ISSN 2616-5775 Vol. 4, Issue 3: 94-101, DOI: 10.25236/AJCIS.2021.040315

Research on Network Communication Data Encryption Method under the Security of Enterprise's Internal Network

Wei Li[1,2,3,*], Ding Ma[4], Limei Wang[5]

[1]*School of Railway Engineering, Zhengzhou Railway Vocational and Technical College, China*
[2]*College of Civil Engineering and Architecture, Henan University of Technology, China*
[3]*Chongqing University Industrial Technology Research Institute, China*
[4]*Marketing, Limkokwing University of Creative Technology, Malaysia*
[5]*HR, Shenzhen Jieruitong Technology Co., Ltd, China*
**Corresponding Author*

Abstract: *With the continuous development of computer communication network technology, it is inevitable to deal with various security risks in the development process. In this regard, relevant departments must pay special attention to and take active and effective preventive measures. The typical application technology is data encryption technology. Data encryption technology can effectively ensure the integrity and confidentiality of data information in the process of computer network communication. Therefore, relevant technical personnel should strengthen the research on data encryption technology and promote the healthy and orderly development of computer network communication. This article focuses on the current status of communication network security, and studies typical data encryption technologies, with a view to helping to strengthen computer network security.*

Keywords: *Network security, data encryption, network communication, wireless channel*

1. Introduction

Data encryption technology can better solve the problem of network communication security. However, there are many attack modes of attackers, which makes it difficult for the person in charge of network communication security protection to deal with it. Therefore, we need to constantly develop new encryption methods and optimize encryption technologies to protect the security of network communications and provide users with suggestions for a safer and cleaner network environment. Data encryption is widely used in all walks of life. By using different data encryption technologies, it can ensure the stability of the computer system itself, maintain data security, prevent criminals from stealing information, enable people to use network communications safely, and maximize the value of network communications.

2. Network communication and data encryption technology

2.1 Telecommunication

Network communication is a data transmission process based on transmission codes and transmission control under the support of fixed communication protocols. Common network protocols include TCP/IP, IPX/SPX under Novell, etc. [2]. For data encryption technology, data encryption technology is the basis for ensuring the reliability of computer information. After the key processes a piece of information, it transforms it according to the function rule to form a meaningless cipher-text for transmission in the network environment. The receiver restores it to meaningful information through a key or a certain rule to realize the transmission of information. In this process, data encryption technology has high requirements for the actual use environment. In network communication, it needs a designated user and a reliable key to achieve stable data transmission.

ISSN 2616-5775 Vol. 4, Issue 3: 94-101, DOI: 10.25236/AJCIS.2021.040315

2.2 Causes of cybersecurity problems

Digital encryption can ensure the safe transmission of network information. Network security is mainly to ensure the security of data transmission in the network environment. At present, with the rapid development of information technology, some information data transmission and instructions are mainly online transmission. The corresponding network communication security is directly related to the personal information security and information transmission efficiency of network users [3]. At present, there are two factors that affect network security: on the one hand, hidden security risks caused by man-made malicious operations; on the other hand, mainly hidden security risks in devices and environments. Among them, human factors have the greatest impact on the safe operation of the network environment, and human factors have various manifestations. Factors such as impersonating a user's identity, intercepting user information and tampering, or illegally invading a device are all personal safety hazards. In addition, it can also monitor the information in the user's network line. Various risk factors seriously affect the stability of network users' communications and bring certain problems to users' work and life. [5]

2.3 The importance of data encryption technology

In order to ensure the stability of network communication, data encryption technology should be used to strengthen management. Data encryption technology processes various network information to form meaningless ciphertext, which is transmitted in the network environment. Only after the receiver receives the ciphertext and decrypts it can obtain accurate information content. Under certain rules, it is converted into plain text and cipher text. By calculating the encrypted information, we call it "key". In the context of continuous development of the times, digital encryption technology plays an important role in personal work, business management, government office, people's entertainment, etc. In the information age, the network has important connections with all walks of life, but some hackers and vulnerabilities threaten the security of network communications. For example, some hackers intercepted the company's important secrets on the network, and implanted Trojans and viruses in the office system. For example, the "Panda Burning Incense" virus that once threatened the whole country has paralyzed the office system of the enterprise and affected the normal development of the enterprise. In addition, some hackers also use illegal means to steal users' online banking, QQ payment, WeChat payment, Alipay payment and other information. They use users' social networks to ask for money from relatives and friends, causing economic losses to others. The application of digital encryption technology can ensure that the data transmission process is not affected by illegal elements, and is stably transmitted to the receiver, avoiding interception of information by illegal elements and causing greater losses. Tables must appear inside the designated margins.

