Hindawi
Security and Communication Networks
Volume 2021, Article ID 7578752, 10 pages
https://doi.org/10.1155/2021/7578752

Research Article

Hybrid Encryption Scheme for Hospital Financial Data Based on Noekeon Algorithm

Fei Yao

The Affiliated Wuxi Children's Hospital of Nanjing Medical University, Wuxi 214023, China

Correspondence should be addressed to Fei Yao; 220142091@seu.edu.cn

Received 30 August 2021; Revised 26 September 2021; Accepted 10 October 2021; Published 19 October 2021

Academic Editor: Jian Su

The previous encryption methods of hospital financial data have the problem of overburden. Therefore, a research study on hybrid encryption of hospital financial data based on Noekeon algorithm is proposed. From the basic principles of the Noekeon algorithm and the application and implementation of the Noekeon algorithm, a hybrid encryption scheme for hospital financial data based on the Noekeon algorithm is designed. In order to improve the security of the encryption system, the RSA algorithm is used to encrypt the encrypted content twice. The hybrid algorithm realizes the hybrid encryption of the hospital's financial data. Finally, a hybrid encryption system for hospital financial data based on Noekeon algorithm is designed. Experimental results show that this method has a higher success rate and better comprehensive performance. It not only improves the encryption efficiency of hospital financial data but also enhances the security of hospital financial data, which has greater application value.

1. Introduction

With the rapid development of computer technology and network technology, the degree of digitization and informatization has also improved, in which a large amount of hospital data has increased sharply. Now that hospitals have entered the information age, many hospitals have learned to use integrated information management systems to manage medical data and financial data, but its security is not high, and data loss often occurs. In order to solve a series of problems such as the storage of large-scale hospital financial data, cloud computing technology came into being, providing reliable support for large hospital financial data retrieval and calculation [1]. Cloud environment is a cluster composed of massive computing nodes. It can not only store large-scale hospital financial data through the cloud, but also process hospital financial data according to the parallel characteristics of the cluster and the computing performance of each node. Among a large number of hospital information data, hospital financial data is most vulnerable to attack and theft in storage and retrieval [2, 3]. Therefore, the privacy protection of hospital financial data is not only an urgent problem to be solved in the operation of large hospital financial data, but also a very important topic in the field of information security, which has attracted extensive attention of relevant researchers.

According to Gu [4], because there is much hospital financial data that need to be encrypted in the hospital financial information, the problem of poor system stability often occurs in the process of information encryption. Therefore, the hyperchaotic two-way authentication method is applied to the design of hospital financial information security encryption system. The hospital financial information security encryption system based on the hyperchaotic two-way authentication is more stable than the traditional system, but the security after application is poor. Pang [5] and others proposed an intelligent mining algorithm for homomorphic encrypted hospital financial data based on improved hybrid jumping. The nonlinear encrypted hospital financial data samples are mapped to the kernel space to solve the nonlinear problem of hospital financial data characteristics, and the hospital financial data samples encrypted in the kernel space are sparsely reconstructed. The expression of the original encrypted hospital financial data in the kernel space is obtained, the corresponding scoring mechanism is established, and the optimal

hospital financial data features are selected. The selected hospital financial data features are clustered by using the improved hybrid leapfrog hospital financial data fuzzy clustering, and the adaptive adjustment factors are set to increase the ability of hybrid leapfrog local search, using the compactness and separation degree in the fuzzy class to construct a new fitness function, obtain the threshold of the class cluster, and complete the privacy protection of homomorphic encryption. The simulation shows that the proposed algorithm can improve the convergence of clustering and improve the accuracy of hospital financial data mining. But the cost of this system is too high to be applied in large quantities. Tian [6] aims at the security and confidentiality of hospital financial data under the cloud platform environment. Based on the MapReduce distributed framework and integrating the advantages of four chaotic mapping systems, a hybrid chaotic encryption method for cloud computing is proposed. Using the chaotic sequence generated by four chaotic maps as the key, the plaintext is encrypted with multiple keys generated iteratively from the chaotic system for many times. The experimental results show that the algorithm has high execution efficiency and large key space. It can effectively resist the attack of brute force key cracking. However, the operating stability of the system is poor.

In recent years, thanks to the increasing popularity of information technology and network tools, great changes have taken place in modern people's work and life. But then, while people enjoy network services, they are also faced with severe risk of information theft. Homomorphic encryption not only has very high security, but also can be directly processed on the encrypted hospital financial data. The decryption result under this method is the same as that obtained by directly processing plaintext, which is very practical. Therefore, combined with the advantages of the current research results of hospital financial data encryption, a hybrid encryption method of hospital financial data based on Noekeon algorithm is proposed.

