Hindawi
Mobile Information Systems
Volume 2022, Article ID 3632298, 10 pages
https://doi.org/10.1155/2022/3632298

Research Article

The Application of Data Encryption Technology in Computer Network Communication Security

Guanxiu Liu

College of Information Technology, Shangqiu Normal University, Shangqiu 476000, Henan, China

Correspondence should be addressed to Guanxiu Liu; gxliu920@sqnu.edu.cn

Received 14 June 2022; Revised 14 July 2022; Accepted 18 July 2022; Published 29 August 2022

Academic Editor: Chia-Huei Wu

With the development of computer network and the popularization of information system, the security of databases, as platforms for centralized storage and sharing of information system data, has increasingly become a serious problem in the field of information security, so data encryption technology has come into people's sight. However, the current data encryption technology still has certain shortcomings, such as the inconsistency of the code text of the encryption and decryption technology, and the low efficiency of decoding and encryption. The purpose of this paper is to study the application of data encryption technology in computer network communication to provide better suggestions and explore better methods for improving network communication security system. This article, through the analysis of the database threat model and database application system structure, puts forward a design scheme of database encryption system model. A complete database encryption system can be divided into five logic modules: a key storage module, key engine module, key information module, key management module, and data storage module, and provides an in-depth analysis of the various parts and implementation details related to these modules. Finally, the designed encryption system model is programmed to be implemented; with the help of online examination system, the function and performance of the encryption system were tested; and the transmission efficiency of data encryption is maintained at more than 95%, which proves the effectiveness of the system.

1. Introduction

With the rapid development of semiconductor industry in the twenty-first century, computer technology is gradually popularized in the world, which promotes the arrival of the information age in the twenty-first century. Government agencies promote online office, and large enterprises and transnational corporations set up their own management systems to ensure the efficient operation of enterprises. Computers are indispensable to e-commerce, distance education, and video and audio entertainment, indicating the important role of computer technology in modern society. However, due to the universality of computer applications, the society is now threatened by data security risks. A large amount of personal information, enterprise information, and business data are leaked, which brings great inconvenience to people's work and life and causes serious consequences. In life, mobile phone applications illegally collect too much identity information; face recognition collects too large an area, resulting in a large amount of personal information leakage.

Enterprises themselves need to protect their confidential information. Individual users also exchange data through the Internet. On the one hand, they obtain useful information from the network; on the other hand, they also leave their basic personal information such as name, id number, address, and telephone number on the Internet. The database administrator has extensive access to all resources of the database and manages user accounts and permission settings. In fact, in real life, personal information has long been leaked, and new industries have been created. Specialized in the protection of information companies and engaged in data encryption and protection management, their emergence has promoted the advancement of encryption algorithm technology.

All walks of life are inseparable from the application of databases; the centralized storage and sharing of data are the characteristics of databases; databases contain more and more information. With the continuous improvement of various technologies and platforms, database security has become the focus of information security. In view of the security problems in the implementation of typical mask

data encryption standard (DES), TAO Wenqing proposed a correlation capability analysis (CPA) method combining the first two rounds of DES algorithm and selecting discrete bits of intermediate data as the objective function. The hamming weight (HW) model was used to guess the 16th round DES key and calculate the correlation between power and data HW. TAO Wenqing broke the shielded DES key by sorting the relevant values. The experimental results of using mask software to attack smart CARDS show that this method can successfully break through the 64 bit DES key [1]. Wendelin Serwe introduced two formal models of the data encryption standard (DES), one using the international standard LOTOS and the other using the newer process calculus LNT. Both models encode DES in an asynchronous circuit. The data flow block of DES algorithm is represented by the process of set communication to ensure the correctness of the model. Some of these techniques have been applied in reality, including model checking and equivalence checking. After comparing the results, the resulting prototype was automatically generated from the formal model to implement DES [2]. Liangliang Lu has designed a wireless blood pressure measurement system to facilitate the measurement of patients' blood pressure and to transmit the measurement data safely and reliably. Through PDA, radio frequency identification (RFID) technology and Bluetooth technology, patient information and data values such as blood pressure and heart rate are read. IDEA and RSA are used to encrypt the patient data and the key of IDEA algorithm to ensure the security of the patient data. The test results show that the system has high accuracy in measuring data, with safe and reliable transmission, and improves the work efficiency of nurses [3]. However, through their research, it can be found that they mainly focus on the data encryption technology in a single scenario and do not discuss the encryption technology in the overall Internet environment.

In this paper, the security of network communication is taken as the research object, and the security of database is discussed in detail. This paper makes an in-depth analysis of database encryption technology and encryption algorithm. A three-level key management scheme is designed: the primary key is the hash value of the user password, the secondary key is the user key or the public user key, and the tertiary key is the working key. The third-level secret key is encrypted through three layers, and only the administrator has the authority to change it, which can greatly improve the security of the secret key. Now, the two-dimensional array index can effectively improve the query efficiency of the numerical data in the database. In particular, for the query with fewer hit records, it has a good effect, but for the query with more hit records, it is still not ideal; this scheme has some room for improvement.

