Research Article

Medical Record Encryption Storage System Based on Internet of Things

Yamei Zhan\textsuperscript{1} and Zhaopeng Xuan\textsuperscript{2}

\textsuperscript{1}Medical Records Room, The First Hospital of Jilin University, Changchun 130000, China
\textsuperscript{2}Hand, Foot Surgery, The First Hospital of Jilin University, Changchun 130000, China

Correspondence should be addressed to Zhaopeng Xuan; xuanzp@jlu.edu.cn

Received 9 October 2021; Revised 2 November 2021; Accepted 5 November 2021; Published 24 November 2021

Academic Editor: Chin-Ling Chen

Copyright © 2021 Yamei Zhan and Zhaopeng Xuan. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

The Internet of Things takes data as the center, and its core is data storage and management. With the emergence and rapid development of wireless communication technology, with the huge number of terminals in human society, massive data will be generated. Undoubtedly, data storage and management technology will attract much attention. In view of this, this paper proposes a data storage scheme based on the Internet of Things. This paper introduces the Internet of Things technology, designs it from the perspective of the massive data storage system of the Internet of Things, realizes the intelligent processing of data storage, and provides security guarantee for information services. By combing the business process management of doctors, nurses and patients, this paper constructs a medical record encryption management system, makes a comparative analysis before and after the system goes online, and carries out simulation experiments. The simulation results show that (1) the cost of paper is significantly reduced, and the related forms of medical records are more unified and standard, (2) medical record inquiry and reading are more convenient and controllable, and (3) the safety of medical records is well guaranteed. Except that the relevant doctors and nurses of patients can view the relevant medical records, and others have no authority to query and access them. Therefore, the encrypted medical record storage system based on Internet of Things technology can effectively solve the collection, statistics, and integration of patient treatment information, which can be summarized into a unified, shared, and interconnected electronic medical record management system to realize the collection of patient treatment information in the whole process.

1. Introduction

At present, e-government, medical, and health information systems need to store personal data. Although the use of personal data is more humanized, the personal data stored in the system may be abused by operators or system administrators. In this context, relevant prevention and control technologies came into being. At the same time, with the development of cloud computing, the demand for arithmetic operations on encrypted personal data is also growing rapidly. The problem of medical record data storage: the electronic medical record system requires long-term preservation of patient information and can be obtained at any time. However, considering the limited life of computer hardware and database capacity, the data cannot be saved online for a long time. How to realize the reuse of data after data transfer and make the patient information separated from the database still maintain a personal centered structure is one of the difficulties encountered in the process of medical record data storage. Medical record data sharing: medical record data sharing is to ensure that the electronic medical record system can automatically identify the data from other systems and access the medical records written by other hospitals. How to realize the data sharing between different information systems in the same medical institution and the information reuse between different medical institutions is another difficult problem faced by the electronic medical record system.

With the continuous development of social economy, the informatization of all walks of life has been gradually
constructed and improved, which greatly facilitates people’s daily life [1, 2]. As far as individuals are concerned, they will generate corresponding information during medical treatment, such as medical information, condition information, and medication information. Traditional management methods are usually filled in manually. On the one hand, safety cannot be guaranteed; on the other hand, it is not conducive to retrospective comprehensive diagnosis of the disease [3, 4]. The development of information technology has spawned a variety of medical business systems, but also convenient for individuals to see a doctor. All kinds of information carriers, from PC Web application to mobile app and WeChat mini program, have greatly enriched the medical experience and made it convenient for people to see a doctor. However, similar to other information systems, information security is still caused by external attacks [5]. The continuous development of cloud computing technology also makes people gradually realize the importance of personal information. In the general trend of hospital management, how to ensure the security of information is extremely important [6, 7]. Different doctors and different patients have different actual needs; so, these issues need to be considered comprehensively [8, 9]. In particular, in the actual treatment process, it is more often to search for relevant cases and provide targeted rescue according to the history and allergy history of existing patients, which delays the treatment time to a certain extent [10, 11].

The continuous development of medical informatization has gradually changed from the initial information flow to the collection of “patient-centered” medical data [12, 13]. In view of these needs and limitations, this paper puts forward a practical encrypted data processing system based on Residents’ electronic medical records, combined with cloud storage technology and traditional homomorphic encryption system, which can realize the operation of data without decryption, prevent data leakage, and greatly protect the security of personal information.

