Research on Fast Encryption of Electronic Health Record Data Based on Privacy Protection

Tianlin Fu[1], Juanfen Shi[2], and Haipeng Ke[3](✉)

[1] College of Mathematics and Data Science, Minjiang University, Fuzhou 350000, China
[2] School of Electronic Engineering, Henan Information Engineering School, Henan 450008, China
[3] Fujian Zhangzhou No.1 Vocational Secondary School, Zhangzhou 363000, China
kehaipeng@163.com

Abstract. Electronic health records data has the characteristics of massive, multimodal, heterogeneous, but electronic health records data is easy to be invaded, leading to the disclosure of patient personal information. Health record management systems often ignore the security problems when patients interact with other roles, and the traditional encryption methods have been difficult to effectively meet the security needs of modern privacy data. Therefore, a fast encryption method of electronic health record data based on privacy protection is proposed. Mainly through the combination of privacy protection and homomorphic encryption technology to achieve distributed user privacy data protection, the mining effect of privacy protection is effectively improved, and the data security is guaranteed. The effectiveness and practicability of this method in data privacy security protection are verified by experiments.

Keywords: Privacy Protection · Electronic Health Records · Health Records · Archival Data · Fast Encryption · Encryption Research

1 Introduction

Electronic health records began to be used as early as the end of the 1960s. It records the occurrence, development and treatment outcome of individual diseases, and has high medical value. Electronic health record data has the characteristics of massive, multimodal and heterogeneous, and its complexity and magnitude of data are far beyond the scope of general data processing tasks. Computer theory, especially the development of emerging technologies such as data storage, machine learning and cloud computing, makes it possible to process massive electronic health archive data and extract useful information such as rules and patterns, which can be used for pathological analysis and disease early warning. However, the information security protection of the medical industry started late, and medical data leakage accidents emerge in endlessly. Hospital managers have absolute control over these electronic health records, which may be maliciously deleted, modified or leaked by internal personnel. If the privacy protection of individuals is not considered, the collection and application of electronic health records data will be greatly hindered [1, 2].

S. Wang (Ed.): IoTCare 2022, LNICST 501, pp. 255–270, 2023.
https://doi.org/10.1007/978-3-031-33545-7_18

The traditional sub health archives data encryption method only uses a single data encryption technology in the data encryption process, resulting in a small coverage of data encryption, a decline in encryption quality, and difficult to meet the security needs of modern privacy data. Therefore, a fast encryption method for electronic health archives data based on privacy protection is proposed. Aiming at the problem of single data encryption method, the distributed user privacy data protection is mainly realized by combining privacy protection with homomorphic encryption technology, which effectively improves the mining effect of privacy protection and ensures data security.

2 Related Work

The extraction and mining of valuable knowledge is realized through big data mining technology in diverse data (with massive and irregular characteristics). The realization methods of mining should be fully considered. The data mining methods based on privacy protection mainly include association rules data mining methods, sequential pattern data mining methods, encryption, and clustering data mining methods. In order to ensure the smooth progress of big data mining, it is necessary to take corresponding restraint measures for different sites to improve their self-restraint management capabilities, and try to avoid the problem of privacy data leakage. In recent years, some academic research results have been achieved, for example, using corresponding data mining methods (based on privacy protection) to improve the execution efficiency and privacy security of data mining based on semi-honest and malicious models; On the basis of in-depth exploration of security protection), a data mining method (based on the hiding of important sequence attributes) is designed, so that the data privacy protection function can be effectively realized; For the distributed environment, a data mining method based on privacy protection is completed. The mining method can effectively solve the problem of privacy leakage in the mining process [3, 4].

3 Methods

3.1 User Privacy Protection

Electronic health record data file management involves user management, authentication, data isolation and other aspects of design. Data isolation can protect individual data, separate the data of different users, and ensure personal privacy, so as to build a user privacy protection structure, as shown in Fig. 1 below:

According to Fig. 1, data sharing can be carried out if permitted. The basic architecture pattern is that a single server is connected to its database and is separated from other architectures. The shared architecture can allow different data information databases, which can be applied to the same a server, users can be distinguished or communicated by ID, with a large degree of freedom and a large capacity, which can effectively ensure the safe communication between users.

