Research and Implementation of Computer Data Security Management System in the New Era

Peng Lu\textsuperscript{1,*}

\textsuperscript{1}Public Security Information Technology and Intelligence College, Criminal Investigation Police University of China, 110035, China

*Corresponding author e-mail: lupeng@cipuc.edu.cn

Abstract. With the popularity of the Internet, computer technology has been applied to various industries, which also requires us to deal with and manage the daily work of the computer. Therefore, data security has become an important issue, which will directly ensure the safe operation of computer Internet. Therefore, we must continue to strengthen the research of computer data security management system (hereinafter referred to as DSMS), which will better improve the security of computer data. Through the gradual improvement of reliability, data security technology has gradually met people's basic needs. However, for some special information, we must strengthen the data security management, which will prevent hackers and virus attacks. Through the DSMS, we can effectively prevent the leakage of sensitive data. Therefore, we must realize the effective management of computer data security, which needs to improve the corresponding system. By improving the computer operation ability, we can ensure the safe and reliable operation of the computer, which will bring users a safe and convenient service experience. In the new era, this paper mainly analyzes the key technology of DSMS. Then, this paper puts forward the implementation method.

Keywords: Computer, Data Security Management System, Security Management

1. Introduction

With the popularization of automation, computer has become an important office tool. However, for some important information, we must strengthen data security management, which will better protect data information [1]. Through the DSMS, we can better save information, which will eliminate a variety of security risks [2]. At present, many units have special computers, which are used to store important data. Therefore, we must strengthen the research of DSMS, which will better put an end to a variety of ways of leakage, such as mobile disk, computer data interface and so on [3]. There are many factors in computer data security management, including transmission path, radiation signal, human factors, user's own operation error and so on [4-6]. Therefore, we must strengthen the data storage software and
hardware security capabilities, which will reduce accidental or malicious data changes, destruction and leakage [7].

2. Key technologies of DSMS

2.1. File management operations

In the DSMS, only the internal U disk can read and write, while the external U disk can only read. In the DSMS, because it involves saving the summary and voucher to the external U disk, the file must be written to the external U disk at last. Therefore, we must do not internal and external U disk, which can better file management operation. In the DSMS, users can only save the internal files to be exported in the internal U disk. The administrator inserts the user's internal and external u disks into the IOT management host at the same time [8]. Through the management program, we can find the internal and external U disk. If only one of the internal and external u disks is inserted, the system will return to the beginning. At the same time, the DSMS can prompt the administrator that the external or internal USB flash disk is not inserted; if the internal or external USB flash disk is found, the file summary under the internal disk will be extracted. By writing to the external disk state transition, we can get the file certificate from the client, which can transfer the file from the internal disk to the external disk on the management side. When the file is transferred successfully, the external U disk will be changed to non-writable [9]. The implementation process of file management operation is shown in Figure 1.

![Figure 1. File management operation execution process.](image-url)

2.2. Encryption and decryption technology

In order to ensure the high security of the export process of internal file authentication, a variety of data encryption technologies are used in the DSMS, Des key is too short, 3DES speed is too slow, idea has weak key. Compared with the previous symmetric key algorithm, AES algorithm has many advantages,
such as fast encryption and decryption, small space occupation, parallel computing, which will be more suitable for the implementation of processors and special chips [10]. Therefore, AES is a better choice. RSA can carry out digital signature and key exchange operation. This paper analyzes the flow chart of hash calculation, as shown in Figure 2.

![Flow chart of hash calculation](image)

**Figure 2.** Flow chart of hash calculation.

2.3. **Verification technology of conversion times**

The purpose of conversion verification is to prevent the user from saving the certificate. After the validity period of the certificate, the conversion times verification technology adjusts the system time to before the validity period, which can export the saved certificate to the file without authorization module. DSMS can prevent such attacks, which is equivalent to the number of certificate conversion and validity [11]. When the number of conversions or expired vouchers is exceeded, the system cannot export the file. The conversion times file is composed of file content summary, conversion times and summary verification. The frame format is shown in Figure 3.

![Frame format of conversion times file](image)

**Figure 3.** Frame format of conversion times file.

2.4. **Certificate technology**

Abstract and voucher are introduced into the system to complete the authentication process of exporting internal files, which is the key point of the system to safely export files. Compared with the certificate technology in digital signature authentication, the certificate technology used in DSMS can not only realize the certificate functions of identity authentication, signature verification and validity check, but
also verify the number of system conversion. DSMS can effectively prevent attackers from tampering with the system time [12].

