東海大學電機工程學研究所

碩士學位論文

運用時間戳記之安全存取機制於電子病歷系統

Applying Timestamp of Secure Access Mechanism to Electronic Medical Record System

指導教授：鐘 玉 芳 博士

研 究 生：曾 博 睿 撰

中華民國 108 年 1 月

東海大學電機工程學系碩士學位

考試委員審定書

電機工程學系研究所 曾博睿 君所提之論文，

運用時間戳記之安全存取機制於電子病歷系統，

經本考試委員會審查，符合碩士資格標準。

學位考試委員會 召集人：沈學勰 (簽章)

委 員：陳澤龍

應有婷

鍾玉男

黃愉閔

中華民國 108 年 01 月 04 日

致謝

秉持著對於電機科學的熱愛，我在進入東海大學部就讀後，對於豐富的課程產生了濃烈興趣,因此想要更加鑽研此領域的心也隨著學習廣度增加而日益堅定。在經過長期的思考，我想要更加鑽研、參與學術研究，並且很幸運地得到了教授們的青睞，而成為了該所的研究生。在這兩年中，我選擇在資訊安全與資料加解密領域做更進一步的研究，途中雖有跌跌撞撞，卻也在教授們的指導與實驗室夥伴的幫助之下，完成了學業，也將我的心血與心得撰寫成這篇論文，因此我想要個別致謝這些對我提供協助的人。

感謝指導教授鐘玉芳老師與師丈陳澤雄老師的推薦，讓我成功進入東海電機研究所就讀，開啟了我鑽研該領域的大門。而也因為教授們不間斷的鼓勵與指導，使我在資訊安全與醫療系統的領域中，能夠提出自己的見解並且使用學術研究方法、運用科學、理性的探討其中的議題並撰寫出本篇論文。此外，我也要感謝口試委員沈榮麟博士、陳澤龍博士、廖郁婷博士、黃愉閔博士對於論文的指正與建議，讓我能夠將此篇論文修飾地更為完整。再來也要感謝我的實驗室夥伴們冠曆與雅昕，在我寫論文與準備口試時提供了許多幫助，也陪我度過了無數的難關，一起在研究所生活中，一一克服各種挑戰。

曾博睿 謹誌

中華民國 108 年 1 月

論文名稱：運用時間戳記之安全存取機制於電子病歷系統

校所名稱：東海大學電機工程學系研究所

畢業時間：2019 年 01 月

研究生：曾博睿　　指導教授：鐘玉芳

論文摘要:

隨著資訊網路日益發達，眾多使用者開始將個人或企業的重要機密文件以數位的方式存放於網路環境中，以利進行網路資源共享，而網路環境本身屬於公開的環境，若是缺乏管理這些重要資訊的存取權限，將可能會誘使網路上的惡意攻擊者對重要資料進行非法存取或是非法使用者在未經授權的情況下任意刪除或修改資料。另一方面，個人隱私資料的保護是現今資訊安全領域的重要議題，因此，透過對使用者存取資料的權限管理確實能有效的防範資料竊取或是資料竄改的問題，藉由實行特定時間發放給合法使用者解密金鑰是必要的。

早期的醫療機構主要是以傳統紙本的方式來記錄醫療資訊，包括病歷資料、護理資料、藥劑資料、檢驗資料等，但也面臨到資料存放空間，以及資料管理上的問題。近年來，各大醫療機構開始採用電子化資料庫系統來存放醫療資訊，包含病患個人資料、醫療機密資訊等，以數位化的形式透過網路將資料存放在資料庫，本論文針對病患的病歷資料以及個人健康紀錄，運用行動代理人本身的優勢，在虛擬網路中，代替使用者到不同的醫療機構，合法地收集病患的醫療資訊，實現跨醫療機構的資訊分享概念，並且使用公開加密系統和 Lagrange 插值法提出一個金鑰管理以及資料存取機制，以提升與維護醫療資訊分享的保密性和安全等級。

此外，採用 Lagrange 插值法的目的主要是對合法使用者進行存取時間的管理，讓特定時間內，特定的使用者有合法的權限取得受加密資料的解密鑰匙，同時，因為各密鑰間沒有相對的關係存在，且各密鑰的產生方式皆為隨機產生，使得非法使用者或是外部攻擊者破解密鑰的困難度會大大的提高。

本論文最後一章節以分析系統的安全性來驗證前面提到的金鑰管理和資料存取控制機制，驗證結果證實論文提到的數學方法，能成功降低密鑰被外部攻擊者破解的機率，為醫療資訊的管理領域，加入一個全新的解決方法。

關鍵字：行動代理人、公開加密系統、Lagrange 插值法、金鑰管理、存取控制

Abstract

With the rapid expansion in information networks technologies, users have begun to store confidential documents of individuals or enterprises in an Internet environment with digital way which facilitates the ability of network resource sharing. The network environment itself is a public form of environment. Lacking access to manage this important information, it may entice unauthorized attackers on the network to illegally access important data, delete or modify data without authorization. On the other hand, the protection of individual privacy has been an important issue in information security. Therefore, effective management in users' authority to access the data can prevent data from being stolen or tampered. It is also necessary to provide legitimate users with decryption key at a particular time.

The early medical institutions recorded medical information mostly in the form of papers which include medical records, nursing materials, pharmaceutical materials, and inspection materials, etc. However, it also faced some difficulties such as data storage capacity and data management. Recently, the majority of medical institutions have begun to use electronic database systems to store the medical information, inclusive of patient personal data, medical confidential information in a digital form to store in the database by means of the network. This thesis is aimed at medical records and personal health records by taking the advantages of the mobile agents. In the virtual network, it legally collects medical information of patients from other medical institutions which realizes the concept of sharing information in all medical institutions. Additionally, it use a public encryption system and Lagrange Interpolation to form a key management and data access control in order to enhance the confidentiality and the level of security in sharing medical information.

Keywords：Mobile Agents, Public Encryption, Lagrange Interpolation, Key Management, Access Control

Content

List of Figures

List of table

Chapter I Introduction

In this chapter, the premise, research motive, the research purpose, and thesis structure were all introduced into this thesis.

Section I Premise

In the era when information transmission system is well developed, information transmitting and receiving are usually happen in an instant. In the past, books and papers are the only two forms which are utilized in transmitting information, and now information can be transmitted and read in digital form. With this method, large amount of information can be instantly stored and shared online which has become the most important way in storing the information. Medical institutions used to manage patient data with manpower and papers which could easily waste resources. Therefore, large medical institutions started to use computers and communication equipment to collect, store, process and transmit the variety of activities in medical institution which includes patient record and administration management in order to meet the users' requirement, in the same time, it can improve patient outcome and decrease the cost on management. Medical management uses HIS which also known as Hospital Information to manage and it is combined by several systems [1]. For instance, management information system (MIS), nursing information system (NIS), laboratory information system (LIS), pharmacy information system (PIS), radiology information system (RIS), picture archiving and communication system (PACS) and clinical information system (CIS).

Each hospital's system is a separate system which leads to the problem of compatibility, so that data cannot be shared with other information system. For example, cases cannot be transmitted during referrals. Therefore, this paper will refer to the network platform and transmission aspect. For instance, Web 2.0 is a practice which

uses internet to transmit data and provides supportive decision for the meeting. The structure of the system is that the main system is connected in parallel with the assisting structure. The implementation of the system includes Internet, Intranet, Extranet. Among all, internet is applied in hospital marketing, patience education, virtual hospital, distance learning, tele-conferencing, on-line reference for clinical practice and research and discussion group/BBS. The application of the Intranet is to use the technology of the Internet to develop the application operating of the organization, which facilitates customer transactions and strengthens internal communication within the organization. The use of Extranet is to connect the LANs or Intranets of the two organizations through the Internet in a secure and secret way, providing organizational information that customers, business partners, vendors and members of the organization the free access. For hospital application, there are referral reports, distance image interpretation and emergency medical care information bulletin.

