5.2 Homomorphic Encryption

Homomorphic encryption is an encryption technology that allows direct operations on ciphertext, and the calculation results after decryption are the same as those of operations on plaintext. This technology supports the processing of encrypted data while protecting data privacy, solving the problem of possible leakage of data during use. The core idea of homomorphic encryption is to use a mathematical method to make the operation result of encrypted data directly obtain the valid result after decryption.

Homomorphic encryption is mainly divided into partial homomorphic encryption and full homomorphic encryption. Partial homomorphic encryption only supports certain specific operations, such as addition or multiplication, while full homomorphic encryption supports any calculation operation. In 2009, Craig Gentry, a researcher at IBM, proposed the first full homomorphic encryption scheme, which pioneered this field. Gentry's scheme is based on ideal lattices and Boolean circuits. Although its computational complexity is high, it provides an important theoretical basis for subsequent homomorphic encryption research.

In practical applications, homomorphic encryption has broad application prospects in cloud computing, database security, and privacy-preserving computing. For example, users can encrypt data and store it

in the cloud, and perform operations such as search and calculation under the condition of decryption in the cloud, effectively protecting data privacy. In addition, homomorphic encryption can also be used in scenarios such as electronic voting, financial computing, and medical data processing, providing a safe and reliable data processing solution.

However, the computational complexity and performance bottleneck of homomorphic encryption are still the main problems that limit its widespread application. The existing homomorphic encryption algorithms have low computational efficiency in practical applications and are difficult to meet the needs of large-scale data processing. To this end, researchers are actively exploring optimization algorithms and hardware acceleration methods to improve the performance of homomorphic encryption. For example, the use of hardware accelerators such as graphics processing units (GPUs) and field programmable gate arrays (FPGAs) can significantly improve the computational efficiency of homomorphic encryption.

In short, although homomorphic encryption still faces some challenges in technical implementation, its unique advantages in data privacy protection give it broad development prospects. With the deepening of optimization research and the improvement of algorithms, homomorphic encryption is expected to be more widely used and developed in the future, providing new solutions for the field of information security.

5.3 Blockchain Encryption

Blockchain technology uses cryptographic means to ensure the immutability and traceability of data. Its decentralized characteristics and high-security structure show great application potential in many fields. Blockchain is a distributed ledger technology that ensures that the data on each node is consistent and immutable through cryptographic algorithms and consensus mechanisms. Its core technologies include hash functions, digital signatures, and consensus algorithms.

In the blockchain system, each data block contains the hash value of the previous block, thus forming a chain structure. This design ensures the integrity and immutability of the data, because any modification to a block will cause the hash values of all subsequent blocks to change. In addition, blockchain uses digital signature technology to verify the authenticity of each transaction and ensure the security of transaction data.

The transparency and immutability of blockchain give it a wide range of application prospects in the financial field. For example, digital currencies such as Bitcoin and Ethereum have realized decentralized currency transactions through blockchain technology, providing a safe and transparent trading environment. Smart contracts are another important application of blockchain technology. It automatically executes contract terms through preset programs without the intervention of third parties, thereby improving the efficiency and security of transactions.

In supply chain management, blockchain can achieve transparent traceability of the entire chain, prevent the circulation of counterfeit and inferior products, and improve the transparency and credibility of the supply chain. For example, Walmart and IBM have jointly developed a

blockchain-based food traceability system to ensure the safety and authenticity of food by recording the data of the entire process from production to sales. In addition, blockchain has also shown great application potential in fields such as medical record management, intellectual property protection, and voting systems.

Despite the many advantages of blockchain technology, its large-scale application still faces some challenges. For example, the performance and scalability issues of blockchain systems limit their application in high-frequency trading scenarios. To this end, researchers are exploring solutions such as sharding technology, side chains, and state channels to improve the processing power and efficiency of blockchain systems.

In short, with the continuous maturity of blockchain technology and the expansion of application scenarios, blockchain encryption will play an important role in more fields and promote the development of data security technology. Through continuous innovation and optimization, blockchain is expected to become an important infrastructure of the future information society, providing secure, transparent, and efficient data management solutions for various industries.

