Research on Data Audit Model of Accounting Information System Based on Data Encryption

Hai Li

School of Economics and Political Science, Wenshan University, Wenshan City, Yunnan Province, 663099, China

Keywords: Data Audit Model, Accounting Information System, Data Encryption

Abstract: Accounting information data belong to the use value category of individuals, enterprises and countries. As an important branch of informatization in contemporary society, especially after the realization of accounting computerization, the problem about how to strengthen the management of accounting data security has become an issue that we cannot ignore. Therefore, establishing a set of effective data security precautions is an important issue that cannot be ignored in realizing the accounting computerization and the network of accounting information. It is the basic guarantee for the normal operation of the computer accounting information system, and directly relates to the information security of individuals, enterprises and countries. Based on the author's learning and practical experience, this paper firstly analyzed the basic principle of data encryption algorithm, then studied the data encryption algorithm, and finally proposed the application of data encryption in the data audit model.

1. Introduction

At present, accounting computerization in China has entered the network stage, that is, from the original single computer or LAN to the Internet stage. At this time, the accounting information system is based on the computer network technology platform. Because of the openness of the Internet, the security of accounting information based on it is threatened. What the computer accounting information system needs is a perfect computer accounting software and safe database security measures. These two aspects of security measures are indispensable. However, the present situation concerning data is that people tend to pay too much attention to the development of computerized accounting software, and pay great attention to the security of accounting software, while neglecting the security of the database stored in accounting. Therefore, the financial and accounting software at home and abroad is springing up like a bamboo shoots after the rain, and it is necessary to ensure the security of the data processed by the software.

2. The Basic Principle of Data Encryption Algorithm

Data encryption is a process in which data and original information are transformed into order and replaced by unidentifiable data. The purpose of data encryption is to make the person who should not know the data and information not know and recognize it. If we want to understand the content of ciphertext, we must use the inverse process of encryption to transform it into plaintext, that is, to convert ciphertext data into visible plaintext data, calling decryption process. In cryptography, the original message is called plaintext, and the encrypted result is called ciphertext. Data encryption and decryption is an inverse process, so encryption is based on encryption algorithm and encryption key. Encryption technology includes two algorithms elements and keys. Among them, the algorithm is a set of carefully designed encryption or decryption process, or it is some formulas, laws or programs. Encryption algorithm adopts encrypt plaintext and decryption algorithm uses decrypt ciphertext. In the process of encryption or decryption, the operation of the algorithm needs the control of a series of numbers. Such parameters are called keys. Corresponding keys are divided into the encryption key and decryption key. Encryption and decryption process constitute a cryptographic system, and plaintext and ciphertext are collectively referred to as

  DOI: 10.25236/iccse.18.057

messages. Any cryptographic system, no matter how complex in form, includes at least the set of plaintext, the set of keys and algorithms, in which the key and algorithm constitute the basic unit of the cryptosystem.

3. Data Encryption Algorithm

3.1 Symmetric Key Encryption Algorithm.

The symmetric encryption algorithm is also called the traditional cryptographic algorithm, that is, the encryption key can be derived from the decryption key. In most symmetric encryption algorithms, the encryption and decryption keys are the same. These algorithms are also called secret key algorithms or single secret key algorithms which require the sender and receiver to agree on a key before secure communication. The security of symmetric encryption algorithm depends on the key, which means that anyone can encrypt and decrypt the message. As long as the communication needs to be kept secret, the key must be kept secret. The characteristic of symmetric encryption algorithm is that the algorithm is open with the computation being small, the encryption speed being fast and the encryption efficiency being high. Its typical algorithms are DES algorithm, Blowfish algorithm. The encryption and decryption of the symmetric encryption algorithm are represented as follows:

$$Ek(M)=C,$$

$$Dk(C)=M.$$

Where k indicates the key, E () means encryption, and D () means decryption.