3. Implementation of computer DSMS

3.1. Data storage

The magnetic disk array in computer DSMS can connect multiple disks or ordinary hard disks, which can form an array. Therefore, DSMS can ensure the speed, accuracy and security of disk data reading and writing. The DSMS has a dual fault-tolerant device, which can ensure that the data is not lost. At the same time, the dual fault-tolerant device can keep the system running, which can provide services and data for the network system. The computer DSMS can form a storage system coordinated with the work, which can manage the data dynamically. Therefore, the computer DSMS has the function of remote disaster recovery, which can protect a variety of data. When the production center is paralyzed, the backup center can take over in time, which can ensure the uninterrupted service. At the same time, the data storage layer of the computer DSMS uses the spring JDBC framework to build the mapping between Java objects and associated databases. In the program layer, the DSMS will design corresponding persistent Java classes, which can be provided to each corresponding data table. In Das mode, the secret text storage technology can create the storage attribute of the corresponding ciphertext retrieval code. The data interaction of the program will be carried out through spring JDBC and persistent Java objects. In the persistence layer, spring JDBC transforms persistent objects into SQL statements in the JDBC layer. Through JDBC, we can save the data in the database, which can load the data from the database into the corresponding Java objects. Therefore, the computer DSMS can save, delete and query data.

3.2. Data security transmission and anti leakage

In the process of data transmission, transmission security is divided into five aspects: message authentication security, check sum security, check sum security, secure message integrity coding and complete non repudiation technology. Generally, the leakage ways of computer data and files are divided into three categories, which are in the process of using data and files, in the state of storage and in the state of transmission. For the safe transmission of data and anti leakage, the computer should do a good job in the triple protection of anti leakage, including detailed and comprehensive operation audit, operation authorization, and transparent encryption with security and reliability. First of all, operational audit is an important foundation in the triple protection system, which is an indispensable part. Operation audit can transparent large and complex information system, which can query the operation and behavior in the system. According to the importance of filing, we can establish a safety protection system for filing. The DSMS can flexibly control the reading, editing, copying, printing and other permissions of different users. Combined with the user's document management system, the DSMS can realize the hierarchical protection of documents. In the system, we can import the pre generated permission configuration file, which will realize the initialization of access control permission configuration process. When the user is performing an operation, we can form a request for data resources in the corresponding server, which will be processed as the role of the access control system. Therefore, users can have corresponding access rights, which can submit the request to the business logic layer. Among them, transparent encryption is the most favorable protection for important information data, which can make confidential information always in the state of encryption. Through the maximum protection of
information and data security, we can affect and change the user's operating habits. It is easy to intercept and listen on the way of transmission, which may lead to the loss and theft of the carrier containing the archive, resulting in leakage. When important documents are transmitted, we can encrypt and authorize them at the sending end, which can be transmitted through carrier or network. Therefore, only the authorized receiver can use ciphertext, which can ensure the security of users in the process of data transmission and interaction.

4. Conclusion

At present, a variety of factors can lead to computer DSMS vulnerabilities, which requires the majority of technical personnel in the discovery and understanding of the current computer DSMS problems. Combined with the causes of the problem, we can put forward the corresponding solutions, which can establish a computer data security management model. By improving the security of the system, we can reduce the loss of important computer data, which can ensure the security of computer data.

Acknowledgments

The key project of Liaoning Provincial Social Science Fund in 2020 is "A Study on the Construction Path of China's Biosecurity Intelligence Capability based on comparative Analysis of THE US Biodefense Strategy in the context of COVID-19", NO. L20ATQ00.

References

[1] Du Haili. Research and implementation of computer DSMS [J]. Computer CD software and application, 2014, 17 (23): 172-173.

[2] Li Lin, Zhang Xuzhou. Computer data security management strategies [J]. Electronic technology and software engineering, 2019 (07): 200.

[3] Liu Xin, Ma Lei, Ren Tiancheng. Research on DSMS [J]. Shandong electric power technology, 2012 (05): 49-51.

[4] Liu Yang. Research on computer operation behavior and DSMS [J]. Information communication, 2015 (12): 155-156.

[5] Tang Kaining. Data security management and maintenance of digital library network system [J]. Sci tech information, 2007 (23): 203.

[6] Xiong fan. Analysis and improvement of computer database security management [J]. Network security technology and application, 2017 (02): 81-83.

[7] Yang Yuying. Security management measures for hidden dangers of office computer data [J]. Information technology and informatization, 2014 (12): 209-210.

[8] Yin Yunfeng. Enterprise computer network data security management application [J]. Computer products and circulation, 2020 (07): 56-57.

[9] Zhang binrong, Du min, Liu Xiaolei, Liu Weihua. Analysis of computer data security
management [J]. China management information, 2014, 17 (16): 131-132.

[10] Zhang Fuhao. Design and development of Surveying and mapping DSMS [J]. Surveying and Mapping Science, 2006 (01): 77-79.

[11] Zhao Yangjie. Research and implementation of computer DSMS [J]. Information and computer (theoretical Edition), 2014 (16): 169.

[12] Zhou Ying. Computer operation behavior analysis and DSMS [J]. Information communication, 2016 (01): 153-154.