The user management of electronic health records is set to the user mode of individual corresponding to their own account. During application, the account and password login is required to ensure the operation safety of the system, and unified management

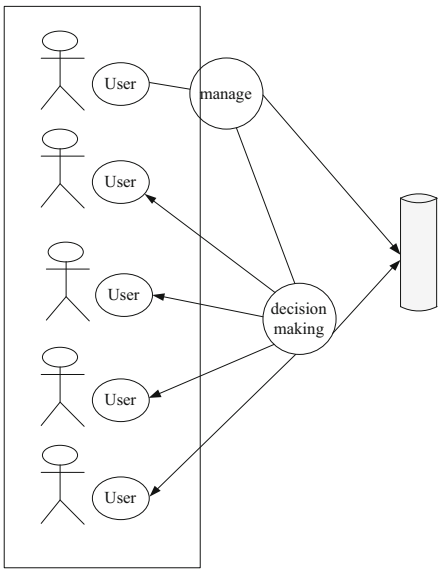

Fig. 1. User privacy protection structure diagram

instructions can be executed. At the same time, the basic information and security of users are guaranteed, and relevant security mechanisms are provided, so as to protect the privacy and precision of users, separate data from the management system, and enhance the information security of users.

3.2 Authority Assignment

The file agent system is mainly used to deal with matters between privacy protection and multi type electronic health record management systems. Different roles have different rights. Through key division, according to the permissions of different files, it can process and retrieve files, write, store and other operations. If necessary, it can be provided to users.

It mainly includes document archives sorting, document storage, information retrieval, access rights design and so on [5].

The program in this paper adjusts the internal management personnel information and system data. The management personnel and the system are divided according to the content and authority scope of their files, and the files are organized to facilitate the user's invocation and rectification [6, 7].

Since the information storage of electronic files involves the access rights of the files, the system design of this paper strengthens the design of the key, makes a reasonable calculation and design for the confidentiality period, and forms a virtual electronic contract to ensure the user's use rights and key confidentiality. Period of security. Build a permission assignment flowchart (Fig. 2):

When users use archives, they need to query and search through the Internet to get the information of relevant archives. Therefore, the retrieval function is an extremely

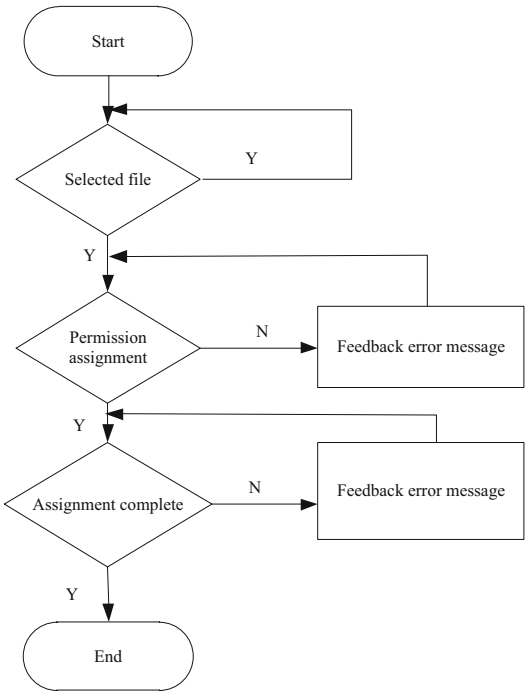

Fig. 2. Permission allocation flow chart

important system design. The application unit puts forward the retrieval request of relevant files to the browser according to the demand, and the request is sent to the processor. Each retrieval unit provides various electronic health files according to the demand, and judges whether to use the key according to the user's role type for security [8].