2. Proposed Method

2.1. Data Encryption Technology

2.1.1. Overview of the Database. Database security refers to protecting the database from data leakage, change, or damage caused by illegal use. A database management system can be classified according to the database model it supports, such as relational and XML model; the type of computer it supports, such as server clusters and mobile phones; the query language used, such as SQL and XQuery; the focus of performance impulse, such as the largest scale and the highest running speed; or other classification methods. The three basic factors of database security are confidentiality, availability, and data integrity [4]. Confidentiality means that only authorized users are allowed to access the data and any unauthorized users are prohibited from accessing it. The availability of the database means that authorized users can perform normal operations, the system runs stably, and can meet the needs of users for normal work. The confidentiality and availability of database are a pair of contradictions. The database encrypts the data, which means that users cannot access the data at any time. To ensure a high level of security protection, the immediacy of information acquisition is inevitably threatened, which requires a balance between confidentiality and availability [5].

2.1.2. Database Security Threats. According to the mode and nature of security attack, the factors threatening database security are classified into the following categories.

(1) Unauthorized Access to the Database. The password of the authorized user's account is leaked, and the unauthorized intruder obtains confidential information through the intercepted authorized account and tampers with the data. The authorized user obtains the downloaded data through normal access but obtains other unauthorized information, confidential information, and basic information of the database through the reasoning of accessing the data. The database in the network environment is vulnerable to the threat of Trojan virus, copying or tampering with the database, but the general database is protected by the firewall and the intrusion detection system, which can prevent the invasion of general viruses. Trojan invasion way is through the disk medium infection database host computer and its internal network, security vulnerability, and injection attack in database system. The design of the code module in the system development process is improper, which is used by the attacker or the developer who is familiar with the system, so that the attacker can bypass the access control of the database and invade the database.

(2) Human Factors. In the field of network security, there is a principle that some security threats come from outside the network, and this is also true in database systems, where threats from outside the system are much less than those from inside the system. In the current database architecture, the database administrator not only undertakes the work of maintaining the normal operation of the system but also manages user rights and user accounts. Database administrators can assign, use, and view all information about the database, including sensitive information, data tables, protected data, and more. There exists the possibility that the administrator divulges the information for personal reasons or economic interests, or the administrator illegally authorizes other users, causing unauthorized visitors to view

the protected data, which will bring serious consequences to the enterprise. This is a common problem in real database system management, which is difficult to solve in a short time [6, 7].

2.1.3. Commonly Used Data Algorithm Encryption Formula and Measures. The original idea of DES can refer to the German Enigma machine in World War II, and its basic idea is roughly the same. The traditional cipher encryption is derived from the ancient cyclic shift idea, and the Enigma machine is diffused and obscured on this basis. Data encryption methods vary. Ciphertext encrypted with certain data encryption methods can remain uncracked for centuries, while data encrypted with certain data encryption methods can be cracked in minutes or even seconds. In the digital age, people rely on data encryption technology. The use of online banking, website registration, e-mail, etc. will involve data encryption, although you do not directly perform encryption or decryption operations.

The relational expression of the data encryption function is denoted as follows:

$$C = E_k(P). \tag{1}$$

The corresponding decryption function relation expression is as follows:

$$P = D_{K1}(C). \tag{2}$$

In the relation, P is the plaintext data, C is the ciphertext data, K is the key, E_k is the encryption function using the key K, and D_{K1} is the decryption function using the key $K1$, where $K = K1$ in the symmetric key algorithm and $K \neq K1$ in the asymmetric key algorithm.

RSA's algorithm involves three parameters, W, x_1, x_2, where W is the product of M and N of two large primes, and the number of bits occupied in the binary representation of W is the key length.

RSA encryption and decryption algorithms are the same. If p is plaintext and c is ciphertext, then

$$\begin{aligned} p &= c \bullet x_1 \bmod w, \\ c &= p \bullet x_2 \bmod w, \end{aligned} \tag{3}$$

where x_1 and x_2 can be used interchangeably; namely,

$$\begin{aligned} p &= c \bullet x_2 \bmod w, \\ c &= p \bullet x_1 \bmod w. \end{aligned} \tag{4}$$

RSA public key cryptosystem is a cryptosystem that uses different encryption keys and decryption keys, and "it is computationally infeasible to derive a decryption key from a known encryption key." The traditional RSA algorithm is the BR algorithm, which represents the exponential E in (5) in binary form and then converts the exponentiation and modulus calculation into a series of square modulus and multiplicative modulus iterations; namely,

$$M = C^E \bmod N, \tag{5}$$

$$E = \sum_{i=0}^{n-1} e_i 2^i, \quad e_i = \frac{0}{1}, \tag{6}$$

$$M = \left(\left((1 \bullet C^{P_{n-1}} \bmod N)^2 \bmod N \bullet C^{P_{n-2}} \bmod N \right)^2 \bmod N \right) C^P \bmod N. \tag{7}$$

Starting from the high position of the binary representation of the exponential E, when $p_i = 1$, find the product modulus first, multiply C times the result of the previous step, and then find the square modulus; When $p_i = 0$, square the result of the previous iteration directly.

