

The Role of Data Encryption in Securing Network Communications

Xiaochen Que

Renmin University of China, Beijing 100000

Abstract: *With the computer network communication technology involved in various industries, enterprise databases and national databases, we need to pay attention to strengthening the maintenance of information data through various means to ensure the security of information data. Therefore, data encryption technology was born and has been better applied. Data encryption technology can effectively solve the problem of data being worn and tampered by virus programs, ensure the security and confidentiality of data, and play a positive role in ensuring the security of their own information and data. With information technology connecting the economic, political, cultural and educational exchanges between countries all over the world, actively carrying out the research on data encryption technology to ensure data security plays an important role in national development and national defense security. Based on this, this paper focuses on the application of data encryption technology, points out the importance of the application of data encryption technology, and analyzes the practical application of new data encryption technology.*

Keywords: Computer; Network communication security; Data encryption technology.

1. INTRODUCTION

The advancement of information technology and the practical development results achieved by information data in various industries have played a positive role in the development of enterprises, people's lives and the construction of the country's economy, politics, culture and other fields. But the computer network is a virtualized technology, the network world is built by the computer network as a virtualised world, It is difficult to be controlled by national laws, so it is easy to have network security incidents. From the frequent network security incidents and information security problems in recent years, there are still big problems in maintaining network security in China [1]. Therefore, our country should pay attention to the security protection of customer information and strengthen the study of data encryption and the corresponding information security technology. The following is the computer network communication security in the application of data encryption technology. Zhou [1] proposed a digital precision distribution strategy for social media content on private domain platforms in the automotive industry, utilizing a collaborative filtering model based on user behavior. Similarly, Wensi [2] explored AI-enabled data visualization marketing for automated production lines, emphasizing its role in building customer trust and improving lead-to-order conversion. In the context of dialogue systems, Ren [3] introduced a novel approach for role-oriented dialogue summarization aimed at balancing role contributions, while also developing a feature fusion-based model for smoking detection in complex contextual environments [4]. For smart city applications, Li, Wang, and Zhang [5] focused on named entity recognition to enhance visualization and interaction within data streams. Lin, Wang, and Hong [6] contributed to computational statistics with their work on the Poisson multinomial distribution, which has implications for ecological inference and machine learning. Meng et al. [7] addressed logistics optimization through deep learning-based research on green warehousing site selection and path planning. Wu [8] concentrated on fault detection and prediction to optimize resource usage in cloud infrastructure, while Tang et al. [9] focused on the design and optimization of shallow-angle grating couplers for vertical emission from indium phosphide devices. Chen [10] emphasized the importance of efficient and scalable data pipelines within gig economy platforms. Yang [11] applied the LightGBM algorithm to analyze the Chinese stock market, and Tang and Zhao [12] utilized neural networks to study the relationship between aging population distribution and real estate market dynamics. Wang [13] developed predictive modeling for sortation and delivery optimization in e-commerce logistics. Tu [14] proposed a platform-aware framework for intelligent 5G network test automation and issue diagnosis, and further introduced a modeling-driven approach for NAS and SIP message sequence modeling aimed at smart regression detection [15]. Xu et al. [16] investigated enhancing user experience and trust in advanced LLM-based conversational agents. Liu [17] explored cross-efficiency analysis and inverse DEA models to optimize supply chain efficiency. Yin et al. [18] applied deep learning for crystal system classification in lithium-ion batteries, while Luo et al. [19] enhanced e-commerce chatbots using Falcon-7B and 16-bit full quantization. Collectively, these studies underscore a growing trend toward leveraging AI, machine learning, and advanced data modeling to optimize system performance, enhance user interaction, and solve complex domain-specific challenges.

2. BASIC CONCEPTS AND IMPORTANCE ANALYSIS OF DATA ENCRYPTION

2.1 Basic concepts of data encryption

Today, with the positive results of computer information network communication technology in various fields, computer network communication technology has an important impact on all aspects of people's lives. But with the continued application of computer communication technology, people's information will also be stored in virtual networks, which are vulnerable to hackers or virus programs, which will cause users' information to be damaged or stolen by others. In order to avoid this situation, it is necessary to reasonably apply to the firewall, data encryption, and so on. And data encryption is through the user data to impose a certain key as a guarantee, If encountered by hackers or other wrongdoers, it will play a role in protecting data, even if the data is stolen by hackers and wrongdoers but due to the lack of decryption technology, it is also unable to obtain the user's data, thus directly safeguarding the user's data security. Build a complete encryption system in computer network communication, including in plaintext form, With the application of data encryption technology and the protection of data, the security of data can be significantly improved and the security of data can be guaranteed.

