The application of data encryption technology in computer network system

Hongyi Liu
Dongying Vocational College
76678773@qq.com

Abstract. Network security as the focus of the application of computer technology, in the construction and development of modern society, in the face of the rapid development of Internet technology, worldwide network communication and network trade, how to effectively protect the security of network data and information, to solve the security problem of network system, is the main issue discussed by the academic circle. As an important basis for ensuring computer information security, data encryption technology plays an important role in effectively improving network security construction. Therefore, on the basis of understanding the concept of data encryption technology, according to the operation requirements of computer network system in the new era, this paper mainly explores the application of data encryption technology in computer network system to clarify the main direction of rapid development of network technology in the future.

Keywords: computer network; Data encryption; Node data; Identity authentication; Storage encryption.

1. Introduction

In essence, data encryption, as a big data technical means, is to encrypt the data information stored in the computer system, prevent the data information from being directly stolen or stolen, comprehensively ensure the security of the computer network, and effectively protect the user's personal information. In the context of the development of data technology, data encryption technology is the basic content of application research in various fields. Data encryption key will be used to convert data encryption letters, and the data stored in the computer network will be transformed into meaningless ciphertext, so as to achieve data encryption protection. After the encryption of the data information, to use the decryption function and decryption, if completely restored, can be used normally. In the application of online computer network construction, data encryption technology is one of the more important contents, which has a positive impact on the construction of network security. As the application range of data encryption technology is more and more wide, it is reflected in many fields, such as bank cards, RFID cards, etc., and the existing data encryption technology includes public key encryption technology, symmetric key encryption technology and private key encryption technology, which contains a variety of data encryption algorithms, laying the foundation for ensuring data information security.

Computer network technology is to connect one or more computers and external devices in different locations independently of each other using corresponding communication lines to ensure that the computer network system can achieve information transmission and resource sharing with the help of network communication protocols and network management software. From the perspective of technology development, computer network technology is divided into the following stages: First, computer network technology remote terminal connection stage. In this stage, the main use of mainframe and communication lines, on the basis of effective connection to form a computer online system, in order to achieve computer remote processing work; Secondly, the network phase of computer network technology. In the late 1960s, human beings have entered the stage of orderly development of computer networks, connecting the communication lines of computer hosts in

different regions together, so that different computers can transmit information to each other, and computers are independent individuals. Third, the computer network technology of the network interconnection stage. In practice, in order to fully realize resource sharing, more computer networks are connected together through technology, and a single computer will become a computer cluster with a certain scale. At this time, the application range of computer network technology is more extensive. Finally, the computer network technology information highway stage. In 1993, the United States proposed the information base construction scheme, which set off the upsurge of the construction of information superhighway and greatly promoted the application and innovation of computer network technology.

In the social development, the fundamental purpose of building a computer network is to realize the rapid and secure exchange of data and information, but the system is faced with many security problems in the operation, which are reflected in the following points: on the one hand, data theft. Data transmission, data analysis and data protection are very important functional modules of network construction, as well as the basic conditions for the application of various technologies. However, in order to achieve certain goals, some malicious attackers will use various information technologies to steal computer network data, such as using malicious connection technology to steal online banking passwords of network users, resulting in partial economic losses for users. On the other hand, data corruption. Some malicious attackers, in order to destroy the stored data, will use the data model to build an attack model, and directly attack the network system after manufacturing computer viruses, such as the frequently appearing Trojan virus is a representative attack virus, which will cause the data stored in the computer to be damaged. Therefore, after understanding the development status of computer network system, according to the basic concept of data encryption technology, this paper comprehensively studies the common data encryption technology means in computer network system, in order to provide technical support for ensuring data information security.

2. Method

2.1 Link Data Encryption

In the operation of computer network system, link data encryption technology is mainly reflected in the data transmission of communication links. Combined with the structural diagram shown in Figure 1 below, it can be seen that data transmission needs to pass through multiple communication links, and each link application needs to encrypt data information before transmission, and then decrypt it after passing through the communication link. The disadvantage of this technology is that a lot of key distribution work is required during encryption, and the decryption process needs to consume more time and energy, and even the problems of information duplication, information leakage and information loss may occur.

