Journal of Electronic Research and Application

Review Article

Application Strategy of Data Encryption Technology in Computer Network Security

Yuantian Zhang[1], Wei Yang[1], Zhongxi Zhang[2]

Chongqing Electric Power College Chongqing, Chongqing 53053, China, [2]Chongqing Power Plant Chongqing Power Plant, Chongqing 400053, China

Abstract: In the context of the information age, on the basis of the convenience of computer networks, security issues have gradually emerged. The data encryption technology is reasonably applied in the process of computer network security practice, which promotes the safe and reliable operation of the computer network to a certain extent. Based on this, our article regards data encryption technology as the main research object, focusing on its specific application in computer network security.

Keywords: *computer network security; data encryption technology; application; strategy*

Publication date: September 2018

Publication online: 30th September 2018

Corresponding Author: Yuantian Zhang, Sai_mail@163.com

0 Introductions

In the process of computer working system operation, computer network plays an irreplaceable role. The interactive characteristics of communication are obvious, and the operational effect is closely related with the security of information data in computer systems. With the advancement and update of modern information technology, it provides the necessary guarantee for the development of computer network. However, the existing loopholes are increasing, which makes the computer network security seriously threatened. The probability of network security accidents is obviously improved, which is not conducive to the transmission and preservation of data information. It even has an impact on user privacy and property security. It can be seen that in-depth study and analysis of the application strategy of data encryption technology in computer network security have certain practical significance.

1 Overview of computer network security and data encryption technology

The so-called computer network security specifically refers to the comprehensive protection of the internal software, hardware, and related data information of the network system to protect against the accidental factors or malicious intrusion, resulting in the internal information data of the system being changed or leaked and seriously damaged, to realize continuous and stable operation of the network system[1]. At the same time, the network server can provide services in real time, resisting different types of network infringement, and further improve the internal information of the computer network system to be complete and confidential, so as to prevent information from being destroyed.

The so-called data encryption technology is an important technology for ensuring the security of network system information data. Based on cryptography, the explicit information is encrypted by function encryption or key encryption to ensure that this part of the information data can only be successfully cracked and used by specific people[2]. While accepting this information data in a specific group of people, the corresponding decryption method is used to effectively decrypt the information data ciphertext and to avoid other people, or the system peeks or steals the information data to ensure that the computer network information data are more secure.

2 The common factors affecting computer network security

2.1 Computer network operating system

In each and every computer, operating system occupies a central position during the operation of the computer system. Before any program runs, it must accept the processing of the operating system. If the system fails, it may easily have a direct impact on the internal program running effect of the computer, which can adversely affect the computer network security. In practice, most lawless elements use computer network operating system vulnerabilities to invade computer systems, to control the running state of the computers, or may even stealing and tampering the internal data information, else can render damage and influence the users usage of computers[3]. On this basis, some lawless elements will use the virus software to interfere or destroy the transmitted data information, resulting in a large loss of information content, stealing the user's key information, and causing them to suffer immeasurable losses. In this case, to ensure the safe and secure operation of the computer network, the most important thing is to use the relevant program software to ensure that the operating system configuration is more optimized, so as not to provide opportunities for criminals[4].

2.2 Database system management

At this stage, most of the users pay much attention to computer network security and use multiple data encryption technologies to strengthen their network security. However, when the computer database system processes data, it adopts a special method, and due to its own security risks, it also makes the computer network insecure[5]. In addition, the database system is mainly based on the hierarchical management system. If there is a problem in the database, it will inevitably have a direct impact on the effect of the computer operation, and it is difficult to ensure the user's use of the computer. This is also a common cause of computer network security incidents. Once the degree is serious, users will suffer immeasurable losses.

2.3 Computer network application

At present, the network is generally applied in various fields, and users can also query and download the required data information through the network by means of a mobile phone or a computer. However, in the process of actual use, due to the obvious openness of the network platform and the lack of standardization regarding the laws and regulations of the network environment, the probability of computer network security risks is directly increased[6]. In daily life, most users will be attacked by the network in the process of organizing and organizing computer activities, which will make the user activities unsuccessful. On this basis, there are still many criminals who use the loopholes in computer protocols and cause damage to the security of computer networks. Summary of the common factors of computer network security is briefed in Table 1.

3 The interpretation of computer network security issues

3.1 Hacking

When you actually use a computer network, you are more likely to be attacked by hackers, and this is the most common security issue. Since hackers have a high level of computer skill, it is easy to break through the ordinary firewall and invade the computer system, tampering the data information and can refer to the file content[7]. Under normal circumstances, hacker's attacks on computer networks are instructed, so it is impossible to avoid hackers from the root cause. In the process of attacking computer networks, hackers will adopt many modern technologies, and the concealment of technology is outstanding. It is difficult to find intrusion problems on time and suffer immeasurable economic losses[8].