2. Design of Hybrid Encryption Scheme of Hospital Financial Data Based on Noekeon Algorithm

2.1. Basic Principle of Noekeon Algorithm. Noekeon algorithm is one of the commonly used symmetric encryption algorithms. It belongs to a block cipher. The packet length is 128 bits and the key length is 128 bits. The overall structure of Noekeon algorithm uses 16 rounds of SP network, each round is composed of byte rotation and linear transformation, and it is composed of 32 parallel 4-bit–4-bit S-boxes. The encryption and decryption structure of Noekeon algorithm are very similar, and each basic module algorithm is matched. [7]. Through actual testing, Noekeon algorithm can safely and effectively complete encryption and decryption operations on various operating platforms. In fact, there are many algorithms that can be used for encryption and decryption, such as symmetric and asymmetric encryption algorithms, digital signature encryption algorithms, and hash encryption algorithms. However, different algorithms are suitable for different occasions. For example, the encryption effect of asymmetric encryption algorithm is good, but the amount of calculation involved is also quite large, which is equivalent to hundred times the level of symmetric encryption algorithm. However, the storage space of the hospital financial database is often very small, and the use of asymmetric encryption algorithms in a small space obviously cannot play its role in its application. Therefore, it is more appropriate to use a symmetric encryption algorithm on the hospital financial database. In addition to the Noekeon algorithm, commonly used symmetric encryption algorithms also include DES, RSA, AES, etc. The four symmetric encryption algorithms are compared, as shown in Table 1.

2.2. Application and Implementation of Noekeon Algorithm. Noekeon algorithm has the characteristics of fast response speed, strong system adaptability, high software and hardware compatibility, and high encryption level. It has good application value in hospital financial data encryption transmission system. Specifically, when designing Noekeon algorithm, its implementation function is as follows:

```
Noekeon_Encrypt (Key, State);//Encryption function
Noekeon_Decrypt (Key, State);//Decryption function
Round (Key,State, Round_ct1, Round_ct2);//Wheel function
Gamma (State);//Gamma function module.
Theta(key, State);//Theta function module.
Pi1(State);//Shift operation module Pi1.
Pi2(State);//Shift operation module Pi2.
```

"Key" is the round key, "State" is the 128-bit intermediate variable, "Round_ct" is the round constant from hexadecimal numbers, such as 8A, 4B, 36, C7, 4D, AE, D4, 5A, 35, etc. When Noekeon algorithm is used for encryption, the round constants are selected one by one from left to right in order; when the Noekeon algorithm is used for decryption, the round constants are selected one by one from right to left in order "Gamma" is a nonlinear function module, "Theta" is a key function module, and "Pi1" and "Pi2" are shift operation modules.

2.3. Design of Hybrid Encryption Scheme for Hospital Financial Data. Figure 1 shows the encryption and decryption scheme of hospital financial data. This paper uses Noekeon algorithm for encryption and logistic chaos algorithm for interference [8]. The process of A1 is the process of using the Noekeon algorithm to encrypt the financial data of the hospital. A2 is the process of decrypting the financial data of the financial hospital. The financial data of the hospital is first encrypted through the A1 process, turning the data into garbled codes. After the A1 process is processed, the timely information is intercepted and the corresponding information cannot be obtained. When the hospital personnel need to read the information, the node password can be used to decrypt it. Using encryption and decryption methods can improve the security of hospital financial data in the

Table 1: Comparison of the addition and decryption of the four algorithms.

Algorithm	Packet length (bit)	Key length (bit)	Encryption and decryption speed (MS/10 kB)	Main application	Security
DES	64	56	2.5	Two-way authentication between IC and POS card, MAC verification of financial transaction hospital financial data packet	Dependent key is attacked by exhaustive search
AES	64	128/192/256	2	Wireless network, information security field, AES software application, etc.	High security level, advanced encryption standard
RSA	Public private key pair	1024	600	Digital signature and key management	Safe, easy to understand, and easy to implement
Noekeon	128	128	3	File content encryption and decryption	Depending on the wheel constant, it is vulnerable to sliding attack

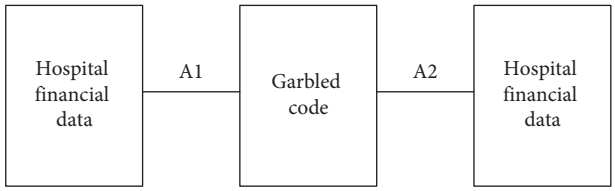

Figure 1: Scheme design of the addition and decryption of hospital financial data.

transmission process, and subsequent experiments can prove that the security of the algorithm is sufficiently reliable.

As shown in Figure 2, the block diagram of hospital financial data scrambled by Noekeon algorithm encryption and logistic chaos algorithm is introduced.

As can be seen from Figure 2, M1 represents the head of the hospital financial data body domain and SMIL domain, M2 represents the attachment part, and K represents the key. The specific encryption steps are as follows:

(1) Select M1 to perform logistic scrambling to obtain information C1

(2) Based on C1, find the attachment part m2, and then XOR encrypt m2 to obtain C4

(3) Based on C1, C2 is obtained by encrypting with key K and Noekeon algorithm

(4) The length of C2 is encrypted by Noekeon algorithm to obtain C3

The decryption process of hospital financial data is shown in Figure 2. It can be seen from the figure that the financial data and decryption process of the financial hospital are an inverse process of the encryption process. When a piece of financial data of the financial hospital is received, the tail of the financial data packet of the financial hospital is extracted to obtain the length of the financial data of the financial hospital and then decrypt the length information of the financial data of the financial hospital, divide the SMIL domain and the attachment domain, decrypt the attachment through the SMIL information and XOR decryption method, then decrypt the head and SMIL domain of the financial data domain of the hospital using the Noekeon algorithm, and decrypt the body domain and SMIL domain of the financial data of the hospital using the scrambling algorithm. Finally, all hospital financial data are merged to obtain the original hospital financial data sent by the sender. Flowchart of the financial data decryption of the financial hospital is shown in Figure 3.