5.4 Multi-party Secure Computing (MPC)

Multi-party secure computing (MPC) is a technology that allows multiple participants to jointly calculate without exposing private inputs. By using cryptographic protocols, MPC allows parties to collaborate on computations without sharing sensitive data, thereby protecting data privacy. The basic idea of MPC is to decompose the computational task into several subtasks, with each participant only processing the part related to itself, and finally obtaining the overall computational result by combining the computational results of all parties.

One of the core protocols of MPC is the secret sharing scheme, in which each participant holds a part of the data called a "share". These shares are generated in a mathematical way so that no single share can leak the information of the original data. Only when enough participants join together can the original data be restored. The Shamir secret sharing scheme is one of the most famous secret sharing algorithms, which is based on polynomial interpolation theory and has high security and flexibility.

In practical applications, MPC has broad application prospects in privacy protection, data sharing, and secure computing. Especially in the fields of healthcare, finance, and government, MPC can achieve cross-institutional data sharing and joint analysis without exposing personal privacy. For example, in medical research, multiple hospitals can use the MPC protocol to share patients' genetic data and medical records, so as to conduct joint analysis and discover potential factors and treatments for diseases without leaking patients' private data.

In the financial field, MPC can be used for the construction of multi-party joint risk control models and credit assessment. Multiple financial institutions can jointly analyze the credit risk of customers without sharing customer data, thereby improving the accuracy and efficiency of risk management. In addition, MPC can also be used in scenarios such as electronic voting, auctions, and federated learning to provide secure and reliable data processing solutions.

Although MPC has many advantages, its practical application still faces some challenges. First, the computational complexity of the MPC protocol is high, which makes it difficult to meet the needs of large-scale data processing. Second, the design and implementation of the MPC protocol requires complex cryptographic knowledge, which increases the difficulty of development and maintenance. To this end, researchers are actively exploring optimization algorithms and hardware acceleration methods to improve the performance and usability of MPC.

In short, multi-party secure computing technology provides new ideas and methods for data privacy protection and secure computing. With the continuous advancement of technology and the expansion of application scenarios, MPC is expected to be widely used in the future, injecting new vitality into the field of information security.

5.5 Zero-Knowledge Proofs

Zero-knowledge proof is a cryptographic technique that allows one participant to prove to another that a statement is true without revealing actual information. This technique is widely used in identity verification, digital identity authentication, data verification, etc. Zero-knowledge proof can effectively protect personal privacy while ensuring the reliability and integrity of data.

The basic principle of zero-knowledge proof is to use a mathematical method to enable the prover to prove to the verifier that a statement is true without revealing the specific proof process or additional information. Classic zero-knowledge proof protocols include the Fiat-Shamir protocol and the Schnorr protocol, which are based on number theory problems such as the discrete logarithm problem and have high security and efficiency.

In practical applications, zero-knowledge proof technology has broad application prospects in blockchain, digital identity authentication, and privacy-preserving computing. In the blockchain field, zero-knowledge proofs are widely used in transaction verification of privacy coins (such as Zcash), which achieves a highly anonymous and secure transaction environment by concealing the transaction amount and the identity of the participants. In addition, zero-knowledge proofs can also be used for privacy protection of smart contracts to ensure the correctness and privacy of contract execution.

In the field of digital identity authentication, zero-knowledge proof technology can realize anonymous verification of user identity. For example, users can prove to service providers that they have a certain attribute (such as being over 18 years old) through the zero-knowledge proof protocol without revealing specific identity information. This technology not only protects the privacy of users, but also simplifies the identity authentication process, improving the security of the system and user experience.

In the field of privacy-preserving computing, zero-knowledge proof technology can be used for data verification and consistency checking. For example, data providers can prove the correctness and integrity of data to data recipients through the zero-knowledge proof protocol without revealing the specific content of the data. This technology has important application value in cloud computing and distributed storage systems, and can effectively prevent data tampering and leakage.