When the electronic file data is illegally obtained or maliciously tampered, the file agent system can upload the error information, and the administrator can track it through the computer to restore the privacy protected data information file, so that its information security is not infringed. At the same time, a firewall management system is set to protect the integrity of the data. Its working diagram is as follows (Fig. 3):

Set up the encryption model of electronic health records. The application of this model is that electronic health records can complete the information exchange between privacy protection and multi type electronic health record systems, improve the efficiency of information processing and expand the source of information. At the same time, the design of isolation system enhances the security and stability, and ensures the authenticity, reliability and effectiveness of electronic information. The application of cloud computing and smart contract greatly improves the efficiency of data management, realizes the fine management of electronic health records, and has a certain degree of automation ability, reduces the cost of human and material resources and other services, and improves the utilization of resources.

At the same time, the failure of individual data cannot affect the operation of the entire system, which improves the overall security of the system and reduces the possibility

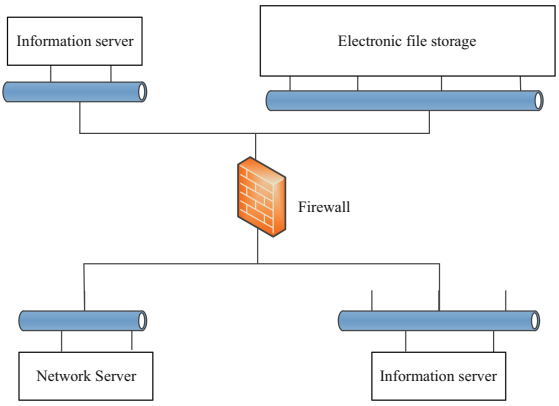

Fig. 3. Schematic diagram of firewall work (Fig. 2)

of illegal access and destruction. Thus, a more complete system software design is constructed.

3.3 Logic Analysis of Electronic Information Resources

Electronic information is stored in the hard disk of the computer. The storage address of each resource in the hard disk has an internal logical relationship. A complete storage area is divided into thousands of storage modules, and each storage module is divided into many levels for encrypted storage of resources. Electronic information includes the basic attribute information, naming, construction time, and logical address of the information. According to the above information, the electronic resources to be stored are logically analyzed. The internal relationship of the same type of electronic resource information has a logical relationship, and different types of resource information has an inverse logical relationship. If different types of resources are stored together, the two resources will consume each other, which is not conducive to the storage of information resources.

Electronic information resources are distributed and stored in different folders of computer hard disk. In order to balance the stability and integrity of information resources in network storage space, this paper optimizes the distribution of electronic information resources through distributed system method. The main working principle of the distributed system method is to convert and identify the format and content of information resources through the signal strength of the information cluster, and finally encrypt the resources according to the identification results. In the process of real-time information storage, the storage location is reasonably distributed to ensure the integrity of resources to the greatest extent. In the process of running, the distributed system converts the format of resources. If the resource is formatted, the format code of information cannot be monitored. When the conversion cannot be carried out, the electronic information resource is directly discarded without content code conversion, which saves the storage space of electronic information resources and improves the storage efficiency of resources. On the other hand, in order to prevent errors in resource conversion, the distributed system

will retain the attribute information of information resources in the process of content conversion for electronic information resources with effective format. When resources are extracted and converted incorrectly, it will use artificial intelligence technology and information attributes to restore the original information resources [9, 10].

3.4 Encryption of Electronic Information Resources

Through the above analysis of the logical relationship between electronic resources and the research on the reasonable distribution method of resources, this paper designs an encryption method of electronic information resources based on artificial intelligence technology.

The real-time encryption process of electronic resources studied in this paper is divided into two parts: obtaining the basic information of electronic resources and encrypting electronic resources into the effective encryption area of the computer. The basic information of electronic resources includes attribute information, naming, time information of resource receiving, receiving way and address information of information resources [11]. When reading the basic information of electronic resources, you need to obtain the authority authentication of the resource holder before reading. After reading the resource information, in order to ensure the security of information resources, this paper encrypts the information. Because the resource information is displayed in the form of bytes, and each resource information is represented by a combination of multiple bytes, the core of the encryption of electronic resources is to effectively number the resources. An effective number consists of two 1024 bytes, and the two 1024 byte variables have the same meaning after exchange. Set the two byte read key and the overall key. The specific process is summarized as the following formula:

$$S_i = S_{i-1} + A_{i-1} \tag{1}$$

$$C_i = S_i, X_i + C_{i=1} \tag{2}$$

Among them, A is a byte of 1024; $C_o = 0$; X is the number of the electronic resource.