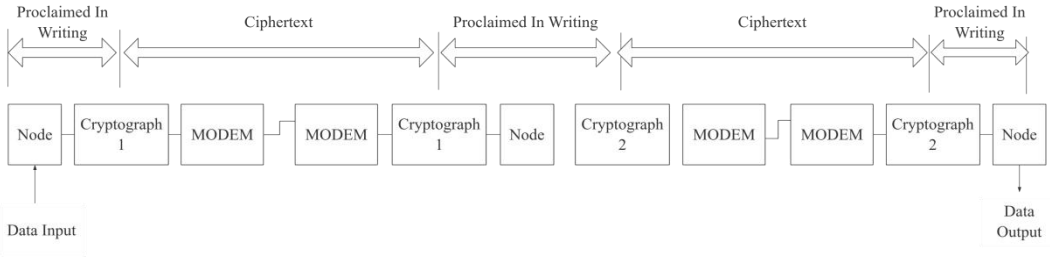

Figure 1 Structure of link data encryption

2.2 Node Data encryption

This counting method will be operated through the encrypted data transmission route, and the data will be decrypted and encrypted on the node. Based on the structural diagram shown in Figure 2 below, it can be seen that data cannot appear in plaintext at the node, and must be encrypted and decrypted in the security module. In this way, the intermediate node needs to obtain the information of processing data, and the routing information and header need to be carried out in plaintext during transmission, which will increase the difficulty of analysis to prevent communication services from being attacked.

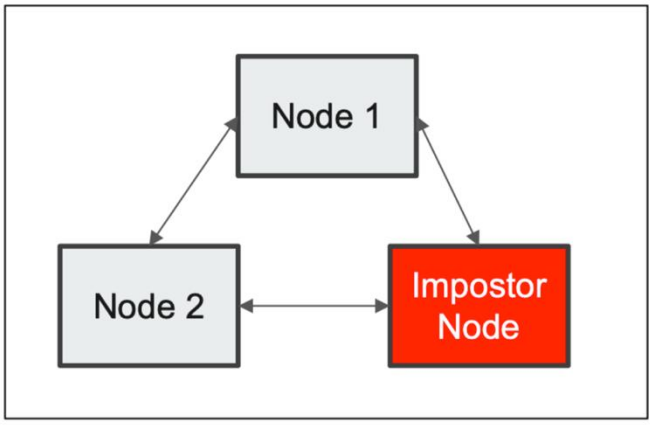

Figure 2 Structure of node data encryption

2.3 End-to-end Data encryption

In this way, all data information is encrypted during the entire data transmission process, and no decryption operation exists at any intermediate node. According to the analysis of the flow chart shown in Figure 3 below, this technology only needs to encrypt the data before transmission, and no operation is required in the transmission process. The data will be decrypted after receiving, so that the data information will be restored to the plaintext form. From the perspective of computer system operation, this technology can not cover the sending point and receiving point, and it is easy to expose the target address and origin information, thereby increasing the security risk of data transmission.