3. Hybrid Encryption of Hospital Financial Data Based on Noekeon Algorithm

3.1. RSA Algorithm Principle. RSA algorithm is mainly used for further encryption of Noekeon key, and its security level is largely determined by the decomposition level of integer factor. In terms of the structure of design and implementation, RSA algorithm mainly includes three links: key generation, information encryption, and information decryption. RSA algorithm requires a large number of primes, which are all in 2048-bit level [9]. Therefore, when using RSA algorithm for information encryption, a large number of complex large numerical operations must be carried out. In this way, although RSA algorithm can effectively improve the security of hospital financial data information, its operation efficiency is inevitably at a lower level compared with other encryption algorithms. Therefore, the hospital financial data encryption transmission system should still be based on Noekeon algorithm, and only RSA algorithm is used for the encryption of Noekeon key.

In order to improve the efficiency and security of hospital financial data encryption, a hybrid encryption method of hospital financial data based on Noekeon algorithm is proposed. This paper analyzes the operation principle of RSA algorithm, parameter selection, and prime judgment, puts forward an improved RSA algorithm, and discusses the key technologies in the improvement process. Considering that RSA algorithm has strong security, but the encryption speed needs to be improved, DES algorithm is introduced to form a hybrid algorithm for homomorphic encryption of private hospital financial data sets. During the operation of the hybrid algorithm, the plaintext hospital financial data set

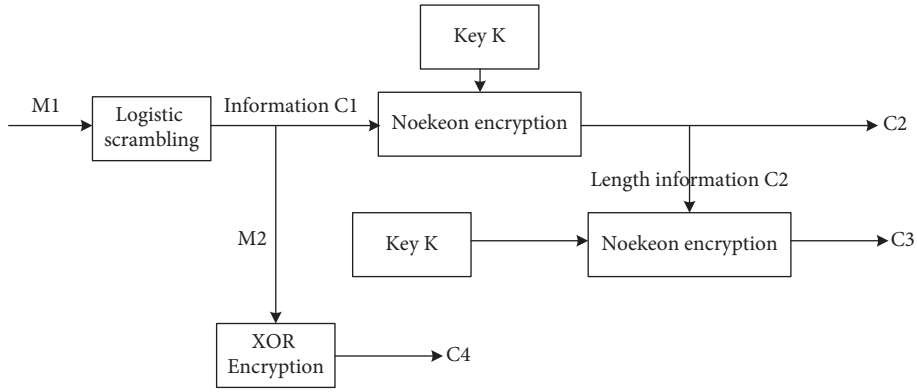

Figure 2: Box diagram after encryption and chaos of financial data of financial hospitals.

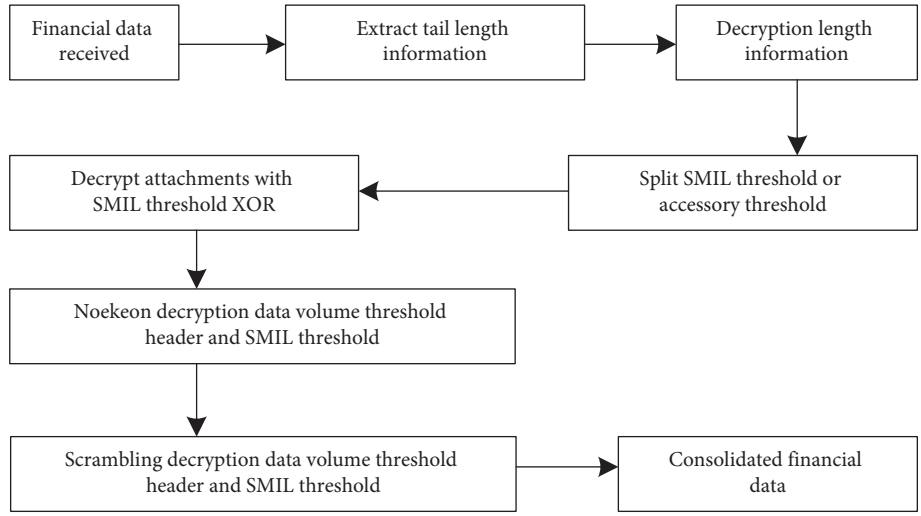

Figure 3: Flowchart of the financial data decryption of the financial hospital.

is encrypted by DES algorithm, and the key used by DES algorithm is encrypted by RSA. The packed ciphertext and the encrypted key are transmitted to the receiving end. After the receiving end obtains the hospital financial data packet, the key ciphertext is decrypted to obtain the key encrypted by DES algorithm. Because the encryption and decryption keys of DES algorithm are the same, the ciphertext decryption can be realized after obtaining the key. The experimental results show that this method has the advantages of short encryption time, strong security performance, and wide application range compared with the improved RSA algorithm. According to the experimental results, this method has strong reliability and can provide support for the security protection of private hospital financial data.