2. Demand for Electronic Medical Record Whole-Process Management System

2.1. Electronic Medical Records

2.1.1. Definition of Electronic Medical Record. To electronic medical records, it is different with the traditional medical record, medical institution oriented personnel of the diagnosis and treatment of patients with accordingly, and intervention in the use of information guidance; at the same time, auxiliary by text, graphics, data, etc., through images, oscillogram of multimedia information such as records, covers the corresponding information resources in the process of patients in the hospital the whole.

2.1.2. Problems Existing in Electronic Medical Records. Need to be worthy of the electronic medical record still exists some limitations, such as (1) electronic medical record data storage, because this is an incremental process, and when people in the clinic is the cumulative again, if you have to go to the situation of the hospital, you will need to incremental updates, but is limited by factors such as hardware capacity and service life, the data cannot be stored for a long time, and how to realize the limited storage and effective transfer of personal electronic medical records is extremely important and also a difficult problem worthy of study [14, 15]. (2) The sharing of electronic medical records, ordinary people in different institutions for medical treatment, different institutions have different forms, writing habits, and how to effectively and comprehensively use, is also an important and urgent problem to be solved. (3) Security of electronic medical record: electronic medical record contains many personal privacy issues such as physiology, which are easy to be leaked. At the same time, there are certain security risks in the process of information transmission.

2.2. Manage Requirements. The electronic medical record of ordinary people is related to the whole process of personal medical treatment, involving the corresponding data collection, query and analysis, etc. How to carry out the comprehensive management and storage of relevant information realizes multiple summaries and analysis and mining of information, so as to support doctors’ medication and analysis, etc. [16, 17].

2.3. Cloud Storage. So-called cloud storage is based on the storage of the cloud computing technology, the corresponding data resources stored in the cloud, for others to share and use methods; on the one hand, from the user’s own, cloud storage is very convenient, does not need to prepare the corresponding hardware equipment, and storage space can meet, easy access, and high efficiency, can realize the backup and so on; on the other hand, due to the high efficiency of cloud storage, the access efficiency is also high. However, data resources in the cloud have certain security risks, which should be paid attention to [14, 15, 18].

2.4. Holomorphic Encryption

2.4.1. Homomorphic Encryption Technology. Homomorphic encryption is an encryption method that encrypts a specific ciphertext by calculating the ciphertext. In turn, the ciphertext can be decrypted by the corresponding inverse operation. From another perspective, this technology allows people to perform operations such as retrieval and comparison among encrypted data to obtain correct results without the need to decrypt the data during the entire process. Its significance lies in truly fundamentally solving the problem of confidentiality when entrusting data and its operations to a third party.

2.4.2. The Principle of Homomorphic Encryption. Assume that the encryption operation is $E$, the plaintext is $M$, and the encryption results in $E$, as shown in Formula (1),

$$e = E(m), m = D(e). \quad (1)$$

If there is operation $F$ for plaintext, it can be constructed for $E$, as shown in Formula (2):

$$F(e) = E(f(m)). \quad (2)$$
2.4.3. The Realization of the Homomorphism Algorithm. Encrypt(pk, m), encrypted plaintext message \( m \in \{0, 1\}^* \), calculates \( E(m) = c = m + p + rpq \), and the corresponding ciphertext can be obtained.

Decrypt(sk, c) calculates \( D(c) = m = c \mod q \), the algorithm is a retrieval algorithm.

(1) Encryption Process. Firstly, the corresponding plaintext should be divided into subunits according to the corresponding security requirements, and the encryption operation should be carried out according to the corresponding groups, as shown below:

(1) Form the corresponding prime number \( P \) through random number and select fixed prime number

(2) Divide the corresponding messages into plaintext and group them accordingly

(3) Generate a random number \( R \)

(4) Use encryption algorithms \( C = \Sigma c_i = \Sigma_i (m_i + P + PQR) \) to calculate the ciphertext \( C = c_1, c_2, \cdots, c_i \)

(2) Decryption Process.