Although zero-knowledge proof technology has high security and privacy protection capabilities in

theory, its practical application still faces some challenges. For example, the computational complexity of the zero-knowledge proof protocol is high, and the verification process may require a long time and large computing resources. To this end, researchers are actively exploring efficient zero-knowledge proof algorithms and optimization methods to improve the performance and usability of its practical applications.

In summary, zero-knowledge proof technology provides a powerful solution for information security and privacy protection. With the continuous development of technology and the expansion of application scenarios, zero-knowledge proof is expected to be widely used in the future and make important contributions to the security and privacy protection of the digital society.

5.6 Combination of Deep Learning and Encryption

With the widespread application of deep learning in various fields, combining deep learning and encryption technology has also become a research hotspot. This combination can play an important role in protecting model privacy, securely transmitting data, and enhancing the security of machine learning models. Deep learning models usually require a large amount of training data, which often contains sensitive information, so protecting data privacy and model security becomes particularly important.

Homomorphic encryption is an encryption technology that can perform calculations directly on encrypted data. It provides an effective solution for privacy protection of deep learning models. Through homomorphic encryption, users can upload encrypted data to the cloud, and the cloud can perform model training and reasoning without decrypting the data, thereby protecting data privacy. For example, companies such as Microsoft and IBM have begun to explore the application of homomorphic encryption to deep learning models to achieve secure model training and reasoning.

Federated learning is a distributed machine learning technology that protects data privacy by training models on local devices and sharing model parameters instead of sharing the data itself. Combined with encryption technology, federated learning can further improve the security of data transmission and model parameters. For example, using differential privacy technology, noise can be added to model parameters to prevent malicious attackers from recovering the original data by analyzing model parameters.

The security of deep learning models is also an important research direction. Attackers can disrupt the normal operation of deep learning models through adversarial attacks, causing the model to make incorrect predictions. Combined with encryption technology, the model's defense against adversarial attacks can be improved. For example, by encrypting and obfuscating model parameters, it is more difficult for attackers to reverse engineer the model, thereby improving the security of the model.

In the fields of healthcare, finance, and intelligent transportation, the combination of deep learning and encryption technology has broad application prospects. For example, in the medical field, homomorphic encryption and federated learning technology can be used to achieve cross-hospital joint model training to discover potential factors and treatments for diseases without sharing patients' privacy data. In the financial field, encryption technology can be used to protect transaction data and

customer information, improving the security and privacy protection level of the financial system. In the field of intelligent transportation, encryption technology can be used to protect vehicle data and traffic information to prevent data leakage and malicious attacks.

Although the combination of deep learning and encryption technology has broad application prospects, its actual implementation still faces some challenges. First, the existing homomorphic encryption and federated learning algorithms need to be optimized in terms of computing efficiency and communication overhead, and it is difficult to meet the needs of large-scale deep learning models. Secondly, how to design efficient encryption algorithms and security protocols to protect the security of model parameters and data is also an urgent problem to be solved.

In short, the combination of deep learning and encryption technology provides a new solution for data privacy protection and model security. With the continuous advancement of technology and the expansion of application scenarios, this field is expected to be widely used in the future, providing safe and reliable technical support for the development of the information society.

6. Conclusion

With the rapid development of information technology, the urgency of data encryption technology in information security and privacy protection has become more prominent. Traditional encryption technology and non-encryption technology have been developed in daily data transmission and storage with their respective advantages. However, in the face of evolving threats and challenges, emerging encryption technologies such as quantum encryption, homomorphic encryption and blockchain encryption are gradually coming to the fore, showing great potential and application prospects. Quantum encryption uses the unique properties of quantum to achieve theoretically unconditionally secure key distribution, providing a guarantee for future information security. Homomorphic encryption solves the problem of privacy protection in the data processing process by directly calculating on the ciphertext, which is particularly suitable for fields such as cloud computing and big data analysis. Blockchain encryption has developed strong application potential in fields such as finance and supply chain management with its decentralized, transparent and tamper-proof characteristics, and has promoted the digitalization and standardization process in these fields.