3.2. RSA Algorithm and Its Improved Algorithm

3.2.1. RSA Algorithm. The principle of using RSA algorithm to encrypt hospital financial data is simpler than symmetrical encryption algorithm. The calculation used for encryption and decryption is modular power multiplication [10]. Here, it is assumed that P is plaintext and C is ciphertext. Then the sender can use $C = P^e \bmod n$ to encrypt plaintext and the receiver can use $P = C^d \bmod n$ to decrypt. e represents the public key, d represents the key, and n represents a very large integer. The detailed process is shown in Figure 4.

The encryption and decryption process of RSA algorithm is as follows:

Step 1: select two large prime numbers p, q, and $p \neq q$, $n = p \times q$, $\phi(n) = (p-1) \times (q-1)$

Step 2: select prime $e\,(1 < e < \phi(n))$, where e and $\phi(n)$ are mutually prime

Step 3: take (e, n) as the public key and encrypt the plaintext according to formula $C = P^e \bmod n$

Step 4: calculate the private key $d = e^{-1} \bmod \phi(n)$; decrypt the ciphertext according to $P = C^d \bmod n$

In the above steps, e and n are public and everyone can know, but $\phi(n)$ is the key and needs to be kept confidential. When $\phi(n)$ is obtained, the security of the RRSA algorithm will be greatly weakened. The security of RSA algorithm is

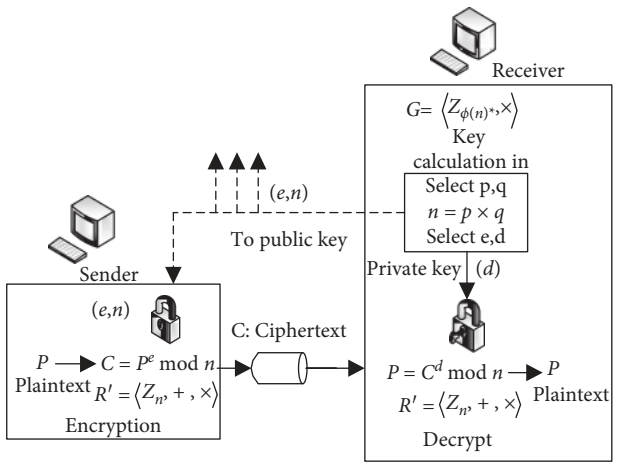

Figure 4: Schematic diagram of the RSA algorithm encryption and decryption and key generation.

directly related to the length of p and q. The longer the length, the higher the security. Therefore, the length of p and q in practical application is at least 512 bits.

3.2.2. Parameter Selection. RSA algorithm is the first encryption algorithm that relies on factor decomposition for system security. It can be predicted that if n can be decomposed very easily, the RSA algorithm is no longer secure. In conclusion, it can be considered that RSA security and factor decomposition are equivalent. This means that the selection of public key n is very important in the running process of RSA algorithm. The following are the selection principles of parameters n, e, and d.

(1) Parameter n Selection. In this process, the n value should be large enough, which is the most fundamental principle to ensure the security performance of RSA algorithm. It must be ensured that the decomposition n cannot be carried out in calculation. For the purpose of ensuring the security of the algorithm, the length of the generated large prime number should be at least a decimal number above 100 bits, and the n can be more than 200 bits [11].

Under the above constraints, $n = p \times q$, p and q are preferably strong prime numbers. Among them, strong prime numbers can be defined as follows:

Condition 1: there are large prime numbers p_1 and p_2, which can make $p_1 | (p-1)$ and $p_2 | (p+1)$

Condition 2: there are large prime numbers r_1, r_2, s_1, and s_2, which can make $r_1 | (p_1 - 1)$, $s_1 | (p_1 + 1)$, $r_2 | (p_2 - 1)$, and $s_2 | (p_2 + 1)$

Finally, the difference between p and q should be large, and the maximum common factor of $p-1$ and $q-1$ should be small enough. Assuming that the difference between p and q is very small, $(p+q)/2 \approx \sqrt{n}$ can be established. Since the basic mathematical principle $((p+q)/2)^2 - n = ((p+q)/2)^2$ is established, the values of p and q can be calculated by substituting the values of the above formula into the following formula.

(2) Parameter e Selection. During the operation of RSA algorithm, e only needs to meet $\gcd(e, \phi(n)) = 1$, which means that e can be selected randomly. According to the basic principle of encryption, the smaller the e value, the smaller the encryption time. Therefore, relevant scholars suggest that the smaller e, the better. However, practice shows that decimal e can trigger security problems. To sum up, in actual operation, the conditions to be followed for parameter e selection are as follows:

Condition 1: e cannot be too small. Considering the efficiency and security of hospital financial data encryption, it is best to select a prime number with a length of 16

Condition 2: in the process of selecting parameter e, the module with the largest order $\phi(n)$ should be selected; that is, the smallest i in $e^i = 1 \bmod \phi(n)$ should be $((p-1)(q-1))/2$

(3) Parameter d Selection. d as the key should be greater than $n^{1/4}$. In practical application, it is hoped to improve the decryption or signature efficiency according to the small number d. When e is determined, d can be obtained based on Euclidean algorithm. In conclusion, assuming that the length of d is less than $n^{1/4}$, the parameter d can be obtained efficiently only by mathematical algorithm.

3.2.3. Prime Judgment. In the running process of RSA algorithm, arbitrarily generating large prime numbers is a necessary operation. Because the p and q digits can determine the security of RSA algorithm, it is a difficult problem to quickly solve the problem of large prime generation.