Information management can improve medical resources and reduce the burden on the doctors. The electronic medical records promoted by the Department of Health and Welfare have been promoted for more than 10 years from the basic level adjustment, system planning and documentation to the verification. To ensure the data security of electronic medical records exchange, each test report must be accompanied by the doctor's electronic stamp and time stamp. At present, many hospitals have started to implement these medical materials under the framework of electronic certificates exchange [2]. In addition to electronic medical records, the Health Insurance Agency is continuing to promote health passbooks and cloud medicines. However, the cloud medication calendar still has to be decided by the public whether to authorize the doctor to view the past data. In other words, the cloud medication calendar is mainly provided to the doctor, so that the doctor can track the patient's previous medication record. Save time in accessing materials and improve the accuracy of drug is used to avoid waste.

Ministry Of Health And Welfare (MOHW) estimates that it can save 1.3 billion Taiwan dollars in drug costs in one season, and hopes to save 30-40 billion Taiwan dollars a year.

Section II Research Motivation

In response to the health insurance system, when the patient visits the doctor, the results of the doctor's examination will be referred to the appropriate medical institution according to the condition of the patient. After the referral, the medical institution will record the condition after the treatment and change according to the patient's condition. Observe treatment in a general ward or a more appropriate medical institution. The hospital's information system has not been developed in cooperation with other hospital systems, resulting in compatibility problems, and electronic medical records will not be instantly transmitted and accessed on the Internet.

The electronic medical records promoted by the Ministry of health and welfare have increased in use every year. However, based on the current hospital information systems (HIS), and the complexity of the system, it is difficult to update them comprehensively. The user's habits are not easy to change, and at the same time, the requirements of the electronic signature must be met. Therefore, most of the methods used by various medical institutions are still unchanged and replaced by the current medical information system, so when the patient turns at the time of diagnosis or visit to other medical institutions, most of the hospitals at this stage will print out the medical records in the information system, and then stick them on the paper medical records. If necessary, they need to be re-examined and recorded. In such cases, often leads to waste of resources, so it is hoped that the case such as transmission and query can be stored through the Internet without interrupting the hospital information system, thereby reducing waste of resources.

東海大學
TUNGHAI UNIVERSITY
1955

Section III Research Purpose

At present, all medical institutions have independently developed medical information systems, such as nursing information systems, digital image storage communication systems, drug information systems, management systems, etc., but medical information has a potential problem of compatibility in various medical institutions. It is impossible to exchange the goods in real time. In order to obtain electronic medical records in various medical systems, if the medical institutions need to replace the new medical information system, the original medical information must be moved to the new system, which requires a lot of time and money. Therefore, the use of medical information that is simpler, more convenient to carry and accessible is the main purpose of this thesis.

In this thesis, an integrated medical information access system is proposed, combined with the several major features of mobile agents. The mobile agent works in a heterogeneous network environment, and the security will be tested. In order to make the mobile agent more secure, we need to understand its features and empower its security measures. The features of the mobile agent can be divided into the following four types: Integrity Attacks, Availability Refusal, Confidentiality Attacks, and Authentication Risks. In order to ensure the security of the mobile agent in transmitting the electronic medical record, the public key encryption method and the Lagrange interpolation polynomial are used as the management and access control mechanism of the key [3-4]. When the mobile agent accesses the electronic medical record, the security performance is greatly improved.

Section IV Thesis Structure

This thesis consists of six chapters plus an abstracts. Firstly, through the abstract, the research motivation and practical application level of this thesis are briefly

introduced. Then, the further introduction into the first chapter summarizes the purpose of this research, research motivation and the composition of the thesis. The content mainly focuses on integrating medical information and security. The large spindle is discussed. The second chapter is the literature discussion which mainly analyzes the detailed research, including the application of electronic medical records and its transmission mechanism and the application of mobile agents in data transfer access. The last part is the preliminary introduction of Lagrange interpolation polynomial. For the third chapter, the mathematical research method is mainly for the Lagrange interpolation polynomial combined with the encryption system to explain the effectively way to manage the user and add time-limited variables, so that users with legal authority (medical staff) can obtain files from the key authentication center. The decryption key, at the same time, verifies whether the access mechanism proposed in this thesis can protect the patient's private data, and uses the equations and entity examples to discuss the research methods. The fourth chapter is about security analysis. Through analysis of four different network data attacks, including equation attack, cooperative attack, reverse attack and external attack, the analysis is carried out in an equation, it combined with the mathematical method of Chapter 3, that is, using the decryption equation of key management to gradually analyze whether different attack types can solve the secure access mechanism proposed in this paper. The fifth chapter is to conclude and to summarize the discussion from the first chapter to the fourth chapter, and the results of the verification illustrate that the time stamp security access mechanism proposed in this paper that combined with the electronic medical record system and the mobile agent can indeed protect the patient. Moreover, it can restrict the medical records and medical staff who manage legal authority. The final chapter is of all the references used during the writing of this paper, including the development of research methods and mathematical formulas.

Chapter II Related Work

Some of related literatures were introduced in chapter II, including electronic medical record, electronic medical record exchange, feature of mobile agent and the Lagrange interpolation.

Section I Electronic Medical Record

In order to assist physicians in improving the efficiency and effectiveness of diagnosis and treatment, including integrated relevant inspection and report results, amount of time saved in the case time, and improve medical quality through the combination of medical information systems. The rest of the work, such as nursing assessment and records, nursing plans, etc., it can save writing time and reduces errors by electronic form. After the electronic medical record is established, it is convenient to transfer and read in the hospital, which can improve the quality of medical treatment for patients, and make clinical decisions. Treatment analysis, medical quality indicators and hospital management audits.

Digitalization is the difference between electronic medical records and traditional medical records, electronic medical records can record more information than paper medical records, and also save more space for files. The electronic medical record (EMR) records the patient's physical condition, which is shown in the Figure- 1 including the past and the future, and is digitally produced. The content includes, transmits, storage, connections, and processes multimedia information. The electronic medical record is mainly auxiliary medical and other related Services [5].

The electronic medical record includes the patient's personal basic information, the main (guest) view, the inspection, the condition assessment, the medical plan, the medical record, the care plan (record), the signs of life, the drug used record, the

surgical consent form, abstract of discharge medical records, relevant medical examination data and inspection reports (including diagnostic imaging reports), past medical history, family history, etc. All necessary information related to the condition is all considered as the electronic medical record content [6].

The electronic medical record can be divided into the following five stages based on the content of the electronic record content: Automated Medical Record, Electronic Medical Record, Patient Medical Record of the provider platform (Electronic) Patient Record), Electronic Patient Record, Electronic Medical Record, etc.

1. Automated Medical Record

The first stage is to turn the paper into an electronic process, replacing the traditional handwritten paper of medical record with an electronic form, and this stage corporates with the electronic process.

2. Electronic Medical Record

The second stage is to make the medical record file into an image file, and the medical record data is completely digitized and represented by an electronic file. The medical records contain medical records, inspection reports (X-ray, CT, MRT, and other medical imaging reports), and medical personnel can obtain these data from hospital computers without passing physical medical records to the clinic or nursing station.

3. Electronic Patient Record

The third paragraph requires good infrastructure, such as the network bandwidth in the data storage device. This stage is a platform for medical personnel or professional therapists to obtain medical records.