3.2 Virus damage

Information transfer is very common in the application of computer networks. However, during transmission,

Table 1. Common factors of computer network security

Safety factor	Specific performance
Computer network operating system	Occupy the core status, it is easy to affect the internal program running of the computer, causing internal data information to be removed
Database system management	There is a security risk in itself, resulting in a lack of security in computer network operation
Computer network application	The openness of the network platform, the laws and regulations of the network environment lack standardization, which is vulnerable to make computer network security at risks

Table 2. Computer network security issues

Computer network security issues	Specific contents
Hacker attack	Break through the ordinary firewall and invade the computer system, tamper with the data information, and check the file content
Virus hazard	During the transmission, network viruses will gradually spread, affecting the use of computer networks, resulting in a large loss of internal information data.
Network defect	The network is open, and the use of new software systems makes it easier to highlight the flaws, resulting in a gradual decline in computer network security

network viruses will gradually spread, affecting the use of computer networks. Among them, ransomware and Trojan viruses are the most common types of viruses, resulting in a large amount of information loss inside the computer, or even a crash, the consequences are very serious.

3.3 Network defects

Although the openness of computer networks has had a positive impact on people, it has also led to the emergence of network problems[9]. In particular, the use of new software systems makes it easier to highlight the flaws, resulting in a gradual decline in computer network security. Summary of computer network security issues is presented in Table 2.

4 The application strategy of data encryption technology in computer network security

4.1 Link data encryption technology for network data protection

In general, for multisession computers, the goal of encryption processing can be achieved by the application of link data encryption technology. In the practice process, the corresponding information and data can be effectively divided, and the difference between the transmission path and the area is used as a reference basis to effectively encrypt the data information content. It should be noted that the encryption methods used for information transmission of different road sections are also different. Therefore, even if a virus invades the data receiving staff, the data ambiguity function can be fully utilized to completely protect the data. On this basis, in the process of using the link data encryption technology, it is also possible to fill and process the data information mainly by transmitting the information data, to ensure that the information transmission process in different sections is different, and to interfere with the judgment of the criminals, provide a solid foundation for the security of network data information.

4.2 Data encryption technology encryption software

At this stage, antivirus software has been widely used in the process of implementing computer security management. When you actually use antivirus software, you can fully protect your computer’s security. However, in the process of encrypting and processing data, the internal virus of the computer will invade the antivirus software, directly affecting the protection function of the antivirus software, and it is difficult to verify the validity of the data. In this case, when encrypting and processing data, it is necessary to check the effectiveness of the antivirus software implementation to ensure that the encrypted information does not have a virus. However, it should be noted that this type of information has high requirements of confidentiality. Therefore, data encryption technology needs to be fully utilized, and antivirus software and virus software should be encrypted to ensure the effective use of protection.

4.3 Combination of public and private keys for cryptographic key data technology

The main purpose of the application of different types of the data encryption technology is to securely protect data information, materials and optimize the effectiveness of information security protection. In general, the key components are composed of a private key and a public key. Among them, the private key refers to the information communication, both parties form a consistent recognition of the key beforehand and use the same key to encrypt and process the information on the basis of reasonable decryption, to ensure the security of the information. The so-called public key, its security level far exceeds the private key[10]. This type of key should be encrypted before sending the file, effectively avoiding the leakage of information. In addition, based on the application of the public key, it can also make up for the private key defects, ensure the encryption effect is continuously enhanced, and optimize the security of the network.

4.4 Comprehensive application of multiple data encryption technologies

At the current stage, with the rapid development of the e-commerce industry, people's productivity and daily life have been effectively improved. To fully promote the progress of the e-commerce industry, the most important thing is to create an ideal and secure network environment and promote the comprehensive and sustainable development of e-commerce. It should be noted that network transaction information security and network platform security are the main components of the e-commerce security system. Under normal circumstances, e-commerce will complete data encryption processing by means of digital certificates and digital signatures. The above-mentioned data encryption methods can play a vital role in the security of transaction information and provide protection, effectively avoiding criminals or network hackers to steal or even destroy information resources, and better realize the efficient development of the e-commerce industry.

5 Conclusion

Computer networks have a tremendous impact on people's life. Both businesses and individuals can use the network to efficiently process information and data. Network users can create private network storage space, as long as they can access the storage information, which is very convenient for users. Therefore, the data encryption technology in computer network security is very important, and it is necessary to pay great attention.

References

[1] Hai L. Application value of data encryption technology in computer network security. Heilongjiang Sci 2016;7:154-156.

[2] Xiaochun Y. Research on the application of data encryption technology in computer network security. Sci Technol Innov 2016;14:179.

[3] Yan W. Application value of data encryption technology in computer network security. Digit Technol Appl 2017.

[4] Wei P. Research on application value of data encryption technology in computer network security center. Netw Secur Technol Appl 2016;11:64.

[5] Wenjing G. Exploring the application and strategy of data encryption technology in the field of network security. Digit Commun World 2016;4.

[6] Hongjun Z. Discussion on the application strategy of data encryption technology in computer information security protection. Digit World 2018.

[7] Chen L. Application value analysis of data encryption technology in computer network security. Inf Technol 2016;7.

[8] Peng L. Application of data encryption technology in computer network communication security. Comput Program Tech Maint 2016;17:87-88.

[9] Yu G. Application analysis of data encryption technology in current computer network communication security. Sci Technol Inf 2017;15:11-12.

[10] Lixin Z. Application analysis of data encryption technologyin computer network communication security. Comput Knowl Technol Exp Skills 2017.