Research on the Application of Data Encryption Technology in Computer Security

Xiangming Zhou1,*

1College of Aviation&Tourism, Jiangxi Teachers College, China, 335000

*Corresponding author e-mail: zxm436@163.com

Abstract. With the continuous development of computer technology, computers have been integrated into our lives. It can be said that the computer Internet has brought tremendous changes to people's lives. Indeed, in many cases, the portability that the online world brings is a good aspect that we can experience. However, on the other hand, people’s computer equipment also faces many security incidents, such as network system vulnerabilities, human errors, hackers and viruses [1]. Based on this background, this article analyzes the application of data encryption technology in computers in order to provide solutions for the security of computer network equipment and software applications.

Keywords: Data Encryption, Computer, Security

1. Introduction

With the updating of science and the popularization of information technology, computer network technology has been completely covered in people's lives. It has gradually become an important technology in the process of people's social history. Its own convenience and characteristics of the times are in line with the development of contemporary information technology. However, due to its own open characteristics, people will face a lot of security risks in the actual learning and working process. The hidden danger of these computer systems is very difficult to deal with and avoid.

According to the literature review, we can find the computer security risks, including information disclosure, account and password theft, virus attack and hacker invasion. In order to alleviate and avoid the invasion of computer data by external factors, scholars have proposed a new data protection technology. This technology is known as data encryption technology[2]. Indeed, the gradual increase of computer security has also had a negative impact on the storage of network data. The emergence of data encryption technology not only effectively alleviates the frequency of security problems in computer network technology, but also protects people's important network data information to a
certain extent.

2. Simple summary of data encryption

2.1. Brief introduction of data encryption technology

According to the literal meaning of a noun, we can guess its specific meaning. Data encryption refers to that electronic equipment can use some special capabilities to effectively encrypt the data information inside the computer. After the data encryption system is added to the electronic system, people need to use the key to extract the database information\[3\]. The old data extraction process can no longer be applied to encrypted data files. Generally speaking, the key is closely related to the identity information of the staff. However, today's data encryption technology has no strict standards. At present, whether data and information can be stolen has become the basic theory of data encryption system design.

2.2. The effective value of data encryption technology in computer security

According to the above description, we can know that the computer provides people with a lot of convenient conditions for work and study. With the development of modern knowledge and the progress of computer culture, a large number of information-based data information has been created by people. After this, people began to gradually realize the security of information data. People began to focus on digital information protection technology. Therefore, the emergence of data encryption technology can be called an important reform stage of the historical development of computer technology. It can also be considered as the innovation stage of computer security system (see Figure 1).

![Figure 1. Demonstration of data encryption technology](image)

3. The important significance of the times of computer security management

3.1. The conditions of network technology

Since China's reform and opening up, in order to meet the needs of China's economy and social
cognition, we must gradually improve the network security. With the establishment of information system, we have put forward data decryption technology, virtual reality technology, cloud computing technology and data encryption technology. According to incomplete statistics, the application of these technologies has become an important driving force for China's economic growth and transformation.

3.2. The premise of data security cognition

With the improvement of people's demand for information data, people gradually realize the convenience and importance of the connotation of computer data. People gradually realize that information data is an intangible wealth. The increasing demand for network security services also reflects the degree of people's attention to network security issues. Thus, network security is a necessary issue related to national security and social stability.

3.3. Revealing the essence of network security

In fact, network security refers to the normal operation of computer system through various technical and management measures. It can ensure the integrity and confidentiality of network data. In essence, network security refers to the security of information and data in the network. From the point of view of information and control technology, it will be related to the network authenticity. From the user experience, this technology will involve personal privacy and business confidentiality issues[4]. From the level of network managers, this technology is an important safeguard measure for our network life. Generally speaking, data security is the fundamental guarantee for people's happy life and safe production.