Calculation of $C^P \bmod N$ using 2^k base algorithm can be simplified into the following form:

$$C^P \bmod N = \left(\left(\left(\left(C^{P_i} \right) 2^k \bmod N \times C^{P_{i-1}} \bmod N \right) 2^k \times L \times C^{P_i} \right) 2^k \right). \tag{8}$$

After the exponent E is recoded according to the sliding window technology, $C^P \bmod N$ are simplified to the following equation:

$$C^P \bmod N = C^{5*2^{20}+7*2^{15}+3*2^9+3*2^2} \bmod N. \tag{9}$$

Calculate $C^P \bmod N$ from the highest digit of the exponent E, and simplify it to the following equation:

$$C^P \bmod N = C^{((((5*2^{5+7})*2^3+3)*2^7+3)*2^2)} \bmod N. \tag{10}$$

The so-called database security measures refer to the collection of various database security policies. These security policies include user identity and identification, access control, view, audit, and key store. It is these policies that make up the security model of the database, and the security measures in the computer are set in layers. Below, we describe the classification [8].

(1) User Identification. User identification is the outermost protection measures in the security model. This method requires the system to provide a certain way for users to identify their identity. After entering the system, the user must use various permissions according to the requirements, and also cooperate with the audit function to perform operations. The function of user identity is to identify the unique identity of the user in the database. Identification refers to the system to check whether the user's identity is legitimate. This method of user identification is relatively easy, but it is not secure, and the password is easy to be disclosed. Therefore, with the development of database applications, password authentication, digital authentication, smart card authentication, and personal identity authentication are also introduced, which improves the security of the system within a limited scope [9, 10].

(2) Access Control. Role-based access control is the association of users with permissions through roles. Simply put, a user has several roles, and each role has several permissions. In this way,

an authorization model of "user-role-authority" is constructed. In this model, there is generally a many-to-many relationship between users and roles, and between roles and permissions (functions). Role-based access control is also one of access control technologies. It connects the subject with the permission through the setting of roles. Each role can be granted permission. Authorization is accomplished when the administrator grants the user a specific role. Each user can be assigned multiple roles. After the user logs in successfully, the system will assign the user a unique session within the system. The session records the user's operation information and corresponds to the roles one by one. This authorization process is greatly simplified, with high manageability and operability [11, 12].

2.1.4. The Connection between Data Encryption and Database. With the popularization of database system application, the security of database has attracted more and more attention and become an important research direction in the development of information technology. Database security has become a problem that must be solved at present, and database encryption technology is an effective and feasible method [13, 14].

A good database encryption system should improve work efficiency as much as possible on the basis of protecting data security and achieve a balance between work efficiency and security. Generally speaking, the following requirements should be met:

(1) Encryption and decryption speed shall be fast enough to reduce the response time of data operation.

(2) The encryption is strong enough to ensure that most of the data will not be deciphered for a long time. However, encryption algorithm is not necessarily theoretically uncrackable, but in practical application, it should be able to ensure that the cost of decrypting ciphertext is greater than the significance of obtaining the data.

(3) The encryption and decryption operation are transparent to the legitimate users of the database, which will not affect the reasonable operation of users. In other words, if a user in the plaintext database system can update, add, delete data, then the user can encrypt and decrypt the database at any time.

(4) The storage capacity of the encrypted database shall not be increased to a large extent.

(5) The key management scheme is flexible, efficient, and convenient to store and use. As we all know, encryption algorithms themselves are not secret, so ensuring the security of encrypted data usually depends on the security of the key [15, 16].

2.2. Network Communication Security

2.2.1. Encryption Granularity of Data Encryption Technology in Network Communication Security. According to the structure level of the database to be encrypted, the optional encryption granularity is divided into database encryption. Inlibrary encryption includes data tables, records, fields, and data items. Each encryption granularity has its own strengths and weaknesses, which are discussed below.

(1) Database Level. Database-level encryption is the use of each database as input to the encryption system. For the database level, the database management system and the operating system use the physical block number of the database in the file system exchange, so the encryption of the database, the encryption of the operating system files, and the encryption of the read database blocks are all indexed according to the database system information table and user data table. Database encryption is easy to implement, and key management is also very simple; a database only needs a key. The most commonly used database is the query operation. The database needs to be decrypted for each frequent query, including the system information table and many irrelevant retrieval data tables. The query efficiency is very low, which may easily lead to a waste of system resources [17].

(2) Table. Table-level encryption is actually similar to database-level encryption. Data tables are encrypted as files. The reading of table information usually adopts the reading of the physical address of the stored data table, which does not support this function. Table encryption has its own advantages over database encryption: it has increased flexibility, you can choose to have the encryption requirements of the data table encryption, other tables can be managed according to the normal table of the database and query, and then the system resources can be greatly saved to a certain extent to improve the performance of the system. However, the encrypted data table may also contain some fields that do not need to be encrypted. For example, in the basic information table of users, it is necessary to encrypt the user's mobile phone number and identity account in daily life, while the encryption of name, gender, and age may have little significance [18].

(3) Record Level. Record-level encryption refers to taking a complete record in the data table as the encryption object, and the corresponding output after encryption is the ciphertext string of each field. The information contained in each record in the database has a certain degree of closure. Generally, the information contained in a record is the complete record of an entity. Record-level encryption is a common encryption granularity, which has higher flexibility and better query performance compared with table level. When encrypting, a record corresponds to a key, but the decryption process also requires the decryption of the whole record, especially the query of a single field, which is less efficient. In order to query the field value, every record needs to be decrypted, which is a heavy workload [19].