The above formula is to encrypt the encrypted electronic resource information, but it does not avoid the interference of external signals, which will affect the encryption efficiency of electronic information encryption. Therefore, the level of encryption should be increased to ensure the confidentiality of electronic information encryption [12]. In order to improve the level of information encryption, this paper sets a signal shielding lock in the encryption area of the computer. Once the electronic information is encrypted, the signal shielding lock automatically locks, and cannot receive scheduling information signals other than the computer, and powers the two keys inside the electronic resources. The power processing method without the key is the same, and it is processed by the following formula:

$$r = s - a_b - k \tag{3}$$

where a_b is the key group with two numbers; s is the code of electronic information resources; r is the external interference signal source; k represents the number of power

processing of electronic information. Calculate the data of k by substituting the above formula, complete the secondary encryption, improve the real-time encryption method of electronic information resources, and ensure the security of information resources while ensuring the encryption efficiency.

The design of the software part of the hospital file encryption system design based on privacy protection in this paper mainly includes the software program database, the system login program, the web browser and the use of each module inside the system. The specific file encryption process is shown in the following figure (Fig. 4):

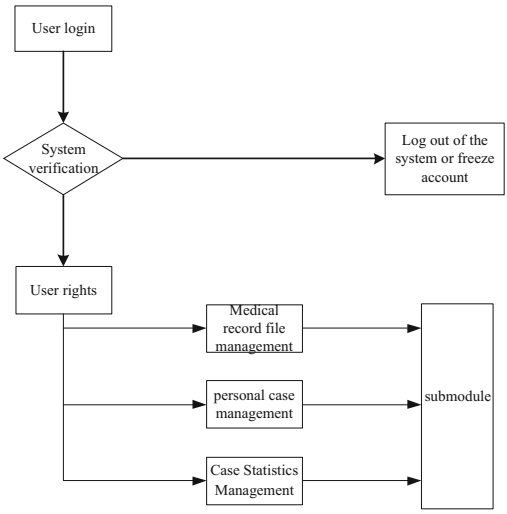

Fig. 4. Encryption process of hospital file encryption system

Database is the core of the file management system. Only with high database security and large memory space, can we ensure the safety of patient information in the hospital. The database is mainly responsible for encrypting the file data and establishing the connection between the file information and various departments. The database E-R diagram is designed. The hospital managers can change and verify the patient information through the identity of the administrator. In the file encryption system, the specific software area program database E-R diagram is as follows (Fig. 5):

The web browser is encrypted by a special code, which can ensure the security of the encrypted data in the hospital file encryption system. The web browser is divided into three browser channels, which are respectively oriented to patients, doctors, and managers, so that the three parties can enter the system at the same time. The login page of the file encryption system software part is registered and logged in through the user's registered mobile phone number, and the system browser is visible to the patient. The hospital doctor also enters the doctor's login browser through the same login page. Through the mutual adjustment between the database of the software system and the various modules in the hardware area, the operation of the browser is maintained, and the stable operation of the file encryption system and the security of file data are guaranteed.

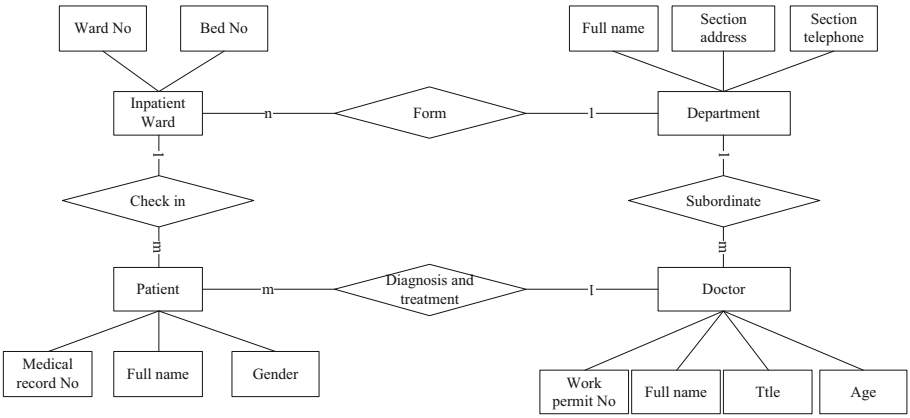

Fig. 5. E-R diagram of the software program database of the hospital file encryption system

