

# Research on Application Value of Data Encryption Technology in Computer Network Security

Xiaoli Meng

Xi'an International University, Shaanxi Xi'an 710077, China

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

**Abstract:** From the current status of the entire computer network security, its security issues cannot be ignored. In order to solve the various computer network security problems brought by the impact, strengthening network security has become the focus of current computer network. Data encryption technology that should be improved ensures the safety of computer networks. Based on the concept of data encryption technology, this paper analyzes the current situation of computer network security and the application of data encryption technology from a new perspective of theory and practice, and validates the data encryption technology in the current computer network security, ultimately to provide a certain theoretical reference for the current computer network security construction work.

## 1. Introduction

As the network continues to open, the degree of resource sharing becomes deeper and deeper, and the complexity of the system and the diversity of the connection cause the computer network security problem which becomes more and more prominent. In such a highly open computer network environment, the data is damaged, like the system and other problems, seriously affects the development of the computer. China has gradually strengthened its concern on the security of computer networks. Data encryption technology with its good advantages in the application of computer network security is more and more widely.

## 2. Data Encryption Technology

Data encryption technology is to ensure the safety of computer network data which is a key technology. Previous data encryption algorithms include improved substitution table algorithm, substitution table algorithm, cyclic shift and XOR operation algorithm, and cyclic redundancy check algorithm. Data encryption technology includes symmetric encryption technology and asymmetric encryption technology. Symmetric encryption technology refers to both sides of the information using the same key for encryption and decryption; this approach is the most commonly used data encryption technology [1].

## 3. The Status of Internet Security

Related studies have shown that the global computer intrusion events occur more and more frequently, which suggests that the global existence of computer network security issues [2]. Frequent computer network security problems are related to the openness of the network system and the in homogeneity of the terminal distribution. All kinds of unauthorized access, posing as legitimate users and other security issues seriously affect the normal performance of the entire computer.

From the current status of computer network security in China, regardless of hacking or computer viruses, have seriously affected China's entire computer system, and even cause a very serious social adverse effects and economic losses. For example, in January 2015 a forum in China was exposed due to the existence of security vulnerabilities, resulting in close to 23 million users of the relevant information was exposed, resulting in adverse effects and a huge panic. In April, 2015,

a certain platform of our country was exposed to the same security problem, many provinces of health and social security system, a large number of high-risk vulnerabilities, a direct threat to the relevant user information security. Even contains personal ID cards and other sensitive information, greatly reduces the confidence of our nationals on the computer network security. A variety of frequent computer network security issues are designed to reflect a problem, that is, China's computer network is very fragile. In fact, regardless of our country or other countries, computer network security, in the face of various viruses or even weak state, reflecting the computer network security is very serious. In 2015, the most cited the whole society cares Ctrip downtime, not only caused a huge economic loss Ctrip, but also to the whole society have stepped up the concern of computer network security [3].

## **4. Analysis on Application Value of Data Encryption Technology in the Computer Network Security**

### **4.1 Data encryption system design requirements and algorithms**

Data encryption technology is one of the most important technologies in the design of data encryption system, but also needs to meet certain requirements according to the characteristics of the data [3]. As mentioned above, symmetric encryption technology of data encryption technology is difficult to decipher and decrypt, but it has some shortcomings, including key distribution and management difficulties. But the public key system is relatively easy to manage [4]. In order to improve the security of key, this paper combines EKE, AES symmetric key encryption algorithm and elliptic curve public key encryption algorithm, hoping to improve the data encryption and decryption speed while ensuring the security of data information.

### **4.2 Network file encryption system communication protocol and key management**

In the development process of computer, different communication protocols are born. In the face of different situations, we need to adopt the best communication protocol. The improved EKE mode is adopted for user and server mutual authentication. And enter the communication phase is the use of elliptic curve public key system.

On the network file encryption system key management, not only includes key management, including encryption algorithms. In the past, computer network security work, before the key management mode has not yet appeared, only the use of encryption algorithm, due to the emergence of a variety of computer network security problems, the application of encryption algorithm advantage is less and less obvious. In the later development of the key management technology, and encryption algorithm will show a good combination of application performance. In this study, consider the use of AES symmetry in all aspects of encryption, which relates to the file packaging module, file encryption password, file information database. In addition, the need for the management of the key, as long as the legitimate users, even if the request to amend the password can only be submitted in the client. To achieve this goal, first need to ensure that users have been legally certified.

### **4.3 File encryption system application design**

(1) Development environment: This study uses Visual C++ development tools, which can facilitate the application of COM interface, to achieve the system function call. Visual C++ structure, including Mierosotf DeveloperStudio IDE integrated development environment. Visual C++ features include resource manipulation, application wizards, class wizards, C/C++ compilers, resource compilers, connectors, and debuggers.