2.2.2. Key Research. The data in the database is encrypted and stored in ciphertext form. The confidentiality of the database depends on the security of encryption keys. The security management of these keys is very important to the database. This section mainly discusses the basic knowledge

of keys, including key source, key family, key cycle, and key replacement [20, 21].

Key generation requires random source, that is, key source, which is usually provided by the system by default. As a key source, the three principles of unpredictability, randomness, and unrepeatability need to be achieved [22].

(1) Unpredictability. The key source must ensure the unpredictability of the key production. If the key can be obtained in advance by pre-prediction or other means, then encryption has no effect on the database and reduces the system efficiency of the database. Unpredictability requires that even if the algorithm, the environment, and the generated key are obtained, the next key cannot be obtained by means of prediction. At the same time, the length of the key must be kept to a certain extent. If the length of the key is short, it can be deciphered by the exhaustive attack method, so that the length of the key cannot be easily deciphered; that is to say, the cost of deciphering the key cannot be lower than the value of the encrypted data [23].

(2) Randomness. Randomness requires that the creation of the key is a random process, and the rule and condition of the key generation cannot be predicted by mathematical methods such as statistics. In the computer environment, it is impossible to generate truly random numbers. The generation of random numbers is usually based on the state of the computer at that time, the time and date at that time, etc. as parameters, with the help of certain mathematical algorithms, which are periodic mathematical functions and can predict the next key through periodicity. The computer implements pseudorandom numbers, which can only be manually input. If the generation period of random numbers is as long as possible, even if the generated finite sequence with a certain length is not periodic, then the generation time is not periodic, and then the randomness can be recognized.

(3) Nonrepeatability. It requires that if the key is produced in the same environment, it is not possible to obtain the same key result. In fact, all of this is done through mathematical probability calculations, where a very small probability event is considered an unrepeatable event. For example, randomly selected characters from a string are considered unrepeatable [24, 25].

3. Experiments

3.1. Experimental Background. When using encryption technology to protect database security, a perfect design is required. Developers can use existing encryption methods for encryption and embed encryption keys into program code, but the security provided by such encryption measures is very limited. As time goes on, more users or applications need to access the database data, hence the need to constantly copy a key and add it to the new application; soon, this key will exist in many applications. Thus, an attacker's opportunities to obtain the key will increase. If an attacker can access the key, then, based on the database encryption key protection measures, it will be easy to crack. Attackers can also use some advanced tools to extract the key from the code.

Designers may embed multiple different keys in different applications, and these keys need to be replaced periodically. Obviously, the long-term maintenance associated with this encryption scheme is quite troublesome. It may not be cost-effective to make a huge maintenance effort to provide security.

Therefore, the design of a reasonable and perfect database encryption system is of great significance to the security of the database. An excellent encryption system not only ensures the security of the database, but also does not bring serious problems and has good expansibility. This paper adopts three-level encryption technology for the database encryption system and uses the advanced decryption and encryption technology of the RSA algorithm to improve the operation efficiency of the system. Finally, based on digital communication technology, the physical communication transmission of the system is encrypted and optimized.

3.2. Experimental Process. A good encryption system architecture should be flexible, modular, and able to adapt to a variety of situations. However, flexibility and modularity enhancements often mean that it is difficult to ensure system security. The design of encryption system should strive to find a balance between functionality and security. Generally speaking, the design model of an encryption system structure should be composed of five logic modules, three of which are data storage modules and the other two are key data processing modules. These modules are introduced as follows:

(1) Key storage module is used to handle the storage operation and protection measures of the master key and the working key.

(2) Key engine module is the module that really performs key addition and decryption operations.

(3) Key information module records the detailed information of the key, including key family and key cycle.

(4) Key management module manages keys in key storage module and key information module.

(5) Data storage module manages data that needs to be encrypted and protected.

The key length has great influence on the security of the key algorithm. For a certain key algorithm, the longer the key length is, the more secure it is.

For multiple key algorithms, there is no definite conclusion.

The design of the key should conform to the principle of singleness; that is, each key should be used in a single encryption process as far as possible, which should meet the following conditions:

(1) Keep the number of key uses as small as possible. Because the security of an encryption system depends on the security of the key, it is better to ensure

Table 1: Linear table corresponding experimental data.

No.	Size of clear text (bit)	Encryption index length (bit)	BR algorithm time (ms)
1	1024	128	14.5
		512	65.4
		1024	115.6
2	512	128	13.2
		512	60.2
		1024	106.2
3	256	128	12.1
		512	57.7
		1024	100.4
4	128	128	11.1
		512	54.3
		1024	97.6
5	64	128	9.6
		512	49.8
		1024	90.5

that the number of uses is kept to a minimum. Limiting the scope of key usage can reduce the number of access key entities.

(2) It shall be ensured that the amount of data in the process of key replacement is limited. In order to maintain the security of the encryption system, the key needs to be changed regularly. When the process is replaced, all data encrypted with the old key needs to be decrypted and then re-encrypted with the new key. It should be ensured that the key update process can be carried out at different times or even run in parallel, so that the process is more controllable.