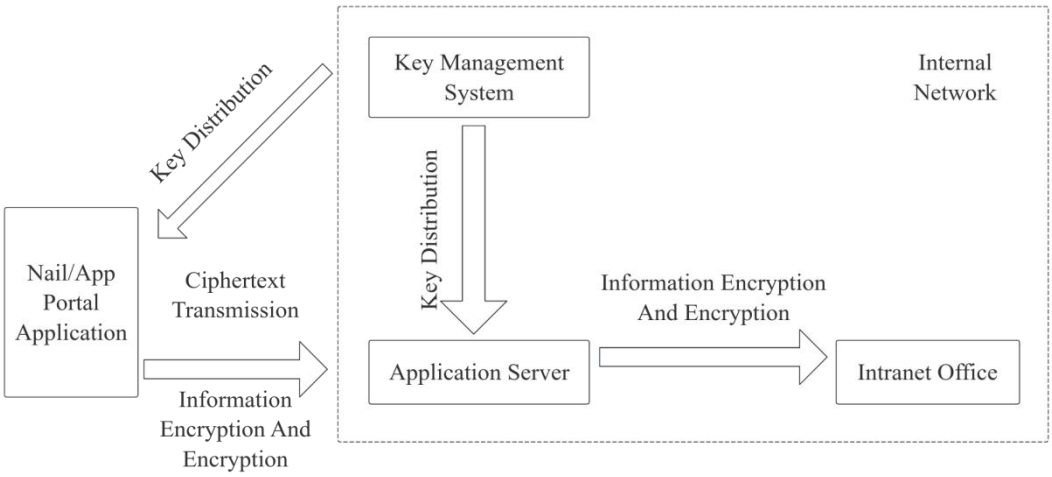

Figure 3 Flowchart of end-to-end data encryption

2.4 Identity Authentication

This technology is mainly used to identify and verify the identity of the user in the computer and computer network system, which is used to determine whether the user has the right to access and use the relevant resources. Based on the structural diagram shown in FIG. 4 below, it can be seen that identity authentication can be used in both symmetric encryption algorithms and asymmetric encryption algorithms to ensure the security of data information and effectively improve the efficiency of user identity verification. By calculating the pixel gray value corresponding to each range, the sequence code corresponding to the face image is generated according to the gray value and coordinate data, so as to ensure the user recognition effectiveness.

Figure 4 Flowchart of identity authentication

2.5 Storage Encryption

This technology converts data into a dense grain and stores it, which can effectively prevent leaks in the storage process. Combined with the data storage encryption protection flow chart shown in Figure 5 below, it not only meets the needs of integrating encryption protection capabilities into business processes, can provide effective protection for complex scenarios, but also can organically integrate with other security technologies such as access control and audit, showing strong authority control capabilities.

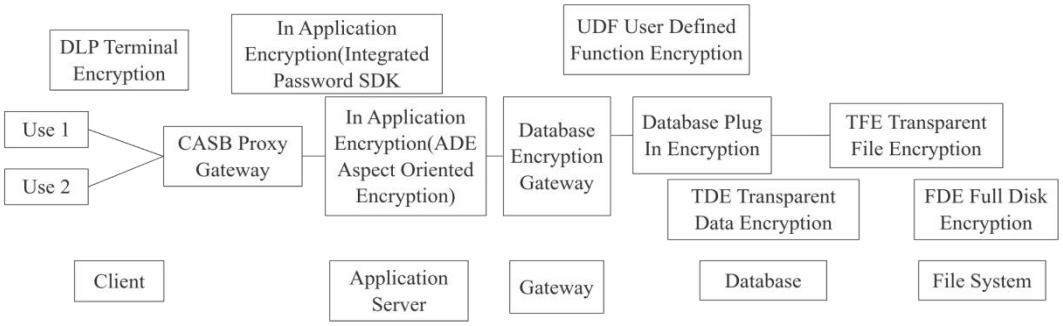

Figure 5 Flowchart of data storage encryption protection

When applying storage encryption technology, one or more combinations of storage encryption technologies should be selected according to user scenarios and requirements, and a security protection system with cryptography technology as the core and access control, audit and other security technologies integrated should be built to fundamentally ensure the security of data transmission and data storage.

3. Result analysis

In the rapid development of Internet technology, faced with more and more serious data security problems, how to meet the needs of data security at the same time, research and promotion of data encryption technology, is the main issue discussed by the academic circle in the new era. In the current social development, all kinds of data collection and processing analysis have been very common, and there are more and more cases of personal and corporate information leakage. Enterprises need to protect customer information and individuals need to protect their privacy, so the requirements for data security are getting higher and higher. As the basic component of data security technology, data encryption technology includes digital signature, asymmetric encryption, hash function, symmetric encryption and so on. As the application range of digital encryption technology is more and more wide, various fields have carried out comprehensive analysis for digital encryption and security needs, and the theoretical innovation of relevant technologies is getting faster and faster, and the future digital encryption technology will develop in the following directions: First, quantum cryptography. Quantum cryptography refers to a technology that uses the principle of quantum mechanics to encrypt data. Because the nature of quantum mechanics can ensure that no one can hack or steal data, it has become one of the more secure encryption technologies. However, there are still many difficulties in practical application, such as high-precision and high-cost technical equipment limiting the scope of application. Second, cloud-based secure computing. This technology makes use of the nature of data protection, data segmentation and node security in cloud computing, which can maximize the security performance of data calculation and storage. Finally, elliptic curve encryption. This technology will use different encryption methods, system users can choose a more secure encryption scheme, mainly the elliptic curve as the encryption algorithm, effectively reduce the key and security weakness. Nowadays, data encryption technology is widely used in technical protection, personal privacy, e-commerce, e-government and network security, etc. As the basis for realizing data security, data encryption technology should also be innovated in the face of the continuous development of various intelligent devices and network technology.