Prime number determination is done using improved Miller Rabin algorithm [12]. In the process, considering that arbitrarily generated large integers are time-consuming in prime judgment, it is necessary to filter out some relatively significant composite numbers before transmitting large integers to the degree of prime judgment [13, 14]. The even number and the number with 5 as the mantissa are excluded first, then divide the decimal by the large number, select 53 small prime numbers, and divide the large integer. The detailed process is as follows:

Step 1: arbitrarily generate a large integer n

Step 2: select a group of prime arrays with a length of 53 from 2 and record the array as $a[i]$

Step 3: $i = 0$

Step 4: when $i < 53$, calculate $y = n \bmod a[i]$

Step 5: if $y = 0$ is assumed, it means that it can be divisible and is not a prime number. On the contrary, if $i = i++$, go to Step 4

According to the improved Miller Rabin algorithm, the primality judgment is carried out for the values after the above processing. The improved prime judgment algorithm is to improve the modular power operation in Miller Rabin algorithm according to Montgomery's fast modular power method.

The expression of Montgomery method is

$$\text{Monpro}(A, B, N) = \text{ABR}^{-1} (\text{mod } N), \quad (1)$$

where R represents the power based on 2 and when R is 2^k, N needs to meet $2^{k-1} \le N < 2^k$ and $\gcd(R, N) = 1$.

3.2.4. Improved RSA algorithm. RSA algorithm has significant advantages and disadvantages. The advantages are high security performance and the disadvantages are low encryption efficiency. The time-consuming operations in the running process of RSA algorithm are generation and determination of large prime numbers and modular power calculation $c^{e'} \bmod n$. The prime judgment has been analyzed above, and the fast calculation of modular power is discussed below.

For the fast calculation of $c^{e'} \bmod n$, the sliding window method is adopted and used in RSA algorithm.

The principle of sliding window method is to modularize the index e' in $c^{e'} \bmod n$. For example, $e' = (15454855115)_{10} = (001110011001001011100101111111001011)_2$, if the length of the setting window is 3, the above binary numbers are grouped from the left, and the length of the grouping is 3 bits. The grouping principle is to ensure that the first bit of each group is 1, so part of 0 may be skipped in the middle. At the end, when the length is smaller than 3 digits, the remaining numbers form a group separately without 0 or 1 [15].

After grouping, the ways of grouping to improve the efficiency of modular exponentiation operation are analyzed. Take $a^{(1011)_2}$ as an example: $a^{(1011)_2} = a^{11} = a^{10}a = a^{(101)_2 \times 2}a$. Thus, the expression of e' can be deduced:

$$e' = 7 \times 2^{31} + 6 \times 2^{26} + 4 \times 2^{22} + 5 \times 2^{19} + 6 \times 2^{16} + 5 \times 2^{12} + 7 \times 2^9 + 7 \times 2^6 + 5 \times 2^1 + 2^0. \quad (2)$$

Simplify e' and substitute the simplified e' into $c^{e'} \bmod n$; then,

$$c^{e'} \bmod n = c^{(((((((((7\times2^5+6)\times2^4+4)2^3+5)\times2^3)+6)\times2^4+5)\times2^3+7)\times2^3+7)\times2^5+5)\times2^1+1} \bmod n. \quad (3)$$

According to the above calculation and analysis, the essence of the operation of the sliding window method is to preprocess the index, so as to reduce the amount of calculation.

3.3. Implementation of Homomorphic Encryption of the Private Hospital Financial Data Set. Considering that RSA algorithm has strong security, but the encryption speed needs to be improved, DES algorithm is introduced. The encryption speed of this algorithm is fast, but there are some problems in key management. The combination of the two algorithms can effectively complement each other.

The key used in the operation of DES algorithm is based on 56 bits, of which 8 bits are parity bits. The encryption operation is implemented for 64-bit plaintext, and 16 rounds of encoding operation are implemented for 64-bit plaintext. In each round of encoding, each 48-bit key value is obtained according to the 56-bit complete key.

Assume that plaintext m' and key k' are 64-bit 0 and 1 strings. Key MEY is only 56-bit valid, and $k'_8, k'_{16}, k'_{24}, k'_{32}, k'_{40}, k'_{48}, k'_{56}$, and k'_{64} are parity bits, which will not affect encryption. Suppose $\text{KEY} = K'_1K'_2 \cdots K'_{64}\text{MING} = M'_1M'_2 \cdots M'_{64}$, m'_i and k'_i are 0 or 1, $i = 1, 2, \cdots, 64$.

According to the above settings, the encryption process is defined as follows:

$$F_{\text{DES}}(\text{MING}) = P'^{-1} \times T_{16} \times T_{15} \times \cdots \times T_1 \times P'(\text{MING}). \quad (4)$$

Step 1: P' represents the initial transformation, P'^{-1} represents the inverse transformation of P', and both meet $IP' \times IP'^{-1} = 1$

Step 2: DES iteration

Step 3: in the subkey generation process, the original key is reordered and divided into two parts, and then the two parts of the subkey are obtained through cyclic shift. Finally, the subkey is synthesized and reordered to form the subkey

The decryption process of the encryption algorithm is similar to the encryption steps. 16 rounds of iteration can be reversed from the key sequence.