The ultimate purpose of designing the hardware area of the hospital file encryption system is to ensure the security of the file encryption system and improve the operation efficiency of the system. Therefore, in order to achieve the design purpose, this paper proposes privacy protection to assist the operation of the encryption function of the system. Privacy protection is an optimized integrated algorithm method of distributed gradient computing. The idea of the algorithm method comes from the gradient lifting iterative decision tree. On the basis of the gradient lifting iterative decision tree algorithm method, the function of computing data encryption by second-order Taylor function is added to improve the encryption speed and accuracy of privacy protection on data files. Specifically, it is completed with the help of the following formula:

$$y_i = \theta(x_i) = \sum_{k=1}^{k} f_k(x_i) \tag{4}$$

Among them, k is the total number of data in the sub-model; y_i is the predicted value of the data sample; x_i is the feature quantity of the input archive data; f_k represents the data encryption regression value of the k cycle of the method.

The above formula introduces the second-order Taylor function to normalize the initial input data to avoid data confusion. In order to calculate the weight value of each file data, this article will refer to the following objective function as follows.

$$0 = 1(y, y_i) + \sum_{k=1}^{k} \beta(f_k) \tag{5}$$

Among them, (y, y_i) integrates the normative model of data; 0 represents the difference between the predicted value of the previous formula and the recorded value of the actual data; β represents the normalization processing coefficient, which is the positive value after calculating the data weight to prevent confusion between data. Use the basic data of deep learning to adjust the state of software encryption method, obtain the state parameters, set the corresponding operation related values, and combine the parameters

in deep learning with the operation related values to find the specific encryption address source. Control the transmission direction of private data, guide the basic transmission direction of data by the deep learning function, issue the transmission password to the operation space, and adjust the transmission quantity according to the transmitted code information to maximize the transmission quantity. Set the corresponding transmission adjustment formula as follows:

$$N = c - t \cdot \sqrt{Q^5} \tag{6}$$

In the above formula, N represents the transmission adjustment result data, c represents the data transmission direction data, t represents the transmission password issuing parameter, and Q represents the operation space transmission password parameter.

When the server cannot respond to the transmission operation, it needs to modify its software information, adjust the data status in time, and set the information modification equation as follows:

$$P = v \cdot \frac{w}{K} + \sum A + c^2 \tag{7}$$

In the above formula, P represents the information modification parameter, v represents the transmission operation parameter, K represents the total number of data transmissions, w represents the received data information, A represents the command response parameter, and c represents the data condition adjustment value. In this way, the real performance of the operating system is analyzed, and it is convenient to accurately grasp the system data.

According to the information situation, install the system information device, build the software conversion platform, improve the operability of the software system, and set the corresponding system adjustment equation:

$$T = \sqrt{\frac{u - l}{d}} + \sum P \cdot S^{0.5} \tag{8}$$

In the above formula, T represents the response system adjustment parameter, d represents the installation system information parameter, u represents the operation step readability parameter, l represents the user information parameter, P represents the overall planning value, and S represents the platform construction parameter. According to the obtained parameter information combined with the key operation content, centralized data adjustment operation, improve the privacy data encryption audit method, strengthen the audit strength, and effectively implement data control.

Through the superposition calculation of multiple data, the predicted value of the iterative sample of the data is brought into the loss function, and the calculation result is multiplied by the normalization coefficient, then the final simplified formula of privacy protection is as follows:

$$o^t = \sum_{i=1}^{N} 1\left(y_i, y^{t-1} + g_i f_i(x_i) + \frac{1}{2} h_i y_i(x_i)\right) + \beta(f_i) \tag{9}$$

Among them, N is the number of integration trees. Encrypt the data files to establish a decision tree. Compare and calculate the input file data with the data in the system database. If the same type of medical record information is retrieved, it will be encrypted in the same encrypted space to facilitate the operation of information call. Integrate and encrypt the redundant data of the decision tree, and finally complete the final management encryption of the data.