4. Analysis of some main factors affecting the security of computer data

4.1. Security vulnerabilities

In fact, the types of computer data security vulnerabilities are many. Generally speaking, it includes the security vulnerabilities of networked intelligent devices and the vulnerabilities of the operating system of computers. The vulnerability of networked intelligent devices generally occurs in the use of the Internet of things. The update of Internet of things technology makes the frequency of security vulnerabilities of intelligent devices increase. These security risks involve a wide range of aspects. There are also many types of vulnerabilities in smart devices. Generally speaking, they include router switching equipment, networking camera equipment and intelligent transportation (see Table 1).

Table 1. Investigation of some main factors affecting the security of computer data

| Influencing factors | Main cause |
|---------------------|------------|
| The emergence of security vulnerabilities | There are no fixed vulnerabilities in the system |
| The emergence of malicious programs Hacking | Download resources from the network at will Loopholes in the network are discovered |
| External malicious information input source | Receiving USB interface of computer |
4.2. The emergence of malicious programs

In fact, the computer malicious program input mainly includes two main aspects. It is similar to the classification criteria of security vulnerabilities. It includes mobile Internet malware and smart device malware. At present, people encounter more malware is the collection of mobile Internet malware. There are many kinds of Internet information input sources. Malicious programs may be input into computer devices from external information sources. App stores, online disks, mobile hard disks and cloud disks can be the source of malicious programs. Compared with the malicious device, the probability of malicious program is not large.

4.3. Hacking

Hacker refers to the occupation of using its superb network technology to invade other computers for profit. In general, the purpose of hacker's invasion is very strong. It is also very threatening. If the hacker's invasion is successful, it will cause serious economic loss and data loss to the target enterprise. According to a large number of investigations, we can understand that the forms of hacker's invasion mainly include network attack and network investigation. We are all familiar with the concept of network attack. I don't need to explain it again here. Network investigation refers to the interception of network data. Hackers can transfer the important information of the target to their own computer through network investigation.

5. Analysis of the application of data encryption technology in computer security

5.1. Application of data encryption tools

At present, in the current computer market, we often see disc encryption technology, hardware encryption technology and compression package encryption technology. The security of CD Encryption technology is relatively high, and its operation is relatively simple[5]. It can use the image file of CD to hide the important files. Hardware encryption technology refers to the effective data protection measures at the interface of the external signal source of the computer. Compressed packet encryption technology refers to the cryptographic technology of compressed packet. We can compress some important files. After that, we can set different password locks on these packages.

5.2. The application of computer database security

We can know that the data volume of an enterprise's database is very large. These data are the property of the enterprise. Setting the encryption technology of data in the database can protect the data from being damaged or tampered by external factors. In the process of data call and input, the data encryption tool can detect the operation environment. If security risks are detected, the data encryption system will immediately force all database operations to be closed[6].

5.3. The use of digital signature authentication technology

Digital signature authentication technology is also an important part of data encryption technology. It can use encryption and decryption to check the identity information of computer users effectively. Users can use electronic pen to set up signature authentication system for important documents. In the process of extracting the file, the system needs the user to show the corresponding signature. The
computer can recognize the user's handwriting. According to different handwriting, important documents will be selected to be extracted or sealed.

6. Conclusion

According to the above description, we can know that the future of data encryption technology is very broad. Computer data is widely used in various industries in real life. Therefore, the application range of data encryption technology is also very large.

References

[1] WU Su-juan. The Research and Application of Data Encryption Technology in Computer Network Security[J]. Computer Knowledge & Technology, 2014.

[2] Feng Z , Officer Z D . Research on the Application of Data Encryption Technology of Computer Network Security[J]. Computer & Telecommunication, 2014.

[3] Xiaoli, Meng. Research on Application Value of Data Encryption Technology in Computer Network Security[C]// 2018.

[4] Wu N , Chen G . The application of data encryption technology in computer security[C]// International Conference on Materials Engineering & Information Technology Applications. 2017.

[5] Li J . Research on the Application of Data Encryption Technology in Network Security Transmission[J]. Revista De La Facultad De Ingenieria, 2017, 32(5):595-604.

[6] Rutledge L S , Hoffman L J . A survey of issues in computer network security[J]. Computers & Security, 1986, 5(4):296-308.