Looking to the future, the development of data encryption technology will continue to innovate with the advancement of information technology. The research and application of emerging technologies will not only improve the security and efficiency of data encryption, but also further expand the application scenarios of encryption technology to meet the needs of dialogue. At the same time, with the increasing complexity and recognition of the network environment, the development of data encryption technology is also facing new challenges and opportunities.

References

Chen, K. T. (2023). A brief analysis of the application of data encryption technology in computer network security. *Electronic Components and Information Technology*, *7*(10), 193-196+202. http://doi.org/10.19772/j.cnki.2096-4455.2023.10.050

Cheng, G. D. (2024). Research on the application of data encryption technology in computer network security. *Information Recording Materials*, *25*(02), 84-86. http://doi.org/10.16009/j.cnki.cn13-1295/tq.2024.02.025

Fan, H. F. (2023). Application of data encryption technology in computer network security. Information *Recording Materials*, *24*(06), 58-60. http://doi.org/10.16009/j.cnki.cn13-1295/tq.2023.06.009

Ji, Q. Q. (2023). Discussion on the application of data encryption technology in computer network security. *Network Security Technology and Application*, *2023*(07), 22-23.

Jiang, S. (2024). Research on the application of data encryption technology in computer network security. *Network Security Technology and Application*, *2024*(04), 31-32.

Jiang, Y. L. (2024). Application of data encryption technology in computer network information security. *Information and Computer (Theoretical Edition)*, *36*(05), 215-217.

Li, R., Xia, T. Y., Zhang, Q., et al. (2024). On the application of data encryption technology in computer network security. *Network Security Technology and Application*, *2024*(01), 24-25.

Li, Z. R. (2023). Research on the application of data encryption technology in computer network security. *Information and Computer (Theoretical Edition)*, *35*(15), 13-16.

Lin, J. (2023). Application strategy of data encryption technology in computer network communication security. *Wireless Internet Technology*, *20*(09), 7-9.

Lin, J. (2024). Research on the application of data encryption technology in computer network communication security. *Digital Communication World*, *2024*(04), 125-127.

Luo, X. G., Tan, J. H., & Zhou, L. (2023). Application of data encryption technology in computer network security Application Research. *China New Communications*, *25*(16), 123-125.

Lv, D. (2023). Analysis of the application of data encryption technology in computer network security. *Science and Technology Information*, *21*(13), 19-22. http://doi.org/10.16661/j.cnki.1672-3791.2211-5042-0488

Song, Y. (2024). Application of data encryption technology in computer network communication security. *Information and Computer (Theoretical Edition)*, *36*(04), 226-228.

Sun, D. X., & Liu, D. J. (2023). A brief analysis of the application value of data encryption technology in computer network security. *Information Systems Engineering*, *2023*(08), 52-55.

Wang, J. X. (2023). Application of data encryption technology in computer network information security. *Digital Communication World*, *2023*(07), 141-143.

Xu, J. L. (2023). Analysis on the application of data encryption technology in computer network security. *Electronic Production*, *31*(08), 113-115+120. http://doi.org/10.16589/j.cnki.cn11-3571/tn.2023.08.015

Yan, J. (2023). Research on the application of data encryption technology in computer network information security. *Information Recording Materials*, *24*(09), 152-154. http://doi.org/10.16009/j.cnki.cn13-1295/tq.2023.09.032

Yang, X. (2023). Application analysis of data encryption technology in computer network communication security. *Network Security Technology and Application*, *2023*(08), 31-32.

Zhang, G. C. (2023). Application significance of data encryption technology in computer network security. *Network Security Technology and Application*, *2023*(06), 30-32.

Zu, X. M. (2024). Application strategy of data encryption technology in computer network communication security. *Information Recording Materials*, *25*(02), 30-32. http://doi.org/10.16009/j.cnki.cn13-1295/tq.2024.02.005