Data encryption is often divided into two kinds of key cryptography, symmetric and asymmetric. By using these two kinds of key cryptography, the data can be protected. Data encryption is further explained by the fact that some data in the process of communicating is passed through a key, Functions such as functions are transformed, which makes the transformed data a string of ciphertext that has no meaning, and only by obtaining the key password and decrypting it can the data be restored to usable data.

2.2 Analysis of the importance of data encryption technology application

At present, with the development of computer network communication technology, people save all kinds of information to the Internet, and accompanied by the use of all kinds of social software, such as QQ, WeChat, Weibo, browser and so on, The network retains a large amount of people's personal information. If people lack network security awareness and do not pay attention to network security protection, it will inevitably lead to information leakage or personal information theft, and even be operated by others to engage in illegal and criminal activities. In order to avoid this problem and ensure information security, it is necessary for people to enhance the awareness of information security. In this way, data encryption can play an active role in the field of data safety. Most scholars have pointed out that data encryption technology is one of the important ways to protect data security, and is often the most effective way.

For individuals, even if some important files will not appear in the network transmission, but also to do a good job in data encryption, in order to ensure that others know through various channels. For enterprises, there is a lot of important data in enterprise information databases. For example, financial data, business data, enterprise development planning, enterprise development strategy and employee information and so on, in order to protect the enterprise in the market competition development, we need to pay attention to the security management of enterprises, pay attention to the application of data encryption technology. For the country, the data held by the central government and local governments have contributed to China's development in various fields. It has a direct role in promoting people's livelihood, etc., and has an irreplaceable role in medical and health reform, education development, national defense security, etc. If these data are stolen or tampered with by others, it will have a huge impact on China's modernization and development. As a result, the importance of data encryption and its position in the protection of information security has been highlighted.

3. CONTENT ANALYSIS OF DATA ENCRYPTION TECHNOLOGY

In order to ensure the safety of all kinds of information and user data, and make these data play a real role, we should pay attention to the introduction of data encryption technology, through the introduction of data encryption technology to protect data security. When using data encryption technology, companies and individuals should pay attention to the specific content of encryption technology, and then use data encryption technology flexibly to play the original role of data encryption technology has a direct relationship. Generally speaking, the use of data encryption technology mainly includes the following:

3.1 Network communication protocol

Analyzing and interpreting network communication protocols actually refers to using symmetric encryption algorithms, The public key cryptography system is created as a precondition that requires the consent of both parties to the data transmission and the application of multi-car encryption to ensure the security of the file transmission process and the file itself, so as to avoid the loss of the file during transmission. In addition, the transmission of data in this way has obvious advantages, because the network communication protocol itself has the advantages of making the server itself extremely stable, so it is difficult to generate false server information. This is the user transmission data, data sharing has played a security role, and through the network communication protocol to access the server, but also to determine whether the server risk, if there is risk, immediately stop access, and thus protect the user's personal information security.

3.2 File Encryption and Key Management

The application of data encryption technology will inevitably involve algorithms, key management and so on, and through a fixed algorithm, formula, rules and so on, the application of data encryption technology can produce reasonable plaintext, ciphertext, and so on, and then through the decryption technology to restore the file. Before communication services occur on the entire system client and server side, by distributing the server public key, the application on the server side will automatically filter the user, realize the allocation of user information, and handle confidential information effectively.

3.3 System structure and design

When using data encryption technology, we should pay attention to the implementation and design of server-side application program and user information management module, and to the construction of system internal system and module. Only do this part of the work, can play the function of system [3].

4. SECURITY RISKS IN COMPUTER NETWORK COMMUNICATION

Today, everything from people's daily life to the production and operation of enterprises, from national news to personal daily life, basically does not depend on the Internet and computer network communication. A lot of information resources have been saved in the virtual network, such as citizens, business, state secrets and so on. However, due to the vulnerabilities of computer network technology, hacker intrusion, the spread of various virus programs, etc., there are huge security risks in computer network communication, which has a great impact on the security of data. In the research of many scholars, it has been pointed out that computer network communication itself belongs to a network behavior pattern, and in this network behavior pattern, The actual situation is extremely complex, and in this series of complex operations, security hazards of various computer network communication are easy to occur, which is easy to cause the disclosure of user information, leading to the theft of user information by others, even to manipulation by others. However, in addition to a series of security problems formed by the computer's own operating system, it may also cause certain data security hazards for a variety of other reasons, ultimately posing a threat to the security of users' private information and data. There are also some security issues in the browsers, which contain a series of uncertain security factors. At the same time, it also has the unsafe Internet protocol, which provides certain basic conditions for hackers and some criminals who know the network vulnerabilities to steal users' personal information, destroy enterprise information base and so on. Often there is some fishing advanced in some insecure websites, users visit through the browser, from the user to see the interface although there is no substantive change, the user can normal operation of the computer, but in the background of the computer may be slowly downloading Trojan virus, In particular, some hackers may use virus programs to remotely manipulate the user's computer program, and steal the user's personal information without the user's knowledge. These are all security issues that exist in computer network communication and need to be taken seriously by the user. If the user is an enterprise employee, enterprise manager, or government employee, it is more important to pay attention to this to prevent security risks.