(3) The amount of data encrypted with the same key should be reduced appropriately, so as to reduce the amount of information used by attackers to crack the key. It is known that plaintext attack is a kind of attack against ciphertext data. If different keys are used to encrypt the data, the amount of data used for single key encryption will be reduced, which will limit the attack to some extent.

(4) Try to control the degree of damage that may be caused by key leakage. If the key is compromised, perhaps by ill-intentioned insiders, then all data encrypted using the key will be in an insecure state. Every effort should be made to reduce the scope of this harm, except, of course, for data encrypted with a compromised key, which is not affected by the use of the same encryption key. That way, the intruder can get the user's name, but not the user's bank account.

In order to verify the encryption efficiency of the combination algorithm, in the VS2010 environment, C# programming language was used to realize the comparison program of BR algorithm, sliding window algorithm, and combination algorithm. The linear table T is created, and the code set is stored to find the linear tables X and L. In the linear table X, the encoded nonzero elements are stored, and the corresponding difference number is stored in the linear table L. According to the data provided by the linear table, RSA algorithm is used for calculation. To ensure the accuracy of the experimental results, the lengths were 128 bit, 512 bit, and 1024 bit. 50 sets of encryption operations were performed on the 256 bit and 128 bit encryption index, as shown in Table 1. As for RSA algorithm, the encryption operation and decryption operation of data are the reverse operations of each other, which are essentially the same. Therefore, in the evaluation of the algorithm, the encryption speed of different algorithms can be compared without the decryption operation.

When implementing the encryption service, analyze the file through the reserved file header to determine whether the file has been encrypted with the file encryption system. If the result is encrypted, analyze the encryption algorithm adopted. It will be triggered when the user does not specify the action to be taken; it is also triggered when implementing the encryption to check whether the encryption algorithm to be adopted conflicts with the encryption algorithm already used, as shown in Table 2.

4. Discussion

4.1. Analysis of Data Encryption under AES Algorithm. The encryption operation structure of AES consists of an AddRoundKey operation, $nr-1$ round operation, and termination round operation. The decryption structure of AES is also composed of an AddRoundKey operation, $nr-1$ turn operation, and terminating turn operation. The turn operation function is the reverse operation of the encryption operation function, and the turn operation number executed by both is the same, as shown in Figure 1.

The key scheduling process of ES algorithm is also the generation process of round key. The round key is the key Ki used in the round operation of AES algorithm in the process of encryption and decryption. Key scheduling consists of two parts: key extension and round key selection. The quantization comparison of AES algorithm's key length and data length is shown in Figure 2.

The AES algorithm key pattern is usually a combination of a basic key, some feedback, and some simple operations. The security of the algorithm depends on the basic key, but

Table 2: List of conflicts.

Project A	Project B	Conflict risk	Conflict resolution proposal
XOR	XOR	High	Get rid of A or B
DES	RSA	Low	Do not deal with them
DES	AES	Low	Do not deal with them
Add	Subtraction	Medium	Get rid of A or B
RSA	AES	Medium	Get rid of A

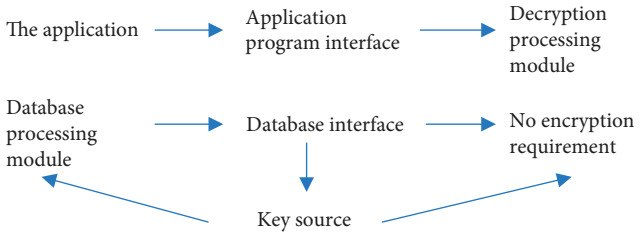

Figure 1: AES algorithm turn operation flow.

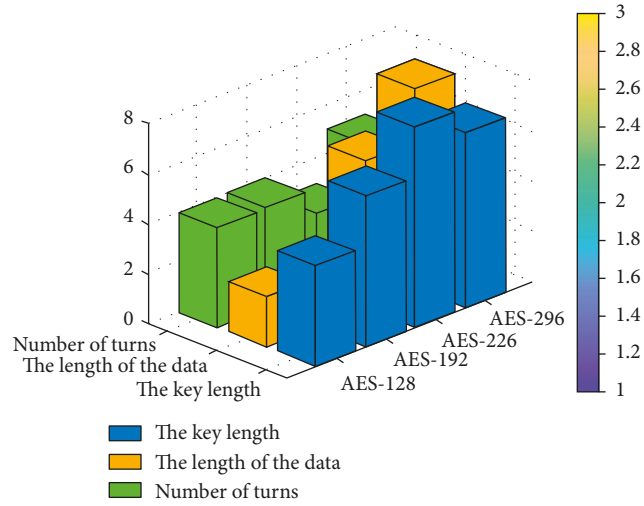

Figure 2: Quantization comparison of key length and data length of AES algorithm.