(1) After receiving ciphertext \( C \), users group ciphertext \( C \) to obtain \( C = c_1, c_2, \cdots, c_i \)

(2) Use key \( P \) and decryption algorithm \( m_i = c_i \mod p \) to calculate \( m_i \)

(3) Get the plaintext message \( M = m_1, m_2, \cdots, m_i \)

2.5. Management Process. The whole process management of hospital electronic medical record information is divided into three parts, namely, the external authority management of the electronic medical record system based on the Internet of Things, internal closed-loop management, and other systems of the hospital health information exchange standard (Health Level Seven, HL7) heterogeneous database middleware. ① External authority management includes label printing, label verification, fingerprint identification, and identity authentication; ② internal closed-loop management includes outpatient medical records, clinical treatment, surgical schedule, appointment sign-in management, follow-up management, cycle management, and cycle management and other links; ③ other systems of the hospital HL7 heterogeneous database middleware: the electronic medical record system and the hospital’s existing hospital information system (hospital information system, HIS), laboratory information system (laboratory information system, LIS), image archiving and transmission system (picture archiving and communication systems, PACS), radiology information system (radiology information system, RIS), ECG acquisition, blood transfusion management, and other clinical support systems and business management system data are transformed through HL7 heterogeneous database middleware and realize the functions of information sharing and mutual visits, as well as data mining and statistical analysis. For patients, the management of medical records can be divided into three basic parts, mainly including the external rights of medical records, internal rights management, and data exchange middleware [19].

(1) External access rights include label inspection, fingerprint identification, and identity authentication; (2) internal rights management mainly includes outpatient medical records, clinical diagnosis and treatment, follow-up management, and cycle management; and (3) data exchange middleware: the corresponding data management system is shared and transmitted to realize the data sharing, query, access, data mining, and statistical analysis of patients’ corresponding information. The specific process management of medical record information management is shown in Figure 1

3. Construction of Paperless Electronic Medical Record Management System

Patient-centered, the Internet of Things is shared based on the Internet of Things using rfid, laser scanning, global positioning, and other technologies and equipment in the Internet of Things technology, to realize information transmission and exchange and to complete intelligent positioning, identification, tracking, management, and monitoring. It adopts a three-tier network architecture of browser/server (B/S) mode, Windows Server server operating system, 10 Gigabit Ethernet, and Oracle system for database. In the network system deployment plan, a clinical information system server with electronic medical records as the core, a certificate authority (CA) electronic signature management server, a time stamp server, various user terminals in the hospital, a medical record high-speed camera, and a computer is specially set up in the network system deployment plan. Mobile handheld devices, etc., seamlessly record patient medical information data throughout the entire process, collect, count, and integrate data to ensure integration and homogeneity, overcome many problems in traditional medical record management, and complete one-stop electronic medical record management with unification of data format and data sharing system. The paperless electronic medical record management system has good man-machine dialogue and powerful functions. The medical record entry interface is completely consistent with the actual work medical record homepage.

3.1. Main Technical Equipment

(1) RFID technology. Radio frequency identification (RFID) technology of electronic tags is the communication technology of target and corresponding system through the identification and data collection of infinite signals. The Internet of Things can connect corresponding devices, which is an extension and extension of Internet technology. Medical records set up a unique RFID code and can achieve rapid search and positioning.
(2) CA electronic signature. Use the corresponding files for CA signature storage management, when the system documents are generated, that is, CA signature, first of all, the doctor in the medical record input CA signature, using the corresponding virtual printing technology method in different systems for sampling and identification, in a standard and correct format of electronic medical record management. However, for the CA signature of ordinary people, HD photography can be imported and transmitted to the corresponding system through the corresponding equipment, to achieve the preservation of paper files, and at the same time assist with the original handwriting signature and time stamp mutual authentication; when conditions permit, the corresponding recordings and photos are left for digital confirmation.

(3) Timestamp server. Timestamp service is based on the certification, the national center for timing, and punctual system according to the time of the trusted timestamp, time monitoring system to ensure the accuracy of time, use of time to clear and unified, doctors and patients, makes the electronic medical record access request, and needs to undertake the corresponding authentication, with appropriate permissions and clear requirements, to allow for a visit. The specific service working architecture is shown in Figure 2:

(4) High-definition shooting of paper medical records and mobile terminals. The basic process of medical record management is to realize the corresponding input and digitization of clinical diagnosis and treatment report by scanning and collecting paper medical record information by using corresponding equipment. On this basis, the corresponding supplement of voice, image, signature, and report can be realized.

(5) Health Level Seven (HL7) heterogeneous data dedicated interface for IoT middleware. The text data conversion interface flow of the paperless electronic medical record management system is shown in Figure 3.

3.2. System Function Modules. The paperless medical record management system includes doctor’s work, nursing work, disease prevention work, medical record quality and safety management, medical record remote borrowing and statistical analysis of scientific research, and other functional modules. Module relationship of paperless electronic medical record management system is shown in Figure 4.