5. CURRENT DATA ENCRYPTION TECHNOLOGY APPLICATION METHODS

In order to protect the computer network communication security, it is necessary to pay attention to the flexible application of current data encryption technology, so that the encryption methods play the original role.

5.1 Online encryption methods

In general, this method is also called "link encryption," which is mainly determined by the specific application characteristics of this method, and the application of this encryption technology focuses on the fact that the encryption work is done through a link. After adopting this method, the computer network information has been encrypted at each node before it is officially transmitted, and this makes some important data must be decrypted step by step during transmission. If it is not possible to decrypt each node during transmission, the data cannot be transmitted effectively, and there may be some security problems.

5.2 Node encryption method

By adopting this method of encryption, each node of data transmission can be encrypted to ensure the security of data transmission. Generally, whether computer network information communication is secure and the entire communication environment is reliable, which plays an important role in the final data security, ensuring the authenticity and validity of data. In order to ensure the trustworthiness of data and the security of information, attention needs to be paid to the security of data through the application of node encryption. As can be seen from the actual application of online encryption methods, online encryption methods also encrypt the various nodes in the transmission. However, the node encryption method is different from this method. The node encryption pays more attention to the prevention and analysis of information service attacks, and needs to deal with the attacks from the network actively on the basis of data encryption. In addition, the data can never appear in plain text, and the amount of encryption and decryption work will continue to increase throughout the transmission process [4].

5.3 End-to-end encryption method

This is also a method often used in cryptographic processing, and the specific application of this method is simpler than the first two methods. This operation is only before the data transmission to do a good job of encryption processing, and transmission does not appear in the transmission of each node in the course of this process, after receiving the data file, Decryption can be performed using decryption methods, so the time cost of such methods is relatively low compared to the first two methods, in addition to the stability of end-to-end encryption methods, which can guarantee the security of data so that it cannot be stolen. However, the disadvantages of this method are also very obvious, and the disadvantages are in the two ports after the data is sent and the data is received. Without effective technology to block encryption, decryption methods and processes, the security of data cannot be ensured if hackers and other wrongdoers are attacked from these two ports.

6. THE PRACTICAL APPLICATION OF DATA ENCRYPTION TECHNOLOGY IN COMPUTER NETWORK COMMUNICATION SECURITY

6.1 Applications in databases

There are a lot of information and data stored in computer and network database, and these data are very important to the development of users, enterprises and governments. In the current application of data encryption technology, more attention is often paid to the encryption of data transmission process to protect the safety of data transmission. In fact, the management of computer network database system also need to use encryption to deal with data, through data encryption to protect the safety of data, to protect the safety of the database, to prevent the intrusion of hackers and viruses. In addition, the database supports the transmission of data information relatively weak, and in order to ensure data security, it is necessary to effectively manage the database together and do the encryption treatment of the database. Especially for businesses and governments, important data is often stored in databases. These data play an important role in innovating products and reforming the mode of production. It is also important for the government to formulate reasonable policies on people's livelihood, to actively promote the implementation of the measures promulgated by the CPC Central Committee, and to promote the socialist modernization process. Once the database is compromised and some damage occurs, it may cause some important information to be corrupted, adversely affect the further development of the enterprise, and hinder the further implementation of the government's work. In order to avoid this problem, it is necessary to strengthen the use of encryption technology in database management, in order to protect information security.

6.2 Application in Local Area Network

At present, in the process of daily production work of enterprises, in order to ensure the effective transmission of information data, ensure the security of information data and fulfill the true role of various data, computer systems are connected to the local area network and applied. Includes important meetings, confidential documents, and

other types of information with a large number of enterprises, All of them are transmitted and stored in the local area network in the form of data, and when an enterprise queries these important meetings and confidential documents, it can log into the platform built by the enterprise to query the specific data. Therefore, local area networks play an important role in the storage and management of various data of enterprises, and play a more significant role in promoting the sustainable development of enterprises. However, it is undeniable that while the local area network provides convenience for enterprises to work, it cannot avoid these problems of viruses and hackers [5]. Many hackers, criminals with computer knowledge, will use the local area network to steal important information from enterprises. Once corporate secrets are stolen, or corporate confidential data is tampered with by hackers and virus programs, it will directly affect the development of various tasks at a later stage. Therefore, data encryption should also be applied to LAN to ensure that the data in the LAN has been automatically saved during transmission. Encryption and so on work, and this data can only be decrypted by decryption method after transmission, which can restore the data as it is for use by enterprise managers.