4. Electronic Patient Record

The fourth stage is characterized by regionalization and internationalization. According to the recognized interoperability agreement, the sharing mechanism can be

exchanged on the network, and the medical records under the situation which must be secure, consistent, and subject to personal privacy.

5. Electronic Medical Record

The fifth stage is to record the personal medical records from the electronic medical records, and to record the individual's health information, medical history, medical records, etc., to provide inquiries, research and self-management management. An example of EMR system interface is shown as Figure- 1.

Figure - 1 The example of EMR system interface

Section II Electronic Medical Record Exchange Center

EEC (Electronic Medical Record Exchange Center) is an exchange mechanism that can obtain the patient's electronic medical record data (within a period of six months) through the doctor's IC card and the patient's health insurance IC card.

EEC's (Exchange electronic medical record) categories can be divided into four types: medical imaging, blood test reports, outpatient medication records, discharge medical records, and so on.

EEC's exchange environment architecture transmits the information files to the hospitals that provide medical records and then to the electronic medical record exchange center via the EEC gateway (Gateway), which is inquired and inspected by the service personnel and then transmitted to the TES via the EEC gateway (Gateway). After the cross-institution review and signing approval, it can be inquired, reviewed and downloaded. The EEC (Electronic Medical Record Exchange Center) proposed by the Department of Health and Welfare, when transmitting electronic medical records which can be divided into three situations: read beforehand, read immediately (outpatient, emergency, hospitalized) and immediately read (transferred).

1. Medical Images

Various medical images such as CT, MRI, X-ray, tomography, ultrasound and other medical images.

2. Blood Test Report

Record blood reports, such as biochemical blood, immune serum, viral serum, blood routines, etc.

3. Outpatient Medication Record

Record prescriptions for the use of drugs, such as general use of drugs, special drugs, controlled drugs, influenza vaccines and other prescriptions.

4. Discharge Medical Record Summary

Summary diagnostic records at the time of discharge, such as physical examination, surgery, medical history, treatment process, diagnosis, and various examination records.

1. Read Beforehand

First, you must apply for an electronic medical record, and then query the patient's exchangeable electronic medical record information through the administrative staff. After the patient signs the consent form, the doctor can log into the system with the patient's health insurance card and doctor card.

2. Read Immediately (outpatient, emergency, hospitalized)

After the physician logs into the system, the medical staff card will be used to check the patient's exchangeable electronic medical record. If the patient does not sign a valid consent form, the doctor can log into the designated hospital with the assistance of the patients, and then print the consent form and ask the patient to sign. After that, the doctor can check the required electronic medical record and you can read it.

3. Read Immediately

At the time of transfer, the doctor obtains the patient consent form and logs in to the transfer system to complete the patient transfer related information. After that, the system automatically transfers the selected electronic medical record to the designated hospital and then transfers to the hospital. The doctor logs in to the system with the patient health insurance card and the doctor card. The system will display the patient's transfer information, and after a valid consent is signed, the physician will have access to the medical record.

Section III Features of Mobile Agent

The mobile agent is a virtual program. It is a program that can be autonomously distributed and processed. When it accepts the user's task, it can move between the network and other computers, collected data, perform operations, and send it back to the user. Since the mobile agent adjusts itself to other adaptive networks and adapts itself to the adaptive state, the mobile agent can work in a heterogeneous environment, not limited to the area or the network, and can be applied to high dispersion systems such as medical information systems [7-8].

1. Autonomy

The acting agent has autonomy and can be operated independently. After the user releases the task, he or she adapts according to the execution environment, collects information, and returns after the operation.

2. Mobility

Mobile agents can act autonomously in other network environments and are the main characteristics of mobile agents.

3. Flexibility

In a heterogeneous network environment, you can change your status and adapt to the situation.

4. Goal-driven

The user will set a specific target at the source, and the mobile agent will achieve the goal.

5. Collaboration

Mobile agents can communicate with other agents through programming language and exchange information to collaborate.

6. Temporarily Continuous

The mobile agent can continue the task or after a period of time.

7. Learning

The efficiency of performing tasks in the future can be improved by completing multiple tasks and accumulating experience in collecting data and processing data.

The mobile agent will move around the Internet during the process of performing the task, and will exchange information with different servers or other agents, so it will face security threats. The main threats can be divided into the following four types: Authentication Risks, Availability Refusal, Integrity Attacks, and Confidentiality Attacks are detailed below.

1. Authentication Risks

   The duplicated mobile agent allows the mobile agent to be properly identified by other servers, or to set up a malicious server to direct the mobile agent to execute the program on his platform in order to steal information from the mobile agents.

2. Availability Refusal

   The server refuses to allow the mobile agent to access the data, or refuses to transmit the mobile agent to the next server, thereby delaying the service delivery time.

3. Integrity Attacks

   Malicious deletion, modification or addition of the agent's code, status, etc., or the failure to fully implement the mobile agent program, so that the action agent's information is not fully executed, resulting in incomplete information.

4. Confidentiality Attacks

   Use malicious servers to monitor or analyze the data, execution code or embarrassment brought by the action agent to steal confidential information.

Section IV Fundamental Principle and Application of Lagrange Interpolation

The Lagrange Interpolation algorithm is named after the famous 18th century mathematician Joseph-Louis Lagrange. Applications include physics, astronomy, and numerical analytics, using functions to represent the results and laws that exist between

results, and using this mathematical method to quickly find the unique polynomial through several distinct points on the *x*-*y* plane. When the difference point coordinates are very large, it is a very suitable choice to solve using Lagrange Interpolation method [9-10].

Below we use mathematical formulas to derive the description. First, let us assume that n+1 points (x_0, y_0), (x_1, y_1), …, (x_n, y_n), and $x_0, x_1, \ldots x_n$ given on the *x*-*y* plane are different, where Lagrange Interpolation provides a unique polynomial of n times through n+1 points.

Suppose there is a polynomial function passing the following point coordinates: (x_0,y_0), … , (x_n,y_n), where x_j corresponds to the position of the argument, and y_j corresponds to the value of the function at this position, ie the function $y_j = f(x_i)$. Assuming that any two different x_j are different from each other, then using the Lagrange Interpolation polynomial, you can get a function form:

$$L(x) = \sum_{j=0}^{n} y_j l_j(x) \tag{2.1}$$

Where $l_j(x)$ is a Lagrange essential polynomial whose expression is as follows:

$$l_j(x) = \prod_{i=0, i\neq j}^{n} \frac{x - x_i}{x_j - x_i} = \left(\frac{x - x_0}{x_j - x_0}\right)\ldots\left(\frac{x - x_{j-1}}{x_j - x_{j-1}}\right)\left(\frac{x - x_{j+1}}{x_j - x_{j+1}}\right)\ldots\left(\frac{x - x_n}{x_j - x_n}\right) \tag{2.2}$$

$l_j(x)$ is characterized by taking a value of 1 on x_j and a value of 0 on other points x_i ($i \neq j$), which is expressed as follows:

$$l_j(x) = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases} \tag{2.3}$$

In the last part, we explain the principle by example: find a minimum number of polynomials $f(x)$ to make its graph pass points A(2,4), B(4,0), C(6,8), D(8,6), E(8,10). Find the y coordinate of the point F(40, y).