(1) Doctor work and nursing work module. ① Doctor work module, including outpatient doctor workstation and inpatient workstation, designed according to the diagnosis and treatment process, the patient is admitted to the hospital to establish the medical record home page information, and then the doctor receives the consultation and collects the patient’s family medical history, past medical history, various examinations, treatment records, and drug allergies through the system. If the patient needs surgical treatment, the system is connected to the surgical anesthesia management system to automatically read the informed consent and PACS report documents. At the same time, the mobile nursing terminal of the nurse workstation uploads the collected nursing documents, surgical records, rescue records and nursing care operation records, etc.; when the patient is discharged from the hospital, the discharge record is generated, and the electronic health file is completed; ② nursing work module: according to the nurse’s execution of the doctor’s order and the scan code confirmation of the test specimen, the daily, monthly, and annual workload and total of a single nurse can be counted. The workload of each ward of the hospital provides a reference basis for the performance evaluation of individual nurses and the hospital. The nursing workstation can also record the patient’s specimens for examination, the execution of hospital orders, and the disinfection of medical equipment. The paperless electronic medical record management system adopts closed-loop management, which greatly reduces the repeated entry operations of medical workers and has stored a large amount of practical data in the database. Doctors rarely need to type in their work and only need to use the mouse to click on the function. The key and template describe the segment, just input, and modify certain specific content.
(2) Disease prevention work module includes 2 submodules of disease reporting and review and hospital feeling registration and review. (3) Disease reporting and review submodule: the doctor on duty logs in to the disease monitoring and reporting system in the doctor’s workstation with his default authority. The system automatically reads patient information from the paperless electronic medical record management system and performs heterogeneous data through data middleware homogeneous processing, screening correct patient information, and filling in the diagnosis information related to the disease after the doctor’s review; (2) hospital infection registration and review submodule: hospital infection management personnel access the paperless electronic medical record management system according to their authority, sorting and patient-related clinical information on hospital infections can be screened, reviewed, and analyzed, and finally generated hospital infection statistical reports. The reports include information such as urethral intubation use, ventilator use, multidrug resistance monitoring, and pathogenic microorganism monitoring.

(3) Medical record quality and safety management module. This module mainly includes two submodules: medical record form review and medical record safety management. (1) Medical record form review submodule: when the patient is discharged from the hospital, the head nurse will organize the medical record and check the completeness of the medical record and the order of the medical record through the mobile nursing terminal. After the medical record is issued by the doctor in charge at the doctor’s workstation, the department director and department quality control personnel conduct the review and then send it to the medical record room. The medical record room staff reviews each electronic medical record. The system also sets up a quality control expert spot check work interface; (2) medical record safety management submodule: medical records are archived within 3 days from the day the patient is discharged. The system reminds doctors of necessary tasks. After the medical records...
are filed, no one is allowed to damage, destroy, alter, forge, or steal medical records at will, to ensure the integrity and accuracy of the electronic medical records, and not to borrow or modify them at will.

(4) The remote borrowing and reading module of medical records. This module includes permission setting and loan application review and statistics. Doctors authorized by the system can check the patient’s medical records, medical history, treatment measures, and insurance details. After the medical record digital filing system is created, digital network resources can be shared. Different personnel can simultaneously access the same medical record in different places. Multiple departments borrow the same medical record at the same time; so, clinicians do not need to go back and forth to the medical record department to read the paper medical records, which saves time for inquiry and retrieval, support discharge follow-up and patient online service platform for mutual visits through interface data, and also provide patients with electronic data copy services such as medical imaging examination images, surgical videos, and interventional operation videos. The current service items that are gradually introduced include some operations of the surgical anesthesia system, system image data and surgical records, PACS original acquired images of digital imaging and communication of medicine (DICOM) 4 format sequence data sets, detailed report data of biological tests, and critical data in emergency and intensive care.

(5) Scientific research statistics module includes the home page search of medical records and the full text search of medical records. Mobile medical devices and wearable devices can not only detect and track personal health data but also help diagnose diseases. Home monitoring devices such as electronic blood pressure monitors have become popular. Wearable devices help big data collect high-quality data, provide healthy decision-making and optimize treatment effects, provide diet adjustment and medical care solutions, and provide hospitals and scientific research institutes with valuable scientific research data. The data mining statistical analysis function can convert various data streams into standardized data and conduct a comprehensive analysis of the obtained medical big data in a unified manner.

A comprehensive analysis of the medical big data is obtained.