7. CONCLUSION

In short, information technology has been widely used in various fields at present and has achieved positive results. Information technology has changed all aspects of people's lives and has played an important role in enterprise development, government work, and national construction. But in the information technology is widely used today, there are a series of information security issues. In order to ensure the safety of information data, to ensure that the data will not be stolen by others, malicious tampering, it is necessary to attach importance to the rational use of data encryption technology, data encryption technology to play a practical role.

REFERENCES

- [1] Zhou, Z. (2025, November). Digital precision distribution strategy for social media content on private domain platforms in the automotive industry: a collaborative filtering model based on user behavior. In Proceedings of the 2025 International Conference on Digital Society and Intelligent Computing (pp. 516-521).
- [2] Wensi, L. (2026). AI-Enabled Data Visualization Marketing for Automated Production Lines: Building Customer Trust and Improving Lead-to-Order Conversion. *Academic Journal of Natural Science*, 3(1), 8-13.
- [3] Zheng Ren, "Balancing role contributions: a novel approach for role-oriented dialogue summarization," Proc. SPIE 13259, International Conference on Automation Control, Algorithm, and Intelligent Bionics (ACAIB 2024), 1325920 (4 September 2024); <https://doi.org/10.1117/12.3039616>
- [4] Z. Ren, "A Novel Feature Fusion-Based and Complex Contextual Model for Smoking Detection," 2024 6th International Conference on Communications, Information System and Computer Engineering (CISCE), Guangzhou, China, 2024, pp. 1181-1185, doi: 10.1109/CISCE62493.2024.10653351.
- [5] Li, X., Wang, J., & Zhang, L. (2025). Named entity recognition for smart city data streams: Enhancing visualization and interaction. *Authorea Preprints*.
- [6] Lin, Z., Wang, Y., & Hong, Y. (2023). The computing of the Poisson multinomial distribution and applications in ecological inference and machine learning. *Computational Statistics*, 38(4), 1851-1877.
- [7] Meng, Q., Wang, J., He, J., & Zhao, S. (2025). Research on Green Warehousing Logistics Site Selection Optimization and Path Planning based on Deep Learning.
- [8] Wu, W. (2025). Fault Detection and Prediction in Models: Optimizing Resource Usage in Cloud Infrastructure.
- [9] Tang, Y., Kojima, K., Gotoda, M., Nishikawa, S., Hayashi, S., Koike-Akino, T., ... & Klamkin, J. (2020). Design and Optimization of Shallow-Angle Grating Coupler for Vertical Emission from Indium Phosphide Devices.
- [10] Chen, J. (2025). Efficient and Scalable Data Pipelines: The Core of Data Processing in Gig Economy Platforms.
- [11] Yang, J. (2025). Application of LightGBM in the Chinese Stock Market.
- [12] Tang, Y., & Zhao, S. (2025). Research on Relationship Between Aging Population Distribution and Real Estate Market Dynamics based on Neural Networks.
- [13] Wang, J. (2025). Predictive Modeling for Sortation and Delivery Optimization in E-Commerce Logistics.
- [14] Tu, Tongwei. "AutoNetTest: A Platform-Aware Framework for Intelligent 5G Network Test Automation and Issue Diagnosis." (2025).
- [15] Tu, Tongwei. "ProtoMind: Modeling Driven NAS and SIP Message Sequence Modeling for Smart Regression Detection." (2025).

- [16] Xu, Y., Gao, W., Wang, Y., Shan, X., & Lin, Y.-S. (2024). Enhancing user experience and trust in advanced LLM-based conversational agents. *Computing and Artificial Intelligence*, 2(2), 1467. <https://doi.org/10.59400/cai.v2i2.1467>
- [17] Liu, M. (2024). Optimizing Supply Chain Efficiency Using Cross-Efficiency Analysis and Inverse DEA Models.
- [18] Yin, Y., Xu, G., Xie, Y., Luo, Y., Wei, Z., & Li, Z. (2024). Utilizing Deep Learning for Crystal System Classification in Lithium - Ion Batteries. *Journal of Theory and Practice of Engineering Science*, 4(03), 199–206. [https://doi.org/10.53469/jtpes.2024.04\(03\).19](https://doi.org/10.53469/jtpes.2024.04(03).19)
- [19] Luo, Y., Wei, Z., Xu, G., Li, Z., Xie, Y., & Yin, Y. (2024). Enhancing E-commerce Chatbots with Falcon-7B and 16-bit Full Quantization. *Journal of Theory and Practice of Engineering Science*, 4(02), 52–57. [https://doi.org/10.53469/jtpes.2024.04\(02\).08](https://doi.org/10.53469/jtpes.2024.04(02).08)