After entering the 21st century, the computer network system began to develop in the following aspects: on the one hand, high-speed mobile. With the advent of the era of big data, the transmission

volume of computer network information resources is getting higher and higher, people need more and more computer network demand, information technology and network transmission lines are becoming more and more perfect, here the construction and promotion of high-speed network provides strong support, and enhances the speed of information transmission. When the computer network technology of wireless network is fully applied, the wireless network is regarded as the basis for development, and then the computer network technology is guided to the direction of high-speed mobility, the data encryption technology should be reformed and innovated accordingly. On the other hand, automation. Nowadays, the diversity and automation of computer software development and application make the development of computer network technology more and more humanized. At the same time, the full automation of network information transmission and the excellent performance of application interface begin to guide the development of computer network technology towards intelligence and automation. Data encryption technology should also start from this aspect, and after integrating previous theoretical and technical experience, comprehensively explore how to ensure the security and effectiveness of data information, so as to lay the foundation for building a high-quality computer network system and information industry.

Conclusion

To sum up, data security, as one of the important areas of data technology research, with the continuous expansion of the application range of data encryption technology, in the face of continuous development and continuous increase of technical information, data encryption technology should also be reformed and innovative according to business needs, and more safe and effective technical means should be developed to promote the progress and development of the entire industry.

Acknowledgment

2023 Philosophy and Social Science Research Project of Hubei Provincial Department of Education:The Narrative Structure of Public Libraries Integrating into Urban Development during the Republican Era: A Case Study of Wuhan.

Reference

[1] Xiuling Zhang，Xiaogang Jiang，Huiqin Yang，Juan Sun. Application value of data encryption technology in computer network security [J]. Architectural Engineering Technology and Design, 2022, 38(1):61-63.

[2] Yajin Zhong. Application of data encryption technology in computer network security [J]. Industry & Technology Forum, 2021, 20(19):2.

[3] Hai Lin. Application value of data encryption technology in computer network security [J]. 2021(2016-12):154-156.

[4] Yu Geng Application of data encryption technology in computer network communication security [J]. Shihezi Science and Technology, 2022(4):22-23.

[5] Guobin Deng, Ping Shen. Application analysis of data encryption technology in Computer network information security [J]. Science and Technology Vision, 2022(27):55-57.

[6] Baolin Jin. Application of data encryption technology in computer network security management [J]. Electronic World, 2021(16):2.

[7] Xin Jin. Application of data encryption technology in Computer Network security [J]. Electronic Technology (Shanghai), 2022, 51(10):2.

[8] Tianzi Shen, and Gang He. Application of data encryption technology in computer network security [J]. Wireless Internet Technology, 2022, 19(8):2.

[9] Xiuling Zhang, Xiaogang Jiang, Huiqin Yang, et al. Application value of data encryption technology in Computer Network security [J]. Journal of Computer Application Abstracts, 2022(001):038.

[10] Wei He. Application of data encryption technology in computer network information security [J]. Journal of Computer Applications Abstracts, 2023, 39(12):130-132.

[11] Rongcheng Yuan, Zhengyao Gu. Application of data encryption technology in computer network information security [J]. Yangtze River Information and Communication, 2022, 35(11):69-71. (in Chinese)

[12] Fei Liu,Zhanying Shao. Application of data encryption technology in Computer Network Communication security [J]. Communication Power Supply Technology, 2023, 40(13):228-230.

[13] Penghui Liu. Application of data encryption technology in computer network security [J]. Journal of Computer Applications Abstracts, 2023, 39(3):58-60.

[14] Zhaodan Wu. Application analysis of data encryption technology in computer network security [J]. Digital Design (I), 2022, 38(2):56-58.

[15] Binsong Wei. Application of data encryption technology in Computer network security [J]. Digital Communications World, 2022(12):99-101.