As shown in Figure 5, the system in this article includes five modules, namely, the client, the random number generation center, the ciphertext storage center, the decryption module, and the computing center. It is assumed that the modules are independent of each other, and the communication channel between the client and the server is secure.

The functions of each module are as follows:

- **Client** defines the polynomial function used to perform ciphertext operations and sends it to the random number generation center to obtain statistical information about personal data. During the whole process, the client does not know the intermediate process and can only obtain the final result through the above function.

- **Random number generation center**: input function $f$ and output random number sends it to decryption module, ciphertext storage center, and computing center through steps (1), (2), and (3). Ciphertext storage center protects the privacy of data, encrypts the plaintext, and then passes the encrypted data to the computing center. Without the decryption key, the original data cannot be learned.

- **Decryption module** possesses the decryption key of the system, receives the ciphertext passed from the computing center and calculate it, then randomizes the result with the random number passed by the random number generation center and then passes it to the computing center, and finally decrypts the final result passed from the computing center and return it to Client.

- **Computing center** receives the ciphertext, polynomial function, and random number passed by other modules, performs addition and multiplication calculations on the encrypted ciphertext, then calls the decryption module to decrypt the calculation result, and finally encrypts the final result and transmits it to the decryption module.
4. Simulation Experiment

4.1. Simulation Environment. The Internet of Things technology is tested on the PC host. The CPU of the host is 2.4GHz and stored in 1G memory. Set the number of system encryption of medical records to 200 and analyze 6 types of main encryption in the early stage, such as buffer overflow and restriction conditions. Some false encrypted information is added to the medical record source code to detect the algorithm.

4.2. Data. The data of a hospital’s paperless electronic medical record management system in the past two years were selected to compare the paperless rate, medical record review rate, and electronic medical record query times before and after the system was used.

4.3. Statistical Methods. SPSS25.0 software was used for statistical analysis of the collected data, and the rate of counting data (%) was expressed by $X^2$ test. $P < 0.05$ was considered statistically significant.

4.4. Application Results. The original algorithm is applicable when the server is trusted, because when the user requests the server to retrieve the keyword, the user must send the encryption key $p$ to the server. In this way, the ciphertext data stored by the user will be completely transparent to the server. If the algorithm is applied to the cloud storage system with untrusted server, the information stored on the server is likely to be leaked, and the security of the information cannot be guaranteed.

The cloud storage system adopts a typical client-server model. The overall structure is shown in Figure 6.

As can be seen from the structure diagram in Figure 6, the storage of the system is mainly divided into client terminal, random number generation, ciphertext storage, decryption module, and computing center. Each module is divided into independent parts with safe links.
medical records are more secure and reliable, which can ensure the effectiveness, safety, and accuracy of medical records, improve the efficiency of relevant staff, further reduce the burden of medical workers, and improve the real-time storage and safety management of medical records.

It can be seen from Table 1 that compared with the traditional encryption method based on rule matching, the medical record encryption storage algorithm based on the Internet of Things has higher accuracy (97.4%), while the encryption time is shortened by 42.3%, which has the advantages of fast and efficient. According to the experimental contrast of the five thresholds in Table 2, 0.95 is used as the similar matching threshold. The algorithm has better balance, high accuracy, false alarm rate ≤ 26%, report leakage rate ≤ 4.5%, false alarm rate, and report leakage rate All remain at a low level. In addition, the threshold can also be adjusted appropriately according to the specific encryption request to meet different encryption requirements to realize the encryption object.

5. Conclusions

With the continuous development and application of Internet of Things technology, individuals pay more and more attention to the management of medical information. In view of this demand and limitation, this paper introduces the Internet of Things technology, analyzes and constructs the medical record encryption management system by sorting out the business process of patients, doctors, and nurses, makes a comparative analysis before and after the system goes online, and conducts simulation experiment research. The simulation results show that the medical record encryption storage system based on the Internet of Things technology can effectively solve the collection, statistics, and integration of patients’ medical record information, form an electronic medical record management system with unified data format, data sharing, and device interconnection, and realize the whole process of patients’ medical record information collection.

Data Availability

Data sharing are not applicable to this article as no datasets were generated or analyzed during the current study.

Conflicts of Interest

The authors declare no competing interests.

Acknowledgments

This study is sponsored by the First Hospital of Jilin University.

References

[2] A. Tembhare, S. Sibi Chakkaravarthy, D. Sangeetha, V. Vaidhi, and M. Venkata Rathnam, "Role-based policy to...