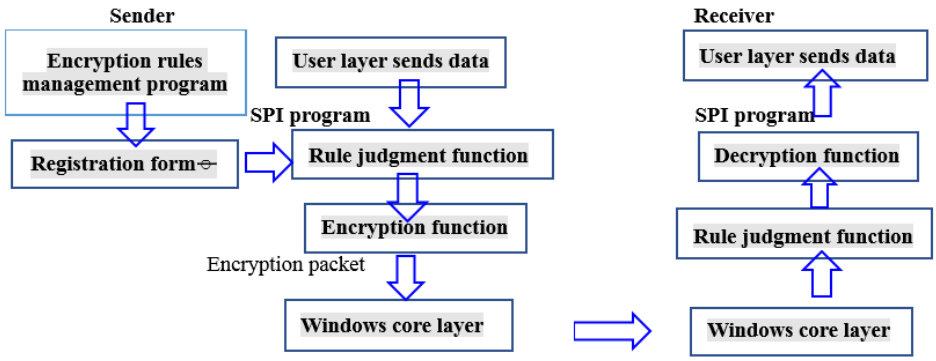

Figure 1: Network data encryption transmission model

In order to ensure the stability of network communication, data encryption technology should be used to strengthen management. Data encryption technology processes various network information to form meaningless ciphertext, which is transmitted in the network environment. Only after the receiver receives the ciphertext and decrypts it can obtain accurate information content. Under certain rules, it is converted into plain text and cipher text. By calculating the encrypted information, we call it "key". In the context of continuous development of the times, digital encryption technology plays an important role in personal work, business management, government office, people's entertainment, etc. [4]. In the information age, the network has important connections with all walks of life, but some hackers and vulnerabilities threaten the security of network communications. For example, some hackers intercepted the company's

ISSN 2616-5775 Vol. 4, Issue 3: 94-101, DOI: 10.25236/AJCIS.2021.040315

important secrets on the network, and implanted Trojans and viruses in the office system. For example, the "Panda Burning Incense" virus that once threatened the whole country has paralyzed the office system of the enterprise and affected the normal development of the enterprise. In addition, some hackers also use illegal means to steal users' online banking, QQ payment, WeChat payment, Alipay payment and other information. They use users' social networks to ask for money from relatives and friends, causing economic losses to others. [7] The application of digital encryption technology can ensure that the data transmission process is not affected by illegal elements, and is stably transmitted to the receiver, avoiding interception of information by illegal elements and causing greater losses.

3. The method of data encryption

Generally speaking, the encryption system mainly includes four parts: plain text, cipher text, encryption and decryption device and algorithm key.

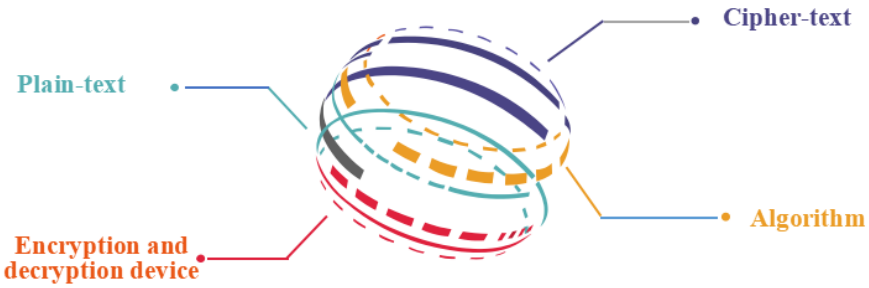

Figure 2: Encryption system

According to the characteristics of the key, data encryption can be divided into symmetric encryption and asymmetric encryption. Symmetric encryption means that both the encryption key and the decryption key use the same key. [8] The most commonly used encryption algorithms are des and AES. The key setting of symmetric encryption technology is simple and efficient, and has been widely used in daily work and life. But just because the key is too simple, the security of the key cannot be reliably guaranteed. In asymmetric key technology, the encryption key and the decryption key are different. There are two types of keys, public and private keys. The public key is for external use and contains only some public file information, while the private key is only for the user's own use, such as some important file information or personal information. The private key is used. Once the key is entered incorrectly, the user cannot open the computer system or the software itself, which greatly improves the security of the computer system to a certain extent. Therefore, although the operation of the asymmetric key is relatively complicated, it is still the most commonly used method to keep its own information safe. [9]