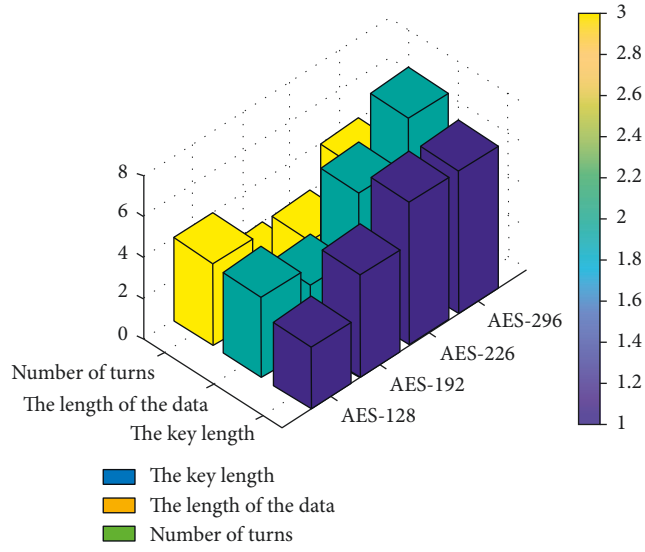

Figure 3: Quantitative comparison of key parameters in packet link mode.

not on the pattern, which will not compromise the security of the algorithm. Efficiency is the first consideration. The operation mode should not significantly reduce the efficiency of the base key. In some cases, it is important that ciphertext and plaintext are of the same size. The second thing to consider is fault tolerance. Some applications need to be encrypted or decrypted in parallel, while others need to be preprocessed as much as possible. However, in a lost or added bit ciphertext stream, it is important that the decryption process be able to recover from bit errors, and different patterns will have different subsets of characteristics. There are other security considerations: clear text patterns should be hidden; input ciphertext should be random; it should be difficult to control plaintext by introducing errors into ciphertext; and encrypting multiple messages with the same key should be allowed.

The five most commonly used modes of AES-Rijndael algorithm are electronic ciphertext (ECB), ciphertext packet link (CBC), ciphertext feedback (CFB), output feedback (OFB), and counter (CRT) mode. In this paper, the encryption system is designed in CBC mode. CBC mode has the advantages of not being vulnerable to active attacks, good security, and being suitable for long data transmission. It is the standard of SSL and IPsec.

The link adds a feedback mechanism to the block key: the encryption result of the previous block is fed back into the encryption of the current block; in other words, each block is used to modify the encryption of the next block. Each ciphertext grouping depends not only on the plaintext grouping that produced it, but also on all previous plaintext groupings. In the key packet link (CBC) mode, the plaintext is XOR with the previous ciphertext being encrypted. Figure 3 is the key program of the packet link mode of the changed data. After the plaintext of the first data packet is encrypted by the feedback register, an XOR operation will be performed. The feedback register is shown in Figure 4. As the input of the next encryption, the result is sent to the feedback register again, and the XOR operation is performed on the next data packet until the end. The encryption of each group depends on all previous groups.

IV is the initialization vector, which is set to make each packet data unique, so that exactly the same message can be encrypted into different ciphertext messages. It is impossible for eavesdropper to attempt to use the packet replay to attack, and it will be more difficult to create the cipher book.

4.2. Key Information and Database Design Analysis. You can assume that the key information module is a table in the database; of course, it can also be a file in the server; the server needs to access the data in the background operation, and it can be very convenient to access the table. But bringing convenience to access means being more vulnerable to attacks. Although the keys are safely stored in the key store, key information data is stored in the same database, so

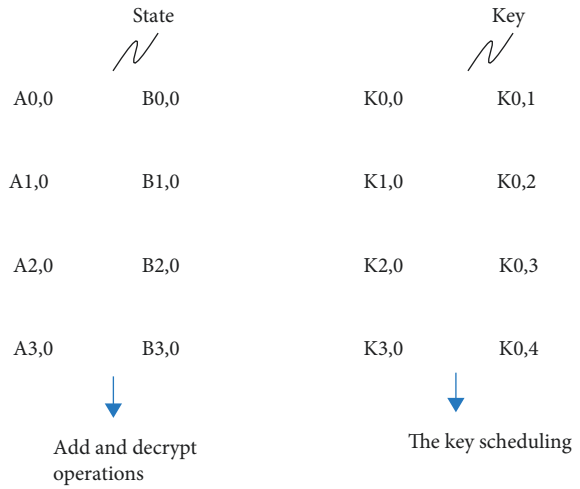

Figure 4: Operation flow of encryption operation under AES algorithm.

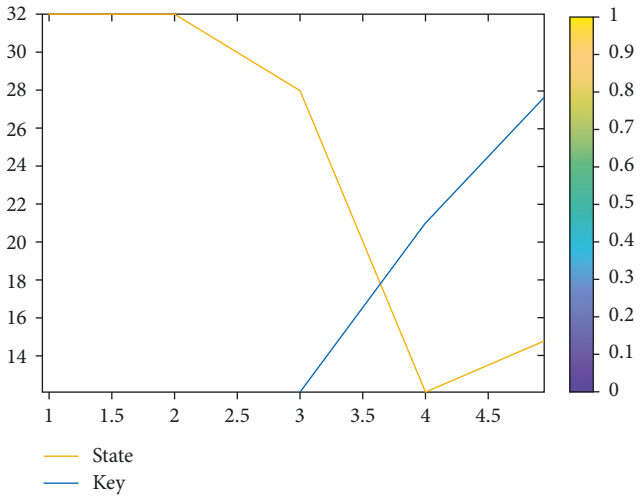

Figure 5: Test data changes under different encryption modes.

for offline attacks, do not worry too much, the encrypted information stored in the key information table is not threatened under any circumstances. However, if it is an online attack, the situation is different, because an online attack may change the data in the key information table. There is no need to worry that tampering with the data will cause damage, so the system will recover from the backup; there is always the threat of an online attacker destroying the data, and we did not design the encryption specifically for that threat.