First, list each basic Lagrange polynomial:

$$l_1(x) = \left(\frac{x-2}{1-2}\right)\left(\frac{x-3}{1-3}\right)\left(\frac{x-4}{1-4}\right)\left(\frac{x-5}{1-5}\right)$$

$$l_2(x) = \left(\frac{x-1}{2-1}\right)\left(\frac{x-3}{2-3}\right)\left(\frac{x-4}{2-4}\right)\left(\frac{x-5}{2-5}\right)$$

$$l_3(x) = \left(\frac{x-1}{3-1}\right)\left(\frac{x-2}{3-2}\right)\left(\frac{x-4}{3-4}\right)\left(\frac{x-5}{3-5}\right)$$

$$l_4(x) = \left(\frac{x-1}{4-1}\right)\left(\frac{x-2}{4-2}\right)\left(\frac{x-3}{4-3}\right)\left(\frac{x-5}{4-5}\right)$$

$$l_5(x) = \left(\frac{x-1}{5-1}\right)\left(\frac{x-2}{5-2}\right)\left(\frac{x-3}{5-3}\right)\left(\frac{x-4}{5-4}\right) \quad (2.4)$$

Then using the Lagrange Interpolation polynomial, we can get the expression of $L(x)$, and $L(x)$ is the interpolation function of the function $f(x)$:

$$L(x) = f(2)l(1) + f(4)l(2) + f(6)l(3) + f(8)l(4) + f(8)l(5)$$

$$= 4 \times \left(\frac{x-2}{1-2}\right)\left(\frac{x-3}{1-3}\right)\left(\frac{x-4}{1-4}\right)\left(\frac{x-5}{1-5}\right) + 0 \times \left(\frac{x-1}{2-1}\right)\left(\frac{x-3}{2-3}\right)\left(\frac{x-4}{2-4}\right)\left(\frac{x-5}{2-5}\right) + 8$$
$$\times \left(\frac{x-1}{3-1}\right)\left(\frac{x-2}{3-2}\right)\left(\frac{x-4}{3-4}\right)\left(\frac{x-5}{3-5}\right) + 6 \times \left(\frac{x-1}{4-1}\right)\left(\frac{x-2}{4-2}\right)\left(\frac{x-3}{4-3}\right)\left(\frac{x-5}{4-5}\right)$$
$$+ 10 \times \left(\frac{x-1}{5-1}\right)\left(\frac{x-2}{5-2}\right)\left(\frac{x-3}{5-3}\right)\left(\frac{x-4}{5-4}\right)$$

(2.5)

At this point, you can find the required value by substituting 40:

$$L(x) = f(x), \qquad L(40) = f(40) = 2933220 \quad (2.6)$$

Chapter III Research Method

With the digitization of medical information, users can store data in the back-end database via the Internet or access and browse data with legal rights. However, the issue of security and personal privacy has also become a major issue of security. Therefore, the purpose of this thesis is to construct a medical information integration system, by giving legal users permission to access data inventory at a specific time, and based on Hierarchical management mechanism and Lagrange Interpolation method add time variables to control the decryption key in the effective time to solve the problem of data access security and privacy [11-12]. In addition, the medical record data can be shared across medical institutions. Improve the efficiency and quality of visiting between hospitals.

Section I Electronic Medical Record Information Integrated with Medical System

The emergence of the electronic medical record system effectively improves the quality of medical care in hospitals. When a patient goes to a clinic, the doctor can access the patient's medical records from the hospital database or the electronic medical record trust center. It would increase the correctness of medical diagnosis. Through the establishment of the electronic medical record system and the improvement of medical information equipment, the domestic medical care system can lead other countries in the world. Generally, electronic medical records can effectively solve the problem that paper-based medical records are not immediacy. The database is regularly updated to allow users (patients and medical staff) to obtain the latest medical information [13-14].

With the implementation of electronic medical records, it is far more convenient for patients or other medical institutions to access personal medical records through the legal verification. Therefore, this research method encrypts medical records via public encryption system and Lagrange Interpolation, and then adds timestamp to limit the access for the legitimate users. The management mechanism sends legitimate users to decrypt the files, allows the user to access the file with the decryption key, and then transmits the file data to the user's computer through the mobile agent [15-16]. The picture shown below in Figure- 2 is a flow chart of the patient's visiting the hospital to see doctors and the schematic diagram of mobile agent trying to cross-institutionally access to confidential medical record.

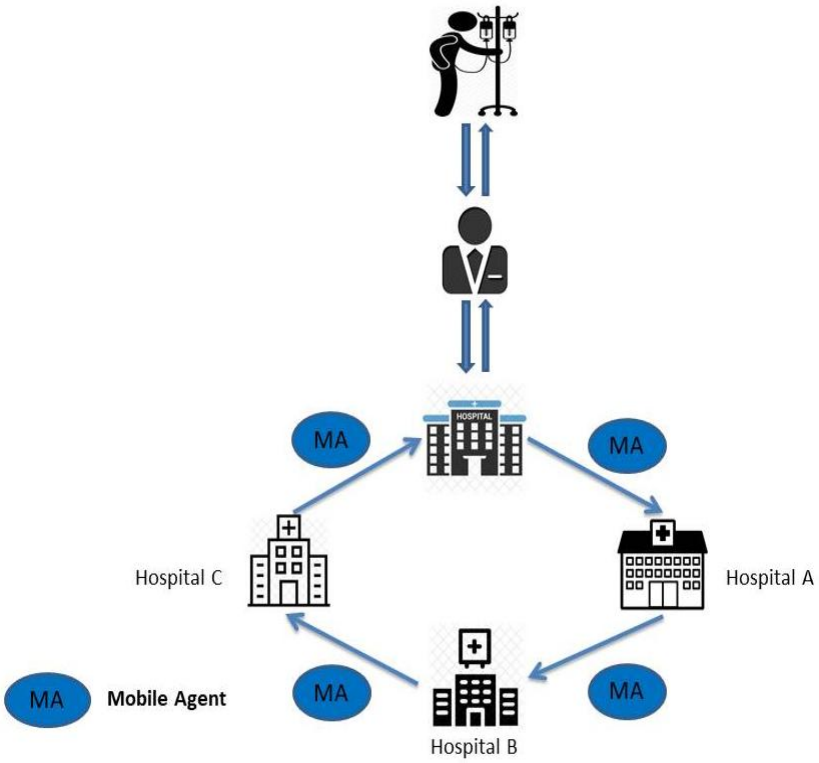

Figure - 2 The structure of mobile agent having cross-institutional access to confidential medical record

Table 1. Algorithm parameters of public encryption system

Symbol	Definition
CA	Key Authentication Management Center, mainly for issuing keys for managing users and files
S_i	Server (user of the system)
ID_t	Confidential file number
TS	The time set of the Kth hour
K_i	Corresponding to the secret key of each legitimate user
DK_t	Corresponding to the ID_t decryption key
$F_{DKt}(x_{i,t})$	Public access polynomial of the decryption key

Section II Key Production in Specific Time Interval

Our main goal is to create the scheme that it can utilize the key to give user a right to access a particular document at particular hours taking values in {1,...,24}. We generalize the decryption polynomial $F_{DKj}(x)$ subject to the previous criterion. Suppose that for Sj, TS is a set collect the hours labeled by integers from 1 to 24 that the server Sj can access the documents as usual. We derive the time-restriction key as following.

Step 1. Randomly pick two large prime numbers p and q as the roots of finite field $GF(p)$. Number g and p remain public.

Step 2. Each confidential document will have non-repetitive decryption key DK_j, $j = 1,...,n$, where n represents the number of documents.

Step 3. Choose non-repetitive secret key K_i, $i = 1,..., m$, where m is the number of users existing in the system.