4. Factors of computer network communication security

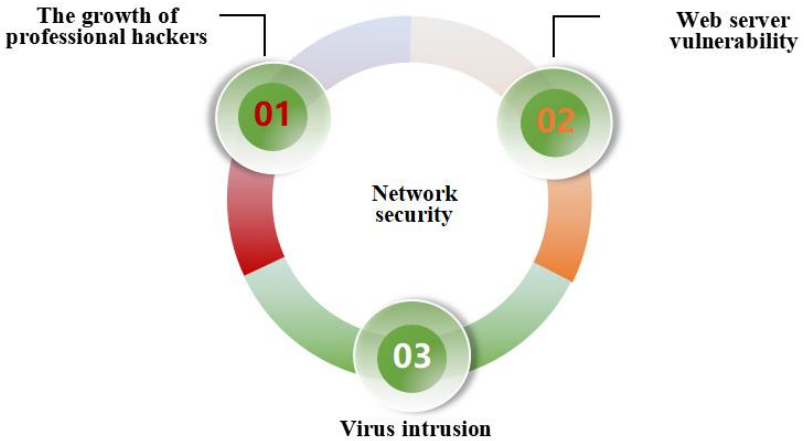

Figure 3: Factors of computer network communication security

ISSN 2616-5775 Vol. 4, Issue 3: 94-101, DOI: 10.25236/AJCIS.2021.040315

4.1 The growth of professional hackers

Internet hackers are groups that illegally steal or modify the privacy information of others. After a hacker steals other people's information, he usually does not use it for his own purposes, but monopolizes the stolen information to others and obtains benefits from it. In contemporary society, there are more and more cybercrime cases, but the age of cybercrime is getting younger and younger. Regardless of educational background, as long as the technology is high enough, someone will issue a task.

4.2 Web server vulnerability

When entering some personal information, it is difficult to ensure that only the current page receives information at the same time. Due to the usual settings or the reading function of some software, it may record the input information, resulting in information leakage. Someone seizes the technical loopholes of this network server, monitors the server with poor security, steals the user's personal information, and sells or uses it in an illegal way. It poses a great threat to the property security and privacy security of users who have leaked information [3].

4.3 Virus intrusion

Computer viruses have always been a headache for technicians and computer users. Computer viruses are spread through media such as web browsers and storage devices. It is a delayed and destructive program that usually causes computer blockage, severe computer system paralysis and straightness, resulting in the user's personal information being uploaded to the public network. It is a very notable security risk, but it is difficult to fundamentally solve the problem of computer virus transmission.