Based on the above contents, the homomorphic encryption of private hospital financial data set is realized by using hybrid algorithm. Figure 5 shows the principle of hybrid algorithm.

During the operation of the hybrid algorithm, the plaintext hospital financial data set is encrypted by DES algorithm, and the key used by DES algorithm is encrypted by RSA. The packed ciphertext and the encrypted key are transmitted to the receiving end. After the receiving end obtains the hospital financial data packet, the key ciphertext is decrypted to obtain the key encrypted by DES algorithm. Considering that the encryption key of DES algorithm is the

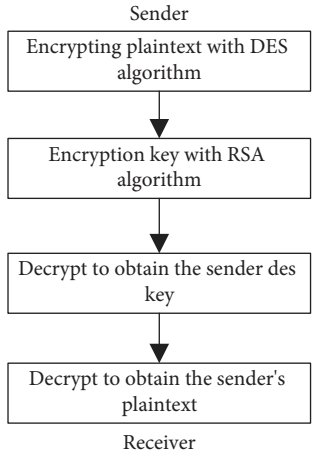

Figure 5: Principles of the hybrid algorithm.

same as that of decryption, ciphertext decryption can be realized after obtaining the key.

The mixed algorithm is implemented on the VC + + platform. Because there are many outputs involved, the MFC interface is written to realize the real-time display of state. The test file used in the implementation is. TXT file. The file encryption is realized according to DES algorithm, RSA encryption is implemented for DES algorithm key, and the encryption results are displayed by MFC interface. Here, the values of p and q of RSA algorithm are defined as 512 bits. The time consumed in the encryption process, including the key generation time of RSA algorithm, is displayed in real time on the interface. In the process of decryption, the DES algorithm key must be obtained first. Thus, in the decryption operation, first decrypt the des key encrypted by RSA and output the result, and then decrypt the file according to the key.

3.4. Design of Hybrid Encryption Interface for Hospital Financial Data Based on Noekeon Algorithm. Based on the above analysis, the hybrid encryption interface of hospital financial data based on Noekeon algorithm is designed.

3.4.1. Design Principle of Hybrid Encryption Interface. Firstly, three information bar modules that can be filled in "user key", "file opening path", and "file saving path" should be set in the main area of Noekeon encryption system interface as the operation basis of information processing and storage. Then, the two path modules should be connected with the storage disk of the computer system and the hospital financial database, and the "Browse" button should be set to facilitate users to freely select the extraction area and storage area of information. Finally, three keys of "encryption", "decryption", and "digital signature" should be set under the key information bar, and Noekeon algorithm and RSA algorithm should be set into the trigger module of the corresponding key.

In this way, users can encrypt, decrypt, and sign files or hospital financial data by operating the main interface of the hospital financial data encryption and transmission system. In addition, in order to ensure the aesthetics and practicability of the system interface, it is also necessary to design the compatibility of the layout, frame, and other appearance structures of the system interface, so as to ensure that system users such as windows 7 and MacOS can complete the interface operation quickly and accurately.

Noekeon algorithm has the characteristics of high encryption strength, fast speed, easy standardization, and easy software and hardware implementation. The main implementation functions of Noekeon algorithm are as follows:

Noekeon_ Encrypt(Key,State); Encryption function.

Noekeon_ Decrypt(Key,State); Decryption function.

Round(Key, State, Round_ ctl, Round_ ct2);//Wheel function Gamma(State);//Gamma function module.

Theta(Key,State);//Theta function module.

Pil(State); Shift operation module Pil.

Pi2(State);//Shift operation module Pi2.

In the above function, Key represents round key, State represents 128-bit intermediate variable, and Round_ct is the round constant, which is taken from the following hexadecimal numbers 80, 1B, 36, 6C, D8, AB, 4D, 9A, 2F, 5E, BC, 63, C6, 97, 35, 6A, and D4. It is selected one by one from left to right during encryption and from right to left during decryption. Gamma is a nonlinear module, theta is a key correlation module, and PIL and Pi2 are shift operation modules, where Theta, Pil, and Pi2 are diffusion layer functions.

3.4.2. Design and Implementation of RSA Algorithm. The security of RSA algorithm mainly depends on integer factorization. The implementation of RSA algorithm mainly includes three parts: key generation, hospital financial data encryption, and hospital financial data decryption. The following is the implementation process of RSA algorithm:

void rsa init(rsa_ context ∗ ctx, int padding, inthash_ id);//Generate key_ _ _

int rsa_ gen_ key(rsa_ context ∗ ctx, int (void ∗),

void ∗ p_ mg,

intnbits, int exponent);

intrsa_ public(rsa_ context ∗ ctx, const (unsigned char ∗ input, unsigned char ∗ output) "public key operation.

intrsa_ private(rsa_ context ∗ ctx, const (unsigned char ∗ input, unsigned char ∗ output) "private key operation.

Because the two large prime numbers selected by RSA algorithm are close to 2048 bits, a large number of large number addition, subtraction, multiplication, division, modulus, and modulus inverse operations need to be performed. This makes the operation efficiency of RSA very low compared with other symmetric cryptographic algorithms, which is also the reason why the system chooses RSA algorithm to exchange Noekeon keys.