Step 4. The mobile agent owner constructs a set of input keys as shown below:

$$x_{i.j.t} = 24\left(q^{k_i \| ID_j} \bmod p\right) + \left(\prod_k \left(t - TS(k)\right) \bmod 24\right) \tag{3.1}$$

Where ID_j represents the number of DK_j, $TS(K)$ represents the time set of the Kth hour. If $DK_j \leq S_i$, it means S_i has legitimate right to get the decryption key DK_j. Therefore, we can construct $F_{DKj}(x)$ as below:

$$F_{DK_j} = x + DK_j - \left\{ \sum_{DK_j \leq S_i} x_{ij} l_{ij}(x) + \prod_{DK_j \leq S_i} \left(l_{ij}(x)\right) R \right\} \tag{3.2}$$

where $l_{ij}(x)$ is the Lagrange Interpolation polynomial formulated as

$$\begin{aligned} & l_{ij}\left(b(x)\right) \\ &= \prod_{t=1, t\neq i}^{m} \left(\frac{b(x) - b\left(x_{ij}\right)}{b\left(x_{ij}\right) - b\left(x_{tj}\right)}\right) \\ &= \left(\frac{b(x) - b\left(x_{1j}\right)}{b\left(x_{ij}\right) - b\left(x_{1j}\right)}\right) \ldots \left(\frac{b(x) - b\left(x_{i-1,j}\right)}{b\left(x_{ij}\right) - b\left(x_{i-1,j}\right)}\right) \left(\frac{b(x) - b\left(x_{ij}\right)}{b\left(x_{ij}\right) - b\left(x_{tj}\right)}\right) \ldots \left(\frac{b(x) - b\left(x_{mj}\right)}{b\left(x_{ij}\right) - b\left(x_{mj}\right)}\right) \end{aligned} \tag{3.3}$$

and h function is

$$a\left(l_{ij}(x)\right) = \begin{cases} l_{ij}\left(b(x)\right) - 1, & l_{ij}\left(b(x)\right) = 1 \\ 1, & otherwise \end{cases} \tag{3.4}$$

First, let $b(x)$ be a integer scalar function of x_{ij}. According to equation (3.1), once we have input key x_{ij}, we'll have:

$$b(x) = 24\left(q^{k_i \| ID_j} \bmod p\right) \tag{3.5}$$

Finally, we combine b(x) (3.5) and Hash Function (3.4) into equation (3.2) to get the ideal access polynomial $F_{DKj}(x)$, as shown in equation (3.6):

$$F_{DK_j}(x) = b(x) + DK_j - \left\{ \sum_{DK_j \le S_i} b(x_{ij}) l_{ij}(b(x)) + \left[\prod_{DK_j \le S_i} a\left(l_{ij}(b(x))\right) + (x_{ij} mod\ 24) \right] R \right\} \quad (3.6)$$

Where R is a random integer number.

Section III Decryption Key's Derivation

Next, the derivation of the decryption key can be extended through the two steps of key generation from the previous subsection. The application principle has a very strong correlation with the user's access rights. At the same time, we will also be specific that the time limit is strictly controlled for the user to obtain the decryption key DK_j, and the key authentication management center can store the keys, which they can be issued to the user in the $F_{DKj}(x)$ decryption polynomial, and then the legitimate user, that is, the action The agent can use his own private key (K_i), as well as other given disclosure conditions, to substitute the $F_{DKj}(x)$ polynomial equation, and successfully obtain DK_j. The following steps and expressions assume that the user (Server) has legitimate right to obtain the confidential file [17-18]. With the granted permission from CA, user can utilize the private key to find the decryption key DK_j.

Step 1. Server S_i provides a decryption key DK_j for the user who has legitimate right to access the *j* document.

Step 2. Server S_i substitutes its secret key K_i and decryption key ID_j in the decryption access polynomial $F_{DKj}(x)$ to get DK_j.

Two calculation steps shown above can be carried through the following derivation.

If DK_j is smaller than S_i, the secret key K_i can provide x_{ij} and the Lagrange interpolation polynomial would become:

$$l_{ij}\left(b(x_{ij})\right) = \prod_{t=1,t\neq i}^{m}\left(\frac{b(x)-b(x_{t,j})}{b(x_{ij})-b(x_{tj})}\right) = 1 \tag{3.7}$$

We can substitute $l_{i,j}(x)$ into $a(x)$ for an intact hash function. Namely, this would give us:

$$a\left(l_{ij}\left(b(x_{ij})\right)\right) = \left\{\begin{matrix} l_{ij}\left(b(x_{ij})\right)-1, & for\ i,j \\ 1, & for\ i'\neq i\ or\ j'\neq j \end{matrix}\right\} \tag{3.8}$$

Thus,

$$\prod_{DK_j\leq S_i} a\left(l_{ij}\left(b(x_{ij})\right)\right) = 1\ldots 1\left[l_{ij}\left(b(x_{ij})\right)-1\right]1\ldots 1 = 0 \tag{3.9}$$

Because

$$\sum_{DK_j\leq S_i} b(x_{ij})l_{ij}\left(b(x_{ij})\right) = b(x_{ij}) \tag{3.10}$$

Now suppose that TS_{ij} is the set of TS that includes a time t and the current time is t o'clock, then current time is t, an integer in {1,...,24}. Then we'll get time access discriminant shown below:

$$x_{i,j.6}\ mod\ 24 \tag{3.11}$$

Based on equation 3.11, DK_j can be derived as follows:

$$F_{Dk_j}(x_{ij}) = b(x_{ij}) + DK_{ij} - b(x_{ij}) = Dk_j \tag{3.12}$$

It shows that the decryption key DK_j can be found from the above mathematical formula, which is the output on the right side of the decryption polynomial equation.

Section IV Example

Assume that the hierarchical key management architecture of this paper is used in a medical institution (Figure- 3). The DK_j in the hierarchical access architecture represents the decryption key used to encrypt and decrypt each confidential file. The other internal nodes S_i represent the folders of the respective servers, and K_i represents the secret key owned by the server. When the server S_i has the right to access certain confidential information, the decryption key of the confidential data is placed in the internal node corresponding to the internal node of the server. Therefore, we establish a hierarchical access architecture to manage keys. The secret key is used to obtain the decryption key of the node located on this server. If the server has permission to access a specific confidential file, it can open its corresponding folder, and derive the decryption key of the confidential file by its secret key and the *ID* of the file [19-20]