5. Data encryption technology

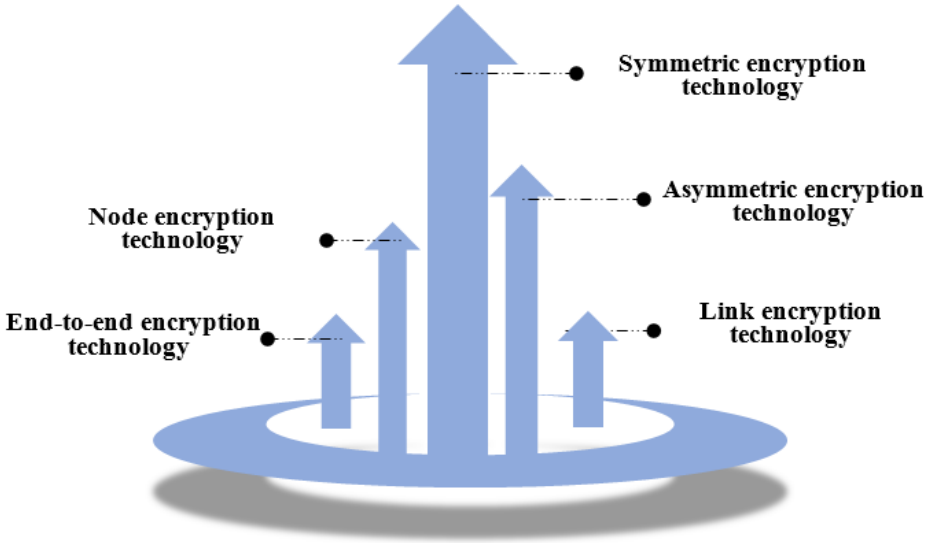

Figure 4: Data encryption technology

5.1 Symmetric encryption technology

Symmetric encryption technology is widely used in various production and life to encrypt data and use the same key. After the data is encrypted and transmitted, the receiver still needs to use the key for decryption, which is called symmetric encryption technology. In the actual operation and application of computers, symmetric encryption technology is simple and easy to understand, and can be quickly applied to data transmission, which is welcomed by the majority of network users [5]. In daily life, in order to improve the global transmission of network information, the transmission information needs to be encrypted. Only in this way can the security of information transmission be ensured, and information can be prevented from being destroyed by criminals, and information can be monitored or intercepted. In addition, symmetric encryption technology also has some problems in practical applications. If there is a problem with key management, the security of data transmission will be insufficient, which will

ISSN 2616-5775 Vol. 4, Issue 3: 94-101, DOI: 10.25236/AJCIS.2021.040315

eventually lead to a lack of security for symmetric encryption keys. [10]

5.2 Asymmetric encryption technology

Asymmetric encryption technology is characterized by different encryption and decryption methods. After one key is used for encryption, the receiver needs to use another key to decrypt and obtain information. It should be noted that asymmetric encryption has two forms: public key and private key. They are widely used in corporate communications and LAN communications. In data communication, we must pay attention to the use of public key management, public key, the use of public key to transmit information. In terms of private keys, private keys have certain confidentiality and are not open to the public. In order to ensure the stability of data information reception, when receiving the data, the receiving end needs to decrypt the data logarithmically, take the private key to decrypt, and use the data directly after decryption. In data transmission, asymmetric encryption technology can be flexibly applied to different occasions and has strong applicability. However, it takes a lot of time to support asymmetric decryption. Compared with symmetric encryption, it takes a lot of time. [11]

5.3 Node encryption technology

As for the node encryption technology, as the name suggests, the node encryption technology mainly implements the encryption protection of the node. Node encryption technology is to decrypt the data after receiving the data information, and then configure different keys for the data to securely encrypt the data node. The use of node encryption technology can effectively avoid serious accidents such as loss or theft during data transmission. In data encryption, information is transmitted in clear text, which can ensure the safe transmission of different data content at the node location. Node encryption technology has its own advantages, but there are also some shortcomings. For example, in data encryption processing using node encryption technology, the encryption devices at both ends of the node need to ensure a high degree of consistency. If there are obvious differences between the devices, the transmission cannot guarantee security. In some special cases, information may be lost, thereby affecting the stability of the system. In node encryption technology, users can ensure the confidentiality of information by setting a high complexity password. For example, in enterprise computer network communication, a company can establish its own local area network, transmit information through node encryption technology, and strengthen the strength of passwords in the form of "letters + numbers" to ensure the security of network communications. Node encryption technology is mainly to ensure that the data can be stably obtained by the intermediate nodes during the entire transmission process. In the header and routing information, clear text transmission is carried out to avoid attacks on communication services. [12]

5.4 Link encryption technology

In order to ensure the safety and reliability of computer network communication data, the information data to be transmitted can be encrypted in the communication link to ensure the stability and security of the entire transmission process. Therefore, the link encryption technology is also an online encryption technology. In actual data information transmission, different keys are used for encryption, but the information has not yet entered the entire transmission system. During the transmission process, we decrypt the network nodes and use different keys to encrypt again, which improves the data security in network communications. After the link is encrypted, the starting point and the receiving point of the data information are safely covered, and the actual frequency of the information is hidden, avoiding the vulnerability of data transmission. For example, in LAN communication, WEP encryption technology is used to implement link encryption technology. Different wireless LANs use the same key for access. WEP provides authentication support. The user connects to the AP, and the AP sends the challenge packet to the client for feedback. The client uses the shared key to feed back the data content to the location of the access point. After identity verification, get resources. In the implementation of link encryption, the control equipment should be fully synchronized to avoid affecting network performance and lighten the network communication burden. [13]

5.5 End-to-end encryption technology

In network communication, data is transmitted in the form of ciphertext. The data cannot be decrypted until it reaches the receiver. Through encryption technology, the entire transmission process can be highly protected. End-to-end encryption technology is in the state of encryption from the data source to the final destination. Using this technology, data encryption and transmission do not require other encryption