4 Experiment

After the realization of the above method design and research, the system improvement operation is carried out according to the designed structure and framework. In order to verify the encryption performance of the encryption method design in this paper, the encryption method design in this paper is compared with the traditional encryption method design, and a comparative experiment is constructed. The experimental comparison indicators are as follows:

(1) Encryption rate
(2) Encryption accuracy

Carry out experimental research according to the above two indicators, build an experimental environment, conduct experimental comparison operations on the basis of software management, pay attention to maintaining system service security when testing the operation status of encryption methods, archive the encrypted electronic health record information, and build a file encryption map (Fig. 6):

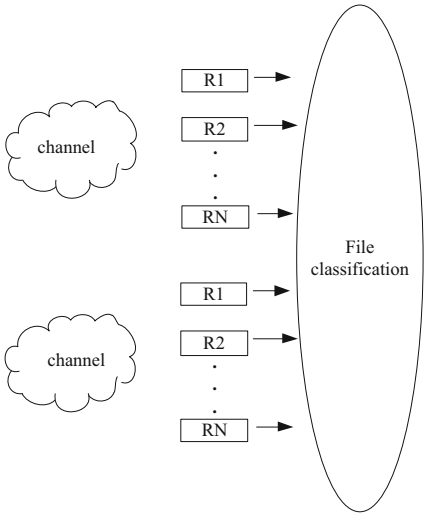

Fig. 6. File encryption diagram

Adjust the final encryption position of the electronic health record data, and set the encryption rate according to the encrypted data results. The comparison table is as follows (Tables 1, 2 and 3):

Table 1. Encryption method design encryption rate table in this paper

Encryption time/d	Encryption rate percentage
10	89%
20	93%
30	96%
40	100%

Table 2. Encryption rate table of traditional encryption method based on SaaS technology

Encryption time/d	Encryption rate percentage
10	77%
20	80%
30	85%
40	89%

Table 3. Traditional encryption method design encryption based on SOA architecture

Encryption time/d	Encryption rate percentage
10	64%
20	72%
30	75%
40	82%

According to the above table, the encryption rate designed by the fast encryption method of electronic health records based on privacy protection technology in this paper is faster than that designed by the other two traditional encryption methods. Because this method uses privacy protection to build a security system in the design process, so as to ensure the security of electronic health records in the transmission process, and adjusts the operation mode of the system according to the obtained security information, it has complete situational operation strength, and can transmit files under different network transmission systems. When the internal part is disturbed by external interference signals in the encryption process, the system will automatically send an alarm signal, and send the alarm signal from the file transmission source point to the file collection end point, so as to prevent abnormal data from invading the encryption method, ensure the complete and safe entry of electronic health file data information, thereby reducing unnecessary system operation waste and improving the overall system encryption rate.

After the above experimental operation is realized, in order to further verify the encryption effect of the system design in this paper, the encryption accuracy of the system

is studied. Based on the electronic health record data obtained by the experiment, the error information sent by the system and the correct display information are distinguished, and the information collection is set. Structure diagram (Fig. 7):

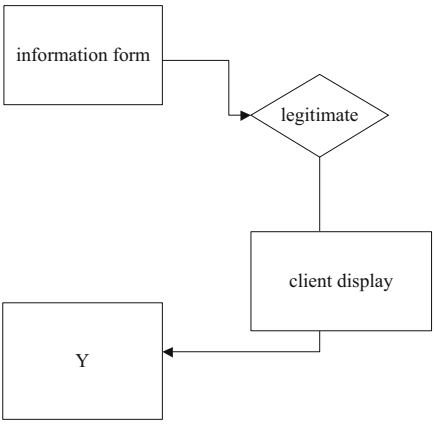

Fig. 7. Information recording structure diagram

According to the experimental information obtained above, the encryption accuracy comparison chart is constructed as follows (Fig. 8):