(2) Management server application design and implementation: the management of the server application package, including the encrypted file. It is worth noting that the main role of the ECC module is to achieve communication between the server and the client security. A function implementation that creates a public-private key:

```
Create; // generate private key information
```

```
Vlong_to_SK (m_secretKey.sk); // Convert to private key format
Vlong_to_SK (m_secretKey.sk); // Convert to public key format
Write (m_secretKey, sizeof (SecretKey)); // Write private key information
CreatePulicKey (m_user_private_key_file_name); // Create a public key file
```

(3) The design and implementation of communication server applications: the client receives the request information, with its ECC private key to decrypt the information, which will extract user information and file information, through internal procedures to determine whether the legitimate users. If it is a legitimate user, it sends the public key encrypted file to the user.

(4) the degree of client application design and implementation: the client's main function is to decrypt the file, in short, is related to the user [6]. Use the same server for the connection-oriented TCP / IP for reliable communication. To one of the file decryption module, for example, to analyze some of its implementation function:

```
Connect (); establish a connection with the server;
InstallPublickey (); Installs the server's public key;
Installprviatekey (); Install your own private key;
Encrypt (package); encrypts the message packet with the server's public key;
```

Regarding the change of the user password, the public key module is modified by using EKE to perform bidirectional authentication, thus completing its change and transmission functions.

(5) On the file encryption system implementation process, on the server side, including registration ODBC data source, ECC module generates the server's public and private keys, generate encrypted files, start the communication server application, start network communication services.

## **5. Application Value of Data Encryption Technology in the Computer Network Security**

### **5.1 Network database**

Most of the current network database management system platform is UNIX or Microsoft, the security level is not very high [7], very easy to tamper with the useful data or password. So through the use of data encryption technology on the entire system strengthen internal and external security management.

### **5.2 Software encryption**

On the software encryption, to anti-virus software, for example, if the process of running its own program infected with a computer virus, in this case not only can not play its own effect, but also affect the security of the entire computer. Through the use of data encryption technology to effectively ensure that the need to encrypt or decrypt the file will not be infected with the virus to ensure the normal operation of the software [8].

### **5.3 E-commerce**

From the current development of China's e-commerce process and future development trend, showing good prospects for development. It is undeniable that the development of e-commerce is built on the basis of computer network security developed, the transaction between users if there are problems not only affect the development of e-commerce, but also to some extent affect social stability. Having a good computer network environment is to ensure the sustained and healthy development of e-commerce in China an effective driving force.

### **5.4 Virtual Private Network**

China's more and more institutions, enterprises will build an internal LAN, a variety of practical conditions lead to the need to use a dedicated route linking the various LANs set up a wide area network. Through the use of data encryption technology effectively ensure the information sender and receiver security, to ensure data security.

## 6. Conclusion

From computer development to the present, various computer network security problems not only affect the development of the computer, but also cause adverse social impact, which is not conducive to the good development of our society. China has gradually attached importance to its various computer network security technologies; a variety of security technology has also been an effective development. For example, identity authentication and access control technology, firewall technology, cryptography and so on. Data encryption technology, as a kind of encryption algorithm using substitution table algorithm to encrypt data, can effectively guarantee the security of computer network, and has very obvious application value.

## Acknowledgements

Shaanxi provincial science and Technology Department fund (2014jm8323).

## References

- [1] Wenya Zhu. Study on Application Value of Data Encryption Technology in Computer Network Security [J]. Manufacturing Automation, 22 (06): 35-36, 2012.
- [2] Application of Data Encryption Technology in Computer Network Security [J]. Xiaoli Li. Digital Technology and Application, 29 (06): 114 2011.
- [3] Application of Data Encryption Technology in Computer Network Security [J]. Nan Zheng, Ping Zhou. Electronic Technology and Software Engineering, 13 (01): 233 + 237, 2014.
- [4] Data encryption technology in the application of computer network security value analysis [J]. Ying Zhang. Wireless Internet technology, 29 (21): 36-37, 2015.
- [5] Application of Data Encryption Technology in Computer Network Security [J]. Ke-jia Zhao. Information Security and Technology, 32 (12): 81-82 + 85, 2015.
- [6] Data encryption technology in the application of computer network security value analysis [J]. Xiaoyan Xu. Journal of Jingdezhen University, 34 (03): 24-26, 2016.
- [7] Data encryption technology in computer network security value [J]. Xian Wu. Information and Computer, 37 (08): 150-151, 2016.
- [8] Application value analysis of data encryption technology in computer network security [J]. Sihua Zhu. Computer Knowledge and Technology, 31 (14): 36-37, 2016.