In key data table, also known as key store, the KEY_ID column is the primary key used to uniquely determine the keys in the key store, and the KEY_DATA column stores the encrypted key, which is encrypted with the MASTERKEY, which represents the MASTERKEY used for KEY_ID encryption. The key encryption key is stored in a separate table (MASTERKEY_STORE). The type of column in which these keys are stored is a small binary type (TINYBLOB), as shown in Figure 5.

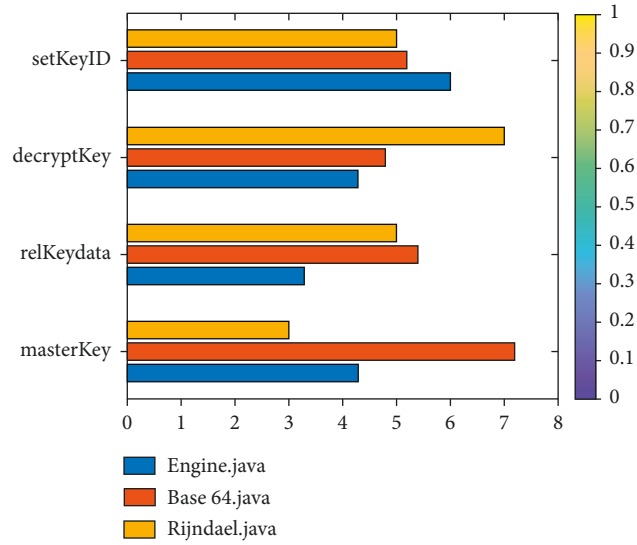

Figure 6: Comparison of key storage module indexes.

A primary key is the primary key used to encrypt the user key. The master key is the MD5 value generated by the user password. Each user will have their own password, a user primary key, so as to ensure that the user's private data cannot be accessed by other users; MD5 value security according to the database access control; and user rights to control the administrator's rights. The secondary key is the user key, and the user key is a 128 bit key assigned to the user by the administrator when the user successfully registers to the system. The primary key is used as the key, which is encrypted by AES encryption algorithm and stored in the user key table. The three-level key is the working key, which is actually used to encrypt the fields in the data table. The three-level key also adopts AES encryption algorithm, and the secondary key is stored in the working key table The comparison of various index lengths is shown in Figure 6. For rights management problems, the user data table is encrypted by the work key, and the work key is encrypted by the user. User keys are encrypted using a password hash and an encryption algorithm. If the administrator does not have access to the user's key, he also has no access to the user's private database, which guarantees the user's privacy to a certain extent.

5. Conclusions

Database encryption can effectively improve the safety level of the database, maintaining the integrity of the data and confidentiality, but encrypted databases can cause a series of problems, including the data type, data length, encrypted string fuzzy matching, cryptograph query, and data integrity and consistency.

This article considers the database security and query efficiency. The use of encryption algorithm is proposed based on two-dimensional array index ciphertext query methods, and this paper adopts the three-level key management scheme to encrypt the database system and design the system

structure. This paper believes that database encryption technology has great application value and is the last line of defense of database security. Secondly, the commonly used data encryption algorithm is introduced, and the AES algorithm and mode are deeply analyzed. Then, by analyzing the basic model structure of database encryption, a solution of database encryption is proposed, and the basic module of database encryption system is designed in detail. Finally, by programming the designed encryption system model and by studying the application of data encryption technology in network security communication problems, the function and performance of the encryption system are tested to verify the effectiveness of the system.

The encryption system designed in this paper only serves as a basic model of database encryption, with few implementation details considered. If it is directly set up and used, there may be some problems, and system developers are still required to further improve the system according to the characteristics of their own database. The research topic of this paper still has some contents that are worthy of further study. Due to my limited knowledge and time, I cannot make in-depth study of these contents one by one. The contents include key distribution management, multi-algorithm and multi-platform encryption system model research, ciphertext database storage efficiency optimization, ciphertext database query optimization, transparent encryption technology, data obfuscation technology, and database validation technology.

Data Availability

This article does not cover data research. No data were used to support this study.

Conflicts of Interest

The author declares no conflicts of interest.

Acknowledgments

This work was supported by Research on the Science and Technology Development Index of Colleges and Universities in Henan Province (Item No. 22A870003).

References

[1] T. Wenqing, G. U. Xingyuan, and L. I. Jing, "Power consumption analysis method based on data encryption standard mask," *Computer Engineering*, vol. 41, no. 5, pp. 133–138, 2015.

[2] W. Serwe, "Formal specification and verification of fully asynchronous implementations of the data encryption standard," *Computer Science*, vol. 196, pp. 61–147, 2015.