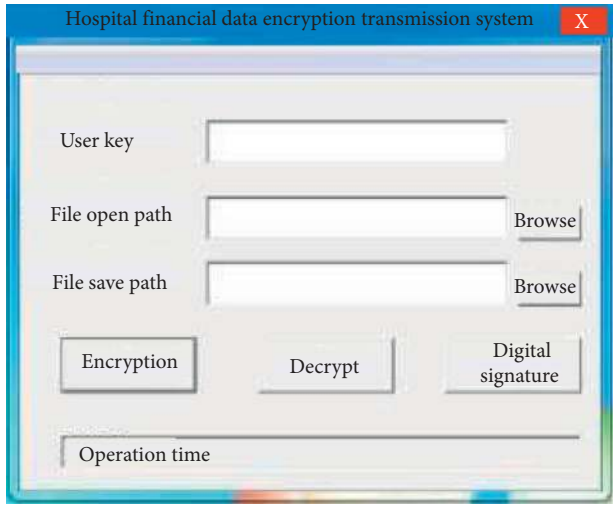

Figure 6: Main interface of the communication system.

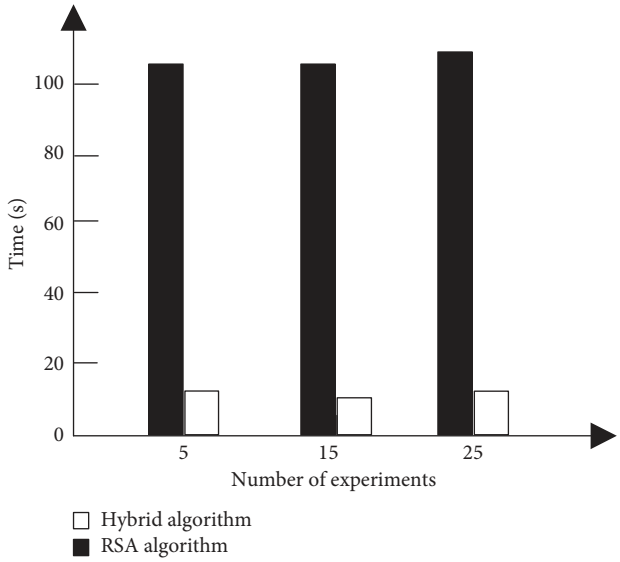

Figure 7: Time consumption for the addition and decryption of hospital financial data.

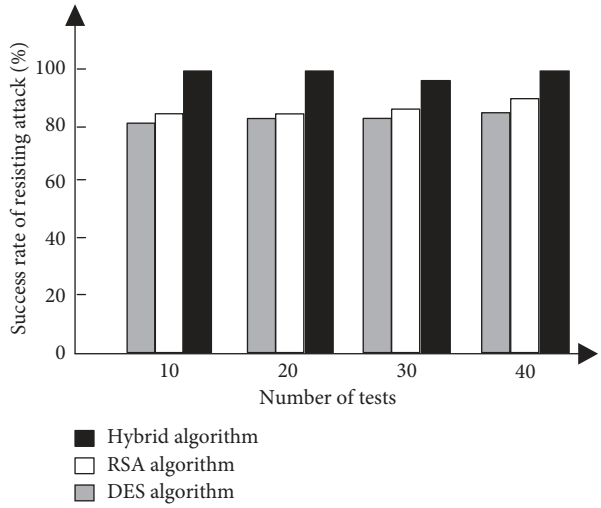

Figure 8: Comparison of hospital financial data encryption and security.

3.4.3. Interface Design. In order to realize the safe storage of files and the safe transmission between networks, the system selects visual studio 2012 programming software in Windows. On the operating system, the hospital financial data encryption transmission system is programmed. The main interface of the hospital financial data encryption transmission system is shown in Figure 6. Users can complete the encryption, decryption, digital signature, plaintext, and ciphertext saving path setting of hospital financial data through the main interface.

4. Experimental Results and Analysis

In order to verify the effectiveness of the hybrid encryption method of hospital financial data based on Noekeon algorithm, a correlation test was carried out. The experimental platform is built on VC + +. The financial data of the experimental hospital is a. Doc text file with the size of 1 MB. The experimental operation process is described above. The experimental results are shown in Figure 7.

According to the analysis of Figure 7, the hybrid encryption method of hospital financial data based on Noekeon algorithm takes less time and is more efficient than RSA algorithm.

Figure 8 shows the success rate of resisting attacks in different research results.

As can be seen from Figure 8, compared with the single algorithm, the hybrid algorithm has a higher success rate in resisting attacks and can better ensure the security of hospital financial data. Table 2 shows the overall performance of different hospital financial data encryption methods, so as to show which aspects of the performance of various hospital financial data encryption methods are more superior.

According to Table 2, compared with other encryption algorithms, the hybrid algorithm has better comprehensive

Table 2: Performance comparison of various financial data encryption methods in hospitals.

Performance index	Comparison results
Encryption efficiency	DES algorithm ≈ hybrid algorithm > RSA algorithm
Safety performance	Hybrid algorithm > RSA algorithm > DES algorithm
Key generation and control	Hybrid algorithm > DES algorithm ≈ RSA algorithm
Implementation and application	Compared with other algorithms, the hybrid algorithm has a wider application range and environment

performance, makes up for the defects of DES algorithm and RSA algorithm, and not only improves the encryption efficiency of hospital financial data, but also enhances the security of hospital financial data.