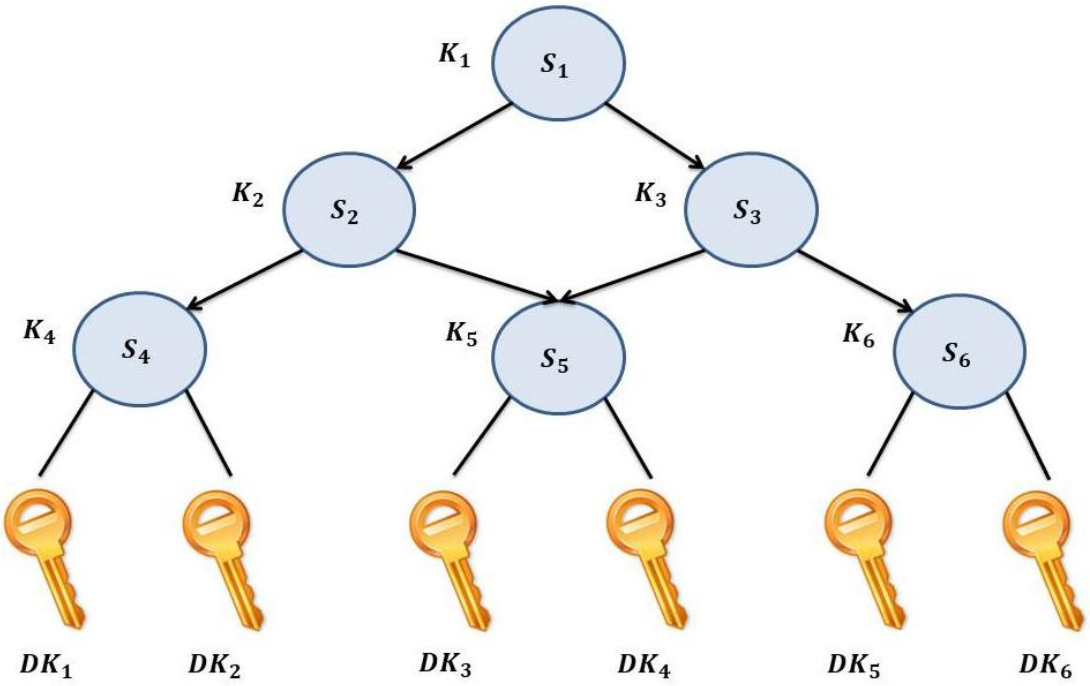

Figure - 3 The architecture diagram of hierarchical access key management

Section V Algorithm Process- Without Adding Timestamp

In the actual examples, we use two different conditional restrictions. In the first part of the operation, we first discuss that the Server (user) enters the database to obtain the confidential file without time access restrictions. Assume that Server (S_6) obtains the credentials of the Key issued by Authentication Management Center and accesses files No. 5 and No. 6 according to the hierarchical access architecture diagram above. First, we provide a key to S_6 to access files No. 1, No. 3 and No. 6. At the same time, S_6 uses the x_{66} input key, and x_{66} is the solution derived from the equation. When i=6 and j=6, x_{66} is obtained from $x_{ij} = \left(q^{K_i \| ID_j} \bmod p\right)$. Next, first calculate the Lagrange interpolation formula of S_6, and substitute $x = x_{66}$ into $l_{16}(x)$, $l_{36}(x)$, and $l_{66}(x)$ to get:

$$l_{16}(x_{66}) = \left(\frac{x_{66} - x_{26}}{x_{16} - x_{26}}\right)\left(\frac{x_{66} - x_{36}}{x_{16} - x_{36}}\right)\left(\frac{x_{66} - x_{46}}{x_{16} - x_{46}}\right)\left(\frac{x_{66} - x_{56}}{x_{16} - x_{56}}\right)\left(\frac{x_{66} - x_{66}}{x_{16} - x_{66}}\right) = 0$$

$$l_{36}(x_{66}) = \left(\frac{x_{66}-x_{16}}{x_{36}-x_{16}}\right)\left(\frac{x_{66}-x_{26}}{x_{36}-x_{26}}\right)\left(\frac{x_{66}-x_{46}}{x_{36}-x_{46}}\right)\left(\frac{x_{66}-x_{56}}{x_{36}-x_{56}}\right)\left(\frac{x_{66}-x_{66}}{x_{36}-x_{66}}\right) = 0$$

$$l_{66}(x_{66}) = \left(\frac{x_{66}-x_{16}}{x_{66}-x_{16}}\right)\left(\frac{x_{66}-x_{26}}{x_{66}-x_{26}}\right)\left(\frac{x_{66}-x_{36}}{x_{66}-x_{36}}\right)\left(\frac{x_{66}-x_{46}}{x_{66}-x_{46}}\right)\left(\frac{x_{66}-x_{56}}{x_{66}-x_{56}}\right) = 1 \quad (3.13)$$

Then, the values of the above three interpolation polynomials are sequentially substituted into the hash function a$\left(l_{ij}(x_{ij})\right)$. When $l_{ij}(x) = 1$, the hash function will output 0; otherwise, when $l_{ij}(x) \neq 1$, the hash function will output 1 and the result as follow:

$$a\left(l_{ij}(x)\right) = \begin{cases} l_{ij}(x) - 1, & l_{ij}(x) = 1 \\ 1, & l_{ij}(x) \neq 1 \end{cases} \quad (3.14)$$

$$a\left(l_{16}(x_{66})\right) = 1$$

$$a\left(l_{36}(x_{66})\right) = 1$$

$$a\left(l_{66}(x_{66})\right) = 0 \quad (3.15)$$

Thus, we have

$$F_{DK_6}(x_{66})$$

$$=$$

$$x_{66} + DK_6 + \{x_{66} + [l_{66}(x) + l_{16}(x) + l_{36}(x)] + a\left(l_{16}(x_{66})\right) \times a\left(l_{36}(x_{66})\right) \times a\left(l_{66}(x_{66})\right)\}$$

$$= x_{66} + DK_6 - [x_{66} + 0] \quad (3.16)$$

$$= DK_6$$

From the above calculation result, the decryption key DK_6 hidden in the decryption polynomial $F_{DKj}(x)$ can be obtained.

In the case that the server S_6 utilizes a key x_*, x_* is not equal to x_{66} and x_* is not equal to any linear combination of other keys (x_{11}, x_{22},... and so on) either, then we'll have:

$$l_{16}(x_*) = \left(\frac{x_* - x_{26}}{x_{16} - x_{26}}\right)\left(\frac{x_* - x_{36}}{x_{16} - x_{36}}\right)\left(\frac{x_* - x_{46}}{x_{16} - x_{46}}\right)\left(\frac{x_* - x_{56}}{x_{16} - x_{56}}\right)\left(\frac{x_* - x_{66}}{x_{16} - x_{66}}\right) = c_1, c_1 \neq 0,1$$

$$l_{36}(x_*) = \left(\frac{x_* - x_{16}}{x_{36} - x_{16}}\right)\left(\frac{x_* - x_{26}}{x_{36} - x_{26}}\right)\left(\frac{x_* - x_{46}}{x_{36} - x_{46}}\right)\left(\frac{x_* - x_{56}}{x_{36} - x_{56}}\right)\left(\frac{x_* - x_{66}}{x_{36} - x_{66}}\right) = c_2, c_2 \neq 0,1$$

$$l_{66}(x_*) = \left(\frac{x_* - x_{16}}{x_{66} - x_{16}}\right)\left(\frac{x_* - x_{26}}{x_{66} - x_{26}}\right)\left(\frac{x_* - x_{36}}{x_{66} - x_{36}}\right)\left(\frac{x_* - x_{46}}{x_{66} - x_{46}}\right)\left(\frac{x_* - x_{56}}{x_{66} - x_{56}}\right) = c_3, c_3 \neq 0,1 \quad (3.17)$$

Substituting the above output value into the $F_{DKj}(x)$ decryption polynomial, after calculating, we obtain:

$$F_{DK_6}(x_*) = x_* + DK_6 - \{x_*(c_1 + c_2 + c_3) + R\} \neq DK_6 \quad (3.18)$$

The above expression can be found because the values of $l_{16}(x_*)$, $l_{36}(x_*)$, $l_{66}(x_*)$ are not equal to 1, so the output value of Hash Function a $\left(l_{ij}(x_*)\right)$ will be equal to 1. So that $F_{DK6}(x)$ is not equal to DK_6, which means that S_6 will not be able to access confidential files.