ISSN 2616-5775 Vol. 4, Issue 3: 94-101, DOI: 10.25236/AJCIS.2021.040315

processing, simple operation, and simple technical design and maintenance. The difference between encryption and synchronization will not affect the stability of the data itself, it has a trend of humanization and intelligence. However, end-to-end encryption technology has its own shortcomings, and the enhancement of the security of its sending and receiving ports requires further study. [14] In enterprise network communication, the end-to-end encryption technology for specific business content can ensure the high quality of network communication. It is mainly supported by digital signatures, digital protocols and digital certificates to ensure the security of communication information transmission at the sending end and the receiving end, avoid the loss of data transmission, and maintain the stability of the corporate network communication environment. [15]

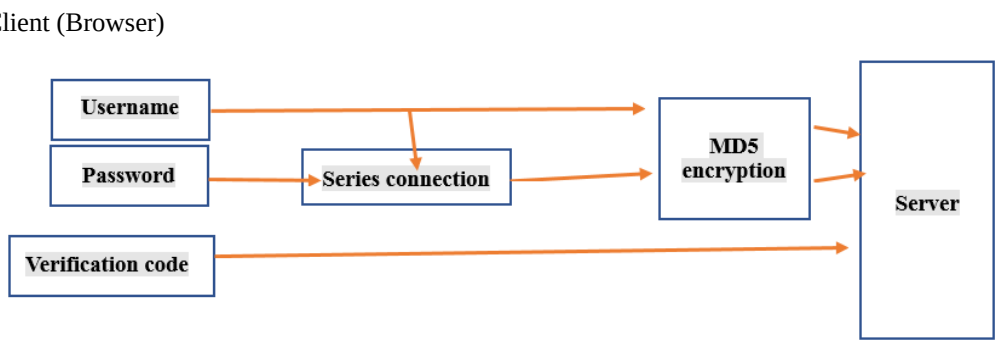

Figure 5: Communication system client encryption process flow chart

6. Application of data encryption technology in computer network security

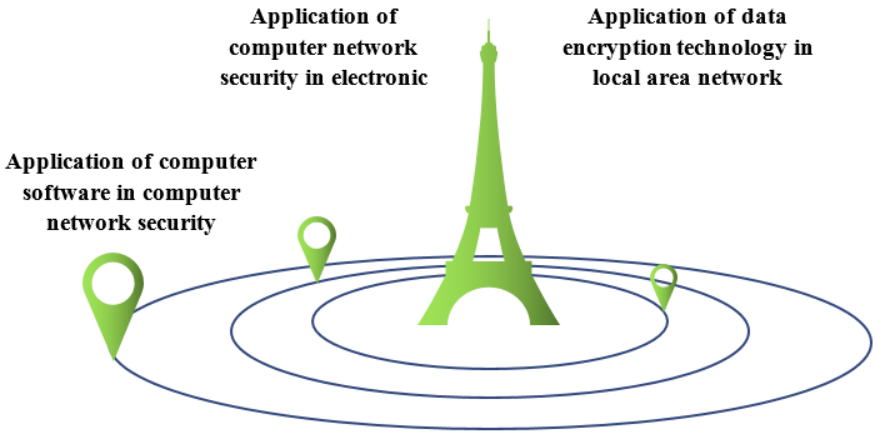

Figure 6: Application of data encryption technology in computer network security

6.1 Application of computer software in computer network security

Viruses, hackers, and other intrusions into computer software are the most common problems. Once successfully invaded the computer software, it will seriously affect the use of computer software. In order to effectively protect computer software, it is necessary to make full use of data encryption technology to maintain the effectiveness of the computer to ensure the safe and stable operation of the computer system. When data encryption technology performs security maintenance on computer system software, it is mainly reflected in the following points:(1) Password protection: When the password used by the criminals is incorrect, it is difficult to make the computer software start normally, which makes it unable to operate normally; (2) Avoid virus intrusion: encryption technology can effectively protect the computer system during virus intrusion software. [16]

6.2 Application of computer network security in electronic commerce

With the rapid development of computer network technology, computer network technology has been widely used in the process of commercial trade. In this environment, e-commerce technology came into being and has achieved rapid development. From the current development status of e-commerce, the core