5. Conclusion

Since the end of the 20th century, with the rapid development of computer and communication technology, computer network has been more and more widely used in public life and work. With the progress of science and technology, the public is entering an information age, in which the security of information becomes more and more important. A hybrid encryption method for hospital financial data based on Noekeon algorithm is proposed. In the process, firstly, RSA algorithm and improved algorithm are analyzed, and then combined with improved algorithm and DES algorithm, private hospital financial data encryption is realized efficiently. Experimental results show that this method has strong encryption performance, higher efficiency, and stronger practicability than the improved encryption method. With the increasing development of computer network, private hospital financial data intrusion technology is also constantly improving. At this time, the hospital financial data encryption method will be more challenged. In the next research, we should constantly improve the encryption algorithm and combine it with the hardware system to lay a more solid foundation for ensuring the security of hospital financial data.

The hospital financial data encryption transmission system designed in this paper adopts the hybrid encryption system and realizes the encryption and decryption of hospital financial data by using the characteristics of fast encryption speed, high encryption intensity, and efficient encryption and decryption of a large amount of hospital financial data. Using public key cryptography algorithm, the encryption strength is high, the key is easy to manage, and the encryption and decryption of plaintext key are realized. The two are combined to ensure the security of hospital financial data storage and transmission. In short, based on the advantages and disadvantages of different encryption methods, the hospital financial data encryption transmission system under Noekeon algorithm should focus on the information processing mode of hybrid encryption, so as to improve the application security of Noekeon algorithm, avoid the inefficient impact of RSA algorithm, and realize the rapid and secure transmission and storage of files, hospital financial data, and other information.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The author declares that he has no conflicts of interest.

Acknowledgments

This study was supported by funding from the project fund of Jiangsu Provincial Health Commission in 2021 (Grant no. cw202133).

References

[1] A. April, "Cloud-computing and precision medicine: big data offers big opportunities," *The European Journal of Public Health*, vol. 29, no. Supplement_4, 2019.

[2] K. L. Tsai, F. Y. Leu, L. L. Hung, and C. Y. Ko, "Secure session key generation method for lorawan servers," *IEEE Access*, vol. 8, 2020.

[3] S. Sen, S. Maity, and D. Das, "The body is the network: to safeguard sensitive data, turn flesh and tissue into a secure wireless channel," *IEEE Spectrum*, vol. 57, no. 12, pp. 44–49, 2020.

[4] L. X. Gu, "Design of hospital financial information security encryption system based on hyperchaos two-way authentication," *Techniques of Automation and Applications*, vol. 40, no. 4, pp. 73–77, 2021.

[5] J. X. Pang and M. M. Sui, "Homomorphic encryption privacy protection data efficient intelligent mining simulation," *Computer Simulation*, vol. 36, no. 6, pp. 316–319, 2019.

[6] J. L. Tian, "Research on hybrid chaotic encryption algorithm based on cloud computing," *Application of Electronic Technique*, vol. 46, no. 10, pp. 79–82, 2020.

[7] V. P. Gerdt, A. Hashemi, and M. Alizadeh, "Involutive bases algorithm incorporating F 5 criterion," *Journal of Symbolic Computation*, vol. 59, pp. 1–20, 2013.

[8] J. Gayathri and S. Subashini, "An efficient spatiotemporal chaotic image cipher with an improved scrambling algorithm driven by dynamic diffusion phase," *Information Sciences*, vol. 489, pp. 227–254, 2019.

[9] V. Kalaichelvi, P. Meenakshi, P. V. Devi, H. Manikandan, and S. Swaminathan, "A stable image steganography: a novel approach based on modified rsa algorithm and 2–4 least significant bit (lsb) technique," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 11, 2020.

[10] A. Parihar and S. Nakhate, "High-speed high-throughput vlsi architecture for rsa montgomery modular multiplication with efficient format conversion," *Journal of The Institution of Engineers (India) Series B*, vol. 100, no. 2, 2019.

[11] S. Nath, S. Som, and M. C. Negi, "Cryptanalysis of a novel bitwise xor rotational algorithm and security for iot devices," *International Journal of Knowledge-Based and Intelligent Engineering Systems*, vol. 25, no. 1, pp. 139–147, 2021.

[12] H. Zare and S. Emadi, "Determination of customer satisfaction using improved k-means algorithm," *Soft Computing*, vol. 11, 2020.

[13] T. J. Cocucci, M. Pulido, M. Lucini, and P. Tandeo, "Model error covariance estimation in particle and ensemble kalman filters using an online expectationaximization algorithm," *Quarterly Journal of the Royal Meteorological Society*, vol. 6, no. 1, 2020.

[14] E. Y. Baagyere, A. N. Agbedemnab, Q. Zhen, M. I. Daabo, and Z. Qin, "A multi-layered data encryption and decryption scheme based on genetic algorithm and residual numbers," *IEEE Access*, vol. 8, 2020.

[15] J. Dai, N. Chen, X. Yuan, W. Gui, and L. Luo, "Temperature prediction for roller kiln based on hybrid first-principle model and data-driven MW-DLWKPCR model," *ISA Transactions*, vol. 98, pp. 403–417, 2020.