In another case, when S_6 uses the input key x_{56} and substitutes the Lagrange interpolation, it can be obtained:

$$l_{16}(x_{56}) = \left(\frac{x_{56} - x_{26}}{x_{16} - x_{26}}\right)\left(\frac{x_{56} - x_{36}}{x_{16} - x_{36}}\right)\left(\frac{x_{56} - x_{46}}{x_{16} - x_{46}}\right)\left(\frac{x_{56} - x_{56}}{x_{16} - x_{56}}\right)\left(\frac{x_{56} - x_{66}}{x_{16} - x_{66}}\right) = 0$$

$$l_{36}(x_{56}) = \left(\frac{x_{56} - x_{16}}{x_{36} - x_{16}}\right)\left(\frac{x_{56} - x_{26}}{x_{36} - x_{26}}\right)\left(\frac{x_{56} - x_{46}}{x_{36} - x_{46}}\right)\left(\frac{x_{56} - x_{56}}{x_{36} - x_{56}}\right)\left(\frac{x_{56} - x_{66}}{x_{36} - x_{66}}\right) = 0$$

$$l_{66}(x_{56}) = \left(\frac{x_{56} - x_{16}}{x_{66} - x_{16}}\right)\left(\frac{x_{56} - x_{26}}{x_{66} - x_{26}}\right)\left(\frac{x_{56} - x_{36}}{x_{66} - x_{36}}\right)\left(\frac{x_{56} - x_{46}}{x_{66} - x_{46}}\right)\left(\frac{x_{56} - x_{56}}{x_{66} - x_{56}}\right) = 0 \quad (3.19)$$

Then combine the result with the Hash Function and substitute it into $F_{Dk6}(x)$:

$$F_{DK_6}(x_{56}) = x_{56} + DK_6 - \{x_{56} \times 0 + R\} \neq DK_6 \qquad (3.20)$$

In the equation, the part of the real number (R) and x_{56} cannot be offset, causing the user, that is, S_6 can't obtain the decryption key DK_6, which indicates that the access to the confidential file is strictly protected.

Section VI Algorithm Process- With Adding Timestamp

According to the structure of hierarchical access diagram of Figure- 3, we assume that Server (S_6) has legitimate right to access files No. 5 and No. 6 at between 6 am and 12 am, that is, TS = {6, 7, 8, 9, 10, 11, 12} is within the time limit of data access. Moreover, the known conditions are sequentially substituted into the decryption polynomial $F_{DKj}(x)$, you can derive the decryption key DK_6 required by the server. The derivation steps are as follows:

Suppose we want to provide a key to S_6 to access files No. 1, No. 3 and No. 6. First, we list an Integer Scalar Function:

$$y = b(x) = 24\left(q^{k_i \| ID_j} \equiv p\right) \tag{3.21}$$

When S_6 uses the x_{66} key, we substitute $x = x_{66}$ into $b(x)$ to get y_{66}, then substituting y_{66} into $l_{16}(x)$, $l_{36}(x)$ and $l_{66}(x)$, respectively:

$$l_{16}(y_{66}) = \left(\frac{y_{66}-y_{26}}{y_{16}-y_{26}}\right)\left(\frac{y_{66}-y_{36}}{y_{16}-y_{36}}\right)\left(\frac{y_{66}-y_{46}}{y_{16}-y_{46}}\right)\left(\frac{y_{66}-y_{56}}{y_{16}-y_{56}}\right)\left(\frac{y_{66}-y_{66}}{y_{16}-y_{66}}\right) = 0$$

$$l_{36}(y_{66}) = \left(\frac{y_{66}-y_{16}}{y_{36}-y_{16}}\right)\left(\frac{y_{66}-y_{26}}{y_{36}-y_{26}}\right)\left(\frac{y_{66}-y_{46}}{y_{36}-y_{46}}\right)\left(\frac{y_{66}-y_{56}}{y_{36}-y_{56}}\right)\left(\frac{y_{66}-y_{66}}{y_{36}-y_{66}}\right) = 0$$

$$l_{66}(y_{66}) = \left(\frac{y_{66}-y_{16}}{y_{66}-y_{16}}\right)\left(\frac{y_{66}-y_{26}}{y_{66}-y_{26}}\right)\left(\frac{y_{66}-y_{36}}{y_{66}-y_{36}}\right)\left(\frac{y_{66}-y_{46}}{y_{66}-y_{46}}\right)\left(\frac{y_{66}-y_{56}}{y_{66}-y_{56}}\right) = 1$$

(3.22)

Since we have $y = 24(q^{K_i \| ID_j} \bmod p)$, we can further calculate the results of the hash function through the above three sets of Lagrange interpolation results:

$$a\left(l_{16}\left(b(x_{66})\right)\right) = 1$$

$$a\left(l_{36}\left(b(x_{66})\right)\right) = 1$$

$$a\left(l_{66}\left(b(x_{66})\right)\right) = 0 \quad (3.23)$$

When the server accesses the data at 8:00 in the morning, we can get the following complete Integer Scalar Functions:

$$\left(x_{i,j,8} \equiv 24\right) = (8-6)(8-7)(8-8)(8-9)(8-10)(8-11)(8-12) = 0 \quad (3.24)$$

Therefore, after the above conditional expression is brought into the $F_{DK6}(x)$ polynomial equation, the decryption key DK_6 can be obtained successfully:

$$\begin{aligned} & F_{DK_6}\left(b(x_{66})\right) \\ &= b(x_{66}) + DK_6 \\ &\quad - \{b(x_{66}) \times [l_{66}b(x_{66}) + l_{16}b(x_{66}) + l_{36}b(x_{66})] + a\left(l_{16}b(x_{66})\right) \\ &\quad \times a\left(l_{36}b(x_{66})\right) \times a\left(l_{66}b(x_{66})\right)\} \\ &= b(x_{66}) + DK_6 - [b(x_{66}) + 0] \\ &= DK_6 \end{aligned} \quad (3.25)$$

Assuming that the server is currently accessing the data at one o'clock in the afternoon, a new set of integer scalar functions can be obtained:

$$\left(x_{i,j,13} \equiv 24\right) = (13-6)(13-7)(13-8)(13-9)(13-10)(13-11)(13-12)$$
$$\neq 0 \tag{3.26}$$

From the above results, we can find that its value will not be equal to zero, because the immediate access time of S_6 has exceeded the time scope, we previously assumed ({6,7,8,9,10,11,12}), and then put the equation above (3.26) into $F_{DK6}(x)$, and the result would be:

$$F_{DK_6}\left(b(x_{66})\right)$$

$$= b(x_{66}) + DK_6 - \left\{b(x_{66}) \times [l_{66}b(x_{66}) + l_{16}b(x_{66}) + l_{36}b(x_{66})] + a\left(l_{16}b(x_{66})\right) \times a\left(l_{36}b(x_{66})\right) \times a\left(l_{66}b(x_{66})\right)\right\}$$

$$= b(x_{66}) + DK_6 - [b(x_{66}) + R] \tag{3.27}$$

$$\neq DK_6$$

The right side of the equation will output a non-DK_6 real number, which indicates that the user will not be able to obtain the correct decryption key to access the file, meaning that the file is protected.

The last part is to introduce another case of user failing to access the data. Suppose Server (S_6) uses a key x_0, we have x_* and x_* is not equal to x_{66} or any linear combination of x_{66}, such as x_{11}, x_{22}, x_{33}, and so on. The access time scope *TS* is set between 6 am and 12 pm ({6, 7, 8, 9, 10, 11, 12}). In this part, we assume that S_6 starts to access data at 6 o'clock in the morning, the operation steps are shown as follows:

We can calculate the Lagrange interpolation $l_{16}\left(b(x_*)\right)$, $l_{36}\left(b(x_*)\right)$, $l_{66}\left(b(x_*)\right)$ respectively:

$$l_{16}(x_*) = \left(\frac{x_* - x_{26}}{x_{16} - x_{26}}\right)\left(\frac{x_* - x_{36}}{x_{16} - x_{36}}\right)\left(\frac{x_* - x_{46}}{x_{16} - x_{46}}\right)\left(\frac{x_* - x_{56}}{x_{16} - x_{56}}\right)\left(\frac{x_* - x_{66}}{x_{16} - x_{66}}\right) = c_1, c_1 \neq 0,1$$

$$l_{36}(x_*) = \left(\frac{x_* - x_{16}}{x_{36} - x_{16}}\right)\left(\frac{x_* - x_{26}}{x_{36} - x_{26}}\right)\left(\frac{x_* - x_{46}}{x_{36} - x_{46}}\right)\left(\frac{x_* - x_{56}}{x_{36} - x_{56}}\right)\left(\frac{x_* - x_{66}}{x_{36} - x_{66}}\right) = c_2, c_2 \neq 0,1$$

$$l_{66}(x_*) = \left(\frac{x_* - x_{16}}{x_{66} - x_{16}}\right)\left(\frac{x_* - x_{26}}{x_{66} - x_{26}}\right)\left(\frac{x_* - x_{36}}{x_{66} - x_{36}}\right)\left(\frac{x_* - x_{46}}{x_{66} - x_{46}}\right)\left(\frac{x_* - x_{56}}{x_{66} - x_{56}}\right) = c_3, c_3 \neq 0,1 \quad (3.28)$$

According to the results shown above, we can easily find the hash function inserted in the decryption polynomial, namely, we will get $a\left(l_{i,j}\left(b(x_*)\right)\right)$.