[3] L. Lu, *Zhongguo yi liao qi xie za zhi = Chinese journal of medical instrumentation*, vol. 42, no. 3, pp. 180-181, 2018.

[4] C. Han, X. Yang, and W. Hu, "Chaotic reconfigurable ZCMT precoder for OFDM data encryption and PAPR reduction," *Optics Communications*, vol. 405, no. 2, pp. 12–16, 2017.

[5] A. Sultan, X. Yang, and A. E. Adnan, Hajomer, Chaotic constellation mapping for physical-layer data encryption in OFDM-PON," *IEEE Photonics Technology Letters*, vol. 30, no. 99, p. 1, 2018.

[6] S. Chen and Z. H. O. N. G. Xian-xin, "Research of cipher chip core for sensor data encryption[J]," *IEEE Sensors Journal*, vol. 16, no. 12, p. 1, 2016.

[7] C. Liang, Q. Zhang, J. Ma, and K. Li, "Research on neural network chaotic encryption algorithm in wireless network security communication," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, 151 pages, 2019.

[8] G.-jun Liu, Z. H. E. N. G. Xiao-kun, and Y. A. N. G. Hui-feng, "Research on the security partition of electric power communication network," *Electric Power Information & Communication Technology*, vol. 14, no. 8, pp. 27–32, 2016.

[9] Z. Wang and B. Fang, "Application of combined kernel function artificial intelligence algorithm in mobile communication network security authentication mechanism," *The Journal of Supercomputing*, vol. 121, no. 5, pp. 27–32, 2019.

[10] H. Hu, H. Zhang, and Y. Yang, "Security risk situation quantification method based on threat prediction for multimedia communication network," *Multimedia Tools and Applications*, vol. 77, no. 16, Article ID 21693, 2018.

[11] W. Lu, X. Zheng, and Xu Jia, "Improving physical layer security and efficiency in D2D underlay communication," *Wireless Networks*, vol. 23, no. 4, p. 78, 2018.

[12] H. Szillat and Hk. Müller-Buschbaum, "CNDO-Berechnung des 13C-NMR-Abschirmtensors von Benzen bei Wechselwirkung mit Protonen," *Isrn Gastroenterology*, vol. 262O, no. 1, pp. 369–373, 2017.

[13] O. Srinivasa, "Performance analysis of DES and triple DES," *International Journal of Computer Application*, vol. 130, no. 14, pp. 30–34, 2015.

[14] Z. Hu and K. Xiong, "A novel key scheduling scheme for AES algorithm," *Wuhan University Journal of Natural Sciences*, vol. 21, no. 2, pp. 110–114, 2016.

[15] N. Lalithamani and M. Sabrigiriraj, "Dual encryption algorithm to improve security in hand vein and palm vein-based biometric recognition," *Journal of Medical Imaging and Health Informatics*, vol. 5, no. 3, pp. 545–551, 2015.

[16] A. Malviya, R. Gupta, and S. Sharma, "A tool for protecting electronic data in centralized database using improved advance encryption standard (AES) and secure hash algorithm (SHA)," *International Journal of Computer Application*, vol. 120, no. 2, pp. 19–24, 2015.

[17] J. A. Álvarez-Cubero and P. J. Zufiria, "Zufiria. Algorithm 959: VBF: a library of C++ classes for vector boolean functions in cryptography," *ACM Transactions on Mathematical Software*, vol. 42, no. 2, pp. 1–22, 2016.

[18] H. M. Mudia and P. V. Chavan, "Fuzzy logic based image encryption for confidential data transfer using (2, 2) secret sharing scheme," *Procedia Computer Science*, vol. 78, no. 2, pp. 632–639, 2016.

[19] B. Adil and K. Karim, "Novel encryption method based on optical time-delay chaotic system and a wavelet for data transmission," *Optics & Laser Technology*, vol. 108, no. 24, pp. 162–169, 2018.

[20] V. Susukailo and Y. Lakh, *IEEE 2018 IEEE 4th International Symposium on Wireless Systems within the International Conferences on Intelligent Data Acquisition and Advanced Computing Systems (IDAACS-SWS) - Lviv*, pp. 158–161, no. 24, IEEE, Ukraine, 2018.

[21] W. Chen, G. Chen, Y. Zhao, and J Zhang, "Security vulnerability and encryption technology of computer information technology data under big data environment," *Journal of*

Physics: Conference Series, vol. 1800, no. 1, Article ID 012012, 2021.

[22] C. Wei, "Application of data encryption technology in computer network security[J]," *Journal of Physics: Conference Series*, vol. 1237, no. 23, Article ID 022049, 2019.

[23] A. Sultan, X. Yang, and A. A. E. Hajomer, "Chaotic constellation mapping for physical-layer data encryption in OFDM-PON," *IEEE Photonics Technology Letters*, vol. 99, no. 4, p. 1, 2018.

[24] Y. Zhang, W. Yang, and Z. Zhang, "Application strategy of data encryption technology in computer network security," *Electronics Research and Applications*, vol. 2, no. 5, pp. 4–10, 2018.

[25] Y. Shi, "Research on implementation method of key management based on data encryption technology," *IOP Conference Series: Materials Science and Engineering*, vol. 677, no. 4, Article ID 042018, 2019.