3.2 Asymmetric Key Encryption Algorithm.

The asymmetric encryption algorithm was proposed by W.Diffie and M.Hellman in 1976. The main feature of this scheme is that the encryption and decryption ability are separated by two keys. It uses two keys, public key and private key, which are used to encrypt and decrypt the data. Specifically, each user has two keys; the one is public key in the information group, which is called public key. The other is saved by the user himself, known as the private key. The public key is closely related to the private key, that is, if the data is encrypted with the public key, only the corresponding private key can be used to decrypt the data; if the data is encrypted with the private key, only the corresponding public key can be decrypted. It is impossible to solve the decryption key by the encryption key. The characteristics of asymmetric crypto system are: The intensity of the algorithm is complex; moreover, the security depends on the algorithm and the key, but the algorithm is complex, which makes the speed of encryption and decryption less fast than that of symmetric encryption and decryption. Symmetric key encryption can be divided into two cases. The one is to encrypt the data with the receiver's public key, and the other is to decrypt the data with the receiver's private key. The other is encryption with the private key of the issuer and decryption with the public key of the sender. The two have the same principle, but they are in different uses. Is represented by public key encryption as follows:

$$Ek(M)=C$$

The public key K is different from the K' private key, and the decryption can be expressed as the following formula with the corresponding private key decryption.

$$Dk'(C)=M.$$

Where K means a public key, K' denotes a private key, and E () means encryption, and D () means decryption.

4. Application of Data Encryption in Data Audit Model

Compared with the common data encryption technology, the database system has its own

requirements and characteristics. The data communication encryption between the financial software and the model is very different from the general network encryption and communication encryption. The network communication sends and receives the same continuous bit stream. No matter how long or short the information is transmitted, the key matching is continuous and corresponding in sequence. So in the process of data transmission, we adopt the typical symmetric encryption method: DES algorithm is in the database; because the length of records is usually short, the storage time of data is usually several years to several decades, and the storage time of the corresponding keys depends on the life cycle of the data. If the same key is used in the database, the encryption of the data in the database is based on the message, and the encryption and decryption are all carried out from the beginning to the end. The method of using database data in accounting information system determines that it is impossible to encrypt the whole database file. When a record that meets the search criteria is retrieved, the record must be quickly decrypted. However, in the data "audit" model, because it is not the direct function of the accounting information system, we can use a relatively complex asymmetric encryption algorithm: RSA algorithm in the data storage process.

4.1 Application of DES algorithm.

DES algorithm is a symmetric encryption algorithm, and it is also a block encryption algorithm. Its key length is 56 bits (add 8 parity bits to 64 bits, but the effective bit is still 56). The key can be an arbitrary number of bits and can be changed at any time. A very small number is considered a weak key, but it is easy to avoid them. So the confidentiality of the algorithm depends on the key. In the process of accounting information data transmission, the accounting data is divided into 64 bits by the agreed method. If not integer times, the DES is used to encrypt the 64 bit block M, which is replaced by an initial replacement IP into Mo,. Then the Mo is divided into the left half and the right half. They then perform exactly the same operations, called functions, in which the data is combined with the key. After 16 rounds, the left and right parts are replaced by one end, which completes a basic encryption process. The process is shown in figure 1:

DES uses the 64bits packaging 64bits key (excluding only 56 bits per byte of the last parity bit in 8 bytes, the plaintext is split into 32 bits left and right after initial permutation, the right data is transformed by the core function f function and the left side is XOR). In this way, after 16 rounds of transformation, the ciphertext is generated. The DES algorithm is reversible. In DES algorithm, the same function can be used to encrypt and decrypt in reverse direction. The only change is that the key must be used in reverse order during decryption. The decryption process is as follows:

$$DES^{-1}=IP^{-1}*T_1*T_2*...*T_{16}*IP(M).$$

Through the encryption of the algorithm, the transmission of accounting information data in the financial software and data "audit" model is more secure. Because of the fast speed of the algorithm, it can ensure that the synchronization of the accounting information data in the homologous database is not in big difference.

4.2 Application of RSA algorithm.

As a typical asymmetric encryption algorithm, RSA algorithm is also the earliest asymmetric key encryption algorithm. It is one of the most widely used and most influential asymmetric encryption algorithms. Its theoretical basis is the intractability of large prime numbers. Although this problem has not been fully proved in theory, RSA has withstood all kinds of attacks and has not yet been breached.