ISSN 2616-5775 Vol. 4, Issue 3: 94-101, DOI: 10.25236/AJCIS.2021.040315

content of people's main concern is the security of the network environment, which is mainly due to the formation of a large amount of information data in e-commerce. It is extremely important for users and provides users with a very high value, so confidentiality requirements are high. Through the maintenance and protection of data encryption technology, it can help the development of e-commerce in a healthy direction. [17]

6.3 Application of data encryption technology in local area network

In the implementation of the corresponding development of modern enterprises in the context of the new era, in order to keep pace with the development of the era, data encryption technology has been widely used. To a large extent, it provides a guarantee for the safe operation of the enterprise. It promotes that important information within the enterprise is not leaked or stolen, so as to obtain the most effective protection for the interests of the enterprise. From the perspective of enterprise management, in order to improve the convenience and speed of data encryption technology, enterprises generally adopt the method of establishing a local area network in the enterprise environment, which can better achieve the organization of meetings and data transmission. Through the effective application of data encryption technology, the local area network can better maintain the security of the computer network and also ensure the healthy development of the enterprise. [18]

7. Conclusion

As a hot research technology, moving target tracking technology has been widely used in various fields. With the help of low cost, low power consumption, self-organization and high error tolerance of wireless sensor networks, moving target tracking based on wireless sensor networks also has broad application prospects.

Acknowledgements

This work was supported by the Technology Development of He’nan Educational Committee (Grant No. 202102310394, No. 202102310316)

References

[1] Liang Yonggang, She Yan, Liu Jianhua. Discussion on the use of "data encryption technology" to protect cultivated land based on GIS [A]. Proceedings of the 2018 Annual Conference of the Chinese Land Society [C]. 2018.
[2] Ma Ji, Wang Gang. A pseudo-attack encryption model based on fractal theory [A]. Proceedings of the Sixth Annual Conference of the Chinese Communications Society (Part 2) [C]. 2018.
[3] Wang Yanjun. Research on data encryption technology in computer network information security [J]. Communication World, 2017 (24): 24-25.
[4] Xu Xiaoyan. Analysis of the application value of data encryption technology in computer network security [J]. Journal of Jingdezhen College, 2016, 31(3): 24-26.
[5] Zheng Xiaolong, Shi Guihua. Research on data encryption technology in computer network information security [J]. Communication World, 2018 (09): 47-48.
[6] Tang Jie, Tan Jun. The specific application of data encryption technology in hospital computer network communication security [J]. China Informatization, 2018 (09): 50-52.
[7] Wu Sujuan. Application Research of Data Encryption Technology in Computer Network Security [J]. Computer Knowledge and Technology, 2017, (36): 8633-8634.
[8] Zhou Guangrui, Yu Guanjie. Discussion on the application of information encryption technology in computer network security [J]. Computer CD Software and Application, 2018, (18): 36+38.
[9] Wang Lixiang, Du Guozhen. Research on Data Encryption Technology of Computer Network [J]. Network Security Technology and Application, 2020(06): 34-35.
[10] Heng Liye. Research on Data Encryption and Abnormal Data Self-Destruction Technology in Network Information Security [J]. Network Security Technology and Application, 2020(06):35-36.
[11] Xu Dahai. Application of data encryption technology in computer network information security [J]. China New Communications, 2020, 22(10): 88-89.
[12] Wu Jingjing. Application analysis of data encryption technology in computer network security[J]. Computer Products and Circulation, 2020(06):41.

ISSN 2616-5775 Vol. 4, Issue 3: 94-101, DOI: 10.25236/AJCIS.2021.040315

[13] Li Zun, Yu Hongping. Application of data encryption technology in computer network security [J]. Computer Products and Circulation, 2020(08): 29.
[14] Chen Yuexia. Application of Data Encryption Technology in Computer Network Security [J]. Network Security Technology and Application, 2020(05): 47-48.
[15] Liu Hui. Application Research of Data Encryption Technology in Computer Network Security [J]. Fireworks Technology and Market, 2020(02): 9.
[16] Xia Xiuyan. Application analysis of data encryption technology in computer network security [J]. Digital Communication World, 2020(05): 212.
[17] Lv Shaoxin. Application of data encryption technology in information network security [J]. Communication World, 2020, 27(04): 66-67.
[18] Bai Haijun. Analysis of the application of data encryption technology in computer network security [J]. Digital Communication World, 2020(04): 115.