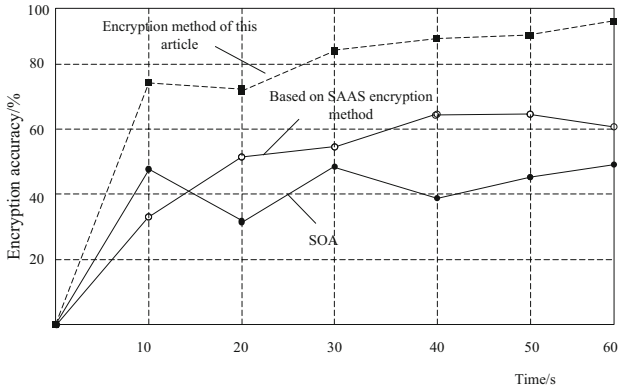

Fig. 8. Encryption accuracy comparison chart

According to the above figure, the encryption accuracy of the fast encryption method of electronic health records based on privacy protection technology in this paper is higher than that of other traditional encryption methods. The reason for this difference is that the software program designed in this paper selects the system encryption mode to manage the electronic health records in transmission, optimizes the encryption structure of the files, simulates the encryption process of the electronic health records, and constructs the

encryption model to intuitively reflect the state and operation form of the model, further speed up the overall file encryption operation process, and count the number of electronic health records at any time, Specify the encryption standard of electronic health records according to the passed quantity information. Set up software emergency procedures. When the electronic health records approved by the software cannot be finally encrypted, the emergency procedures can send protection signals, the main system receives signal information, and issues the encryption instructions of electronic health records. Therefore, these electronic health records can complete the final encryption operation. Further realize the mechanism protection operation of electronic health records and improve the accuracy of overall encryption.

To sum up, the design of the fast encryption method for electronic health records based on privacy protection technology in this paper can greatly improve the speed and accuracy of electronic health records encryption, and provide a large amount of data support for the subsequent processing of electronic health records. Has a good operating effect.

After completing the above experimental operations, in order to further test the encryption performance of the encryption system in this paper, set up a secondary system test experiment, first analyze and process the designed system requirements, and provide certain data support for the processed analysis results. When testing the command, place the command information receiver in time to avoid receiving errors caused by poor receiving status. And build the system instruction transmission structure diagram (Fig. 9):

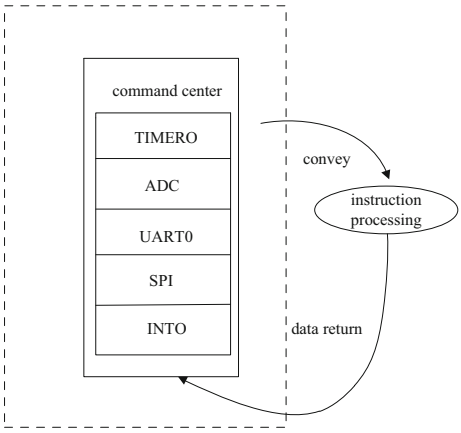

Fig. 9. Encrypted instruction instruction transmission structure diagram

At the same time, allocate the file transmission task at this time, transmit the files in a centralized manner according to different transmission directions, compare the security degree of the files after transmission, and build the encryption security rate comparison table as follows (Tables 4, 5 and 6):

Table 4. Encryption security rate result table of the method designed in this paper

Encryption time/s	Encryption security rate
20	88%
40	94%
60	97%
80	99%

Table 5. Results of system design encryption security rate based on data analysis

Encryption time/s	Encryption security rate
20	67%
40	78%
60	82%
80	86%

Table 6. The result of system design encryption security rate based on file encryption

Encryption time/s	Encryption security rate
20	54%
40	60%
60	66%
80	75%

According to the table of the above experimental comparison results, the file encryption security rate of the hospital file encryption system designed based on privacy protection in this paper is higher than that of the traditional system design, which shows that the system has strong execution and can safely encrypt files. The reason for this difference is that the encryption system in thispaper strengthens the processing of the system hardware structure and assigns different processing information when designing the encryption space. When the external data interference signal is generated, the encryption system will automatically transmit the blocking signal, block and eliminate the interference signal, and ensure the security of the encrypted file. When the hospital archives are in the transmission state, the transmission channel will encrypt and protect the information of this channel, timely collect the security system information related to the encrypted information, and re encrypt the transmitted documents, so as to finally realize the safe transmission of the hospital archives and complete the overall system design and architecture operation. Improve the encryption security rate of the encryption system and enhance the independent protection performance of the system archives.