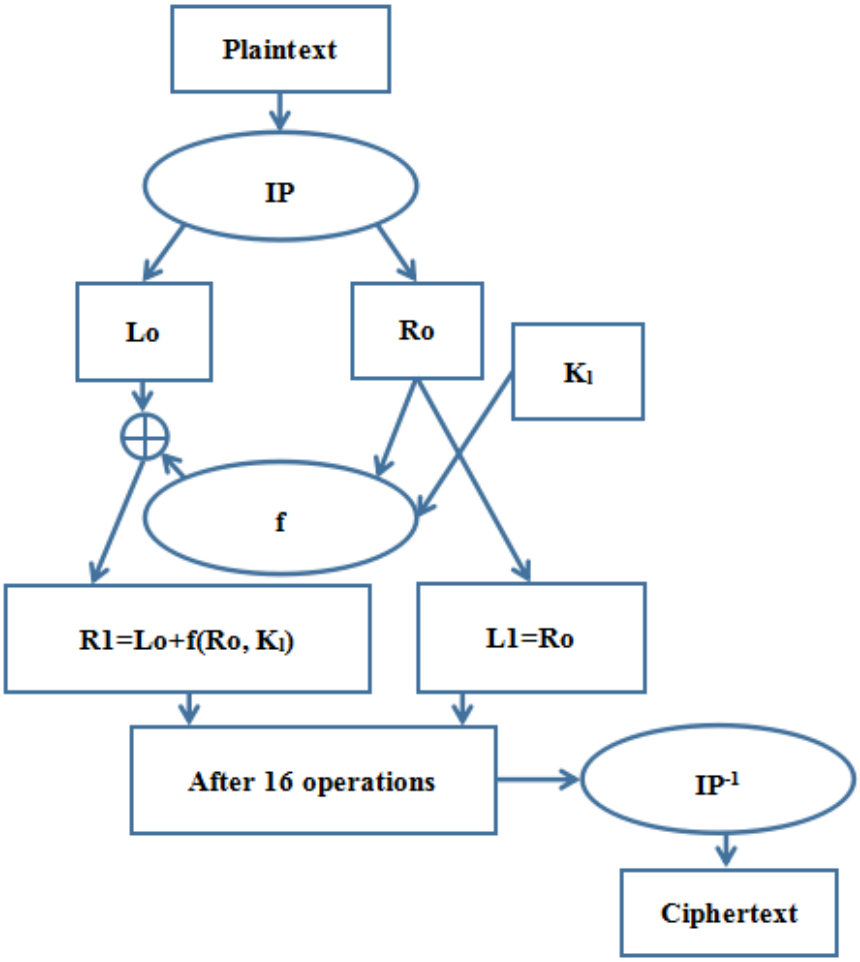

Figure 1 DES Algorithm Flow Chart

The algorithm of RSA involves three parameters, n, e1 and e2, where n is the product of two large prime numbers p and q; the number of bits occupied in the binary representation of n, that is, the so-called key length. e1 and e2 are a pair of related values. Moreover, e1 can be taken at will, but requires that it intersect with (p-1) * (q-1). When selecting e2, it requires that (e1*e2) * mod (q-1) * (q-1) = 1 (n and E1), (n and E2) is the key pair. The algorithm for RSA encryption and decryption is exactly the same. If M is plaintext and c is ciphertext, then $M=(c^{e1})$modn, $c=(M^{e1})$modn, e1 and e2 can be interchangeable, $M=(c^{e2})$modn，$c=(M^{e2})$modn. The above procedure illustrates the encryption of "digital information", and when the information is "string", you can take the ASCII value as encryption character by character. Accounting information data is stored in the data "audit" model through the complex encryption process mentioned above, so the above process ensures that the accounting information data is more secure than in the source database. The source data can be verified by using the data in the data "audit" model.

5. Summary

The concrete realization of the data audit model draws lessons from the relevant principles of the "black box", and tries to create an external closed and confidential one, except for the special interface with the financial software. There is also a database with the same structure and functions. Any operation of the source database through the financial software is transferred to the database in the model and the same operation is carried out. It can reproduce the correct recorded data when the data in the source database is broken or changed. Of course, not everyone can read the data from the "audit" model, and we need professional equipment and technology to do that.

References

[1] Zhao Yuhong. The Impact of Cloud Accounting on Audit and Its Countermeasures [J]. Research on Productivity, 2017, (01): 147-149.

[2] Qu Linlin. Research on Continuous Auditing Based on XBRL[J]. Accountant, 2014, (17): 3-4.

[3] Cheng Ping, Wen Yanhao. The Influence of Cloud Accounting on Audit and Its Countermeasures J]. Chinese Certified Public Accountant, 2013, (11): 121-124.

[4] Cheng Ping, Zhou Huan, Yang Zhounan. Analysis on the Security of Accounting Information under Cloud Accounting [J]. Friends of Accountants, 2013, (26): 28-31.

[5] Shan Guangrong. Internal Control of Accounting Information System Based on Network Environment [J]. Accounting Research, 2002, (07): 17-18.