To sum up, the design of the hospital file encryption system based on privacy protection in this paper has strong file encryption performance, can process complex hospital file information to a certain extent, and query accurate individual files in the complex information flow, which is sustainable. Providing file inspection services can better provide a solid data operation foundation for subsequent research operations.

5 Conclusion

Through the above analysis and the implementation of resource encryption methods, we get the real-time encryption method of electronic health records based on privacy protection. The analysis of information resource logic improves the encryption efficiency of resources, and the research on resource distribution optimization increases the density of real-time encryption of resources to a certain extent. As a new real-time encryption method of resources, it has a very superior application prospect. It is believed that privacy protection technology is an important direction for the development of real-time encryption methods of electronic information resources. In the future, it is necessary to apply the fast encryption of electronic health records data based on privacy protection proposed in this paper to other fields, so as to further expand the application scope of this method, maximize the data security in multiple fields, and promote the further improvement of network security technology.

References

1. Raman, S.R., O'Brien, E.C., Hammill, B.G., et al.: Evaluating fitness-for-use of electronic health records in pragmatic clinical trials: reported practices and recommendations. J. Am. Med. Inf. Assoc. **29**(5), 798–804 (2022)
2. Himmelreich, J., Lucassen, W., Harskamp, R., et al.: Correction:CHARGE-AF in a national routineprimary care electronic health recordsdatabase in the Netherlands: validationfor 5-year risk of atrial fibrillation andimplications for patient selection inatrial fibrillation screening. Open heart **8**(2), 1–10 (2021)
3. Tsai, M.-Y., Cho, H.-H.: A high security symmetric key generation by using genetic algorithm based on a novel similarity model. Mobile Netw. Appl. **26**(3), 1386–1396 (2021). https://doi.org/10.1007/s11036-021-01753-1
4. Xu, W., Zhao, Q., Zhan, Y., Wang, B., Hu, Y.: Privacy-preserving association rule mining based on electronic medical system. Wirel. Netw. **28**(1), 303–317 (2021). https://doi.org/10.1007/s11276-021-02846-1
5. Xu, Z., Luo, M., Kumar, N., et al.: Privacy-protection scheme based on sanitizable signature for smart mobile medical scenarios. Wirel. Commun. Mob. Comput. **20**(1), 1–10 (2020)
6. Chenthara, S.: Healthchain: a novel framework on privacy preservation of electronic health records using blockchain technology. PLoS ONE **15**(12), 105–122 (2020)
7. Yang, Y., Xiao, X., Cai, X., et al.: A secure and privacy-preserving technique based on contrast-enhancement reversible data hiding and plaintext encryption for medical images. IEEE Signal Process. Lett. **27**, 256–260 (2020)
8. Wang, Y., Zhang, L., Zhang, D., et al.: Research on multiple-image encryption scheme based on joint power spectral division multiplexing and ghost imaging. Laser Phys. **31**(5), 055204–055216 (2021)

9. Chen, K., Feng, X., Fu, Y., et al.: Design and implementation of system-on-chip for peripheral component interconnect express encryption card based on multiple algorithms. Circuit World **24**(7), 366–378 (2020)
10. Ay, N., Akpinar Borazan, A., Kuru, D.: Synthesis of boron nitride nanosheets/polyvinyl butyral thin film: an efficient coating for UV protection of extra virgin olive oil in glass bottles. J. Nano Res. **72**(1), 37–51 (2022)
11. Brunekreef, T.E., Otten, H.G., Bosch, S., et al.: Text mining of electronic health records can accurately identify and characterize patients with systemic lupus erythematosus. ACR Open Rheumatol. **15**(3), l147-158 (2021)
12. Zhang, Y.M.: Mathematical model of network data conformal encryption based on block cipher. Comput. Simul. **39**(3), 466–469 (2022)