Next, we have to evaluate time access discriminant:

$$x_{i,j.6}\ mod\ 24 \quad (3.29)$$

And then substitute its value into $F_{DK6}(x)$. We can observe that the right side of the equation will not be equal to DK_6. In the case of data access among medical institutions, it means that the user will not be able to copy or access the patient's medical record data.

$$\left(x_{i,j,6} \equiv 24\right) = (6-6)(6-7)(6-8)(6-9)(6-10)(6-11)(6-12) = 0 \quad (3.30)$$

$$F_{DK_6}\left(b(x_*)\right) = b(x_*) + DK_6 - \{b(x_*)(c_1 + c_2 + c_3) + (1+0)R\} \quad (3.31)$$

Chapter IV Security Analysis

This chapter is mainly analyzing the key management mechanism proposed in the paper. For the previous research method, we conduct an analysis with the assistance of actual attack which helps verify the key management and security access mechanism to identify whether it can be executed in real world situation. This makes the confidential information to be effectively protected in order to reach the highest standard. The following four different types of attacks (For instance: Equation breaking attack, collusion attack, external attack, external collective attack) will be demonstrated as a way to delve into the statement [21-22].

Section I Equation Breaking Attack

In the first part, we will first introduce the first potential attack mode, the equation crack attack. This type of attack mode will be the main focus in this chapter, it is mainly because the research method discussed in the previous section is to hide the decryption key DK_j in the equation using the decryption polynomial equation $F_{DKj}(x)$ combined with the time access restriction. However, a malicious attacker or a user who has not yet obtained permission will use the public decryption polynomial $F_{DKj}(x)$ to attempt to illegally obtain the private key K_i using special mathematical methods.

This type of attack method often occurs in users with different permissions in the unauthorized access time range, through the cracking of the private key K_i, and then solve the $F_{DKj}(x)$, we use the actual example to explain in detail:

Suppose there is a server S_i and the internal node server S_j of the mobile agent are simultaneously in the access system, and when both satisfy the relationship of $S_j<S_k$ and $S_j<S_i$, the architecture diagram of Figure- 4 can be determined. Whether the server S_i can solve the secret key K_k of the server S_k by the arithmetic expression under the server S_j. By example, according to the hierarchical access architecture diagram of Figure- 3, the

server S_2 that does not obtain the legal authority and the access time attempts to solve the decryption gold of the server S_3 by using the algorithm below the server S_5 at one o'clock in the afternoon. Key DK_3, we use the following expression to indicate that a malicious attacker attempts to obtain the decryption key:

$$F_{DK_3}(x_{23})$$
$$= x_{23} + DK_3 - \{x_{23} \times (l_{16}(x_{23}) + l_{26}(x_{23}) + l_{36}(x_{23}) + l_{56}(x_{23})) + R\}$$
$$\neq DK_6 \quad (4.1)$$

The server S_2 has its own private key K_2, but in the absence of other important information, for example, S_2 cannot obtain the private key K_3 of S_3, and at the same time, S_2 also doesn't have time access permission, resulting in time access discriminant not equal to 0:

$$(x_{i,j,k} \equiv 24) \neq 0 \quad (4.2)$$

In addition, the server S_2 still needs to solve the huge exponential operation in the decryption polynomial, and the difficult discrete logarithm problem. Finally, the S_2 cannot successfully obtain the decryption key DK_3 of the S_3, so we verify the safe access proposed in this paper. The mechanism does maintain a high level of security for confidential files.

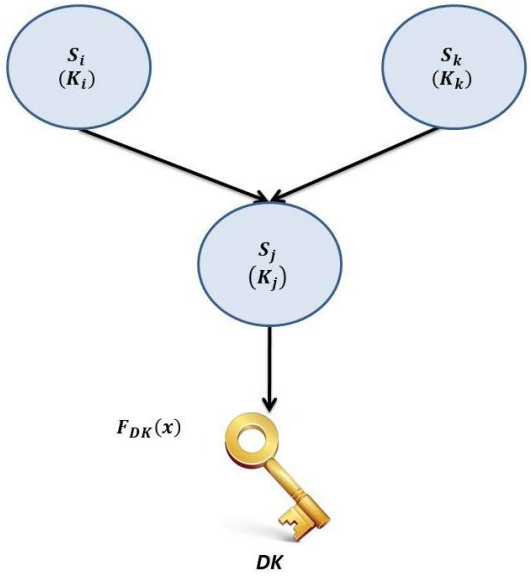

Figure - 4 Equation breaking attack

Section II Collusion Attack

The second part is mainly in the discussion system. Multiple attackers, including internal and external members, try to obtain the decryption key *DK* of the user with higher authority in a cooperative manner. Below we take Figure- 5 as an example. S_j and S_k represent the rights. The lower one is the patient or the doctor, and the S_j is the dean or the hospital executive, which is the user with higher access rights. Basically, the collaborative attack is mainly combined with the users with lower authority, such as the patient and the physician jointly obtains the Dean's decryption key. Since there are many private keys between the attackers, they can be used by each other as input keys. By continuously substituting the decryption polynomial $F_{DKj}(x)$, the probability of the decryption key being cracked is greatly improved. Attacks and coordinated attacks are malicious attacks of a large scale. The number of internal members involved in the attack is relatively large. Even the attack process tends to be diversified, which makes the system maintenance more difficult. In order to solve this problem, the key generation method in this paper adopts a random method, so that there is no regularity between keys, and doctors cannot directly derive the next key by using multiple keys. The system security is based on Crack the access restriction parameters and complex

decryption polynomial functions within a certain time, two major data protection barriers.

Taking the hierarchical access architecture of Figure- 3 as an example, S_3, S_5, and S_6 in the figure are the successors of the server S_1, and S_3, S_5, and S_6 have access rights to DK_3, DK_4, DK_5, and DK_6, respectively. Server S_1 can easily obtain the decryption keys DK_1, DK_2, DK_3, DK_4, DK_5, DK_6 within its authority by using $F_{DK1}(x)$. The following equations can be listed:

$$DK_1 = F_{DK_1}\left(24\left(g^{K_1\|ID_1} \bmod p\right) + \left(\left(\prod_k \left(t - TS(k)\right) \bmod 24\right)\right)\right)$$

$$DK_2 = F_{DK_2}\left(24\left(g^{K_2\|ID_2} \bmod p\right) + \left(\left(\prod_k \left(t - TS(k)\right) \bmod 24\right)\right)\right)$$

$$DK_3 = F_{DK_3}\left(24\left(g^{K_3\|ID_3} \bmod p\right) + \left(\left(\prod_k \left(t - TS(k)\right) \bmod 24\right)\right)\right)$$

$$DK_4 = F_{DK_4}\left(24\left(g^{K_4\|ID_4} \bmod p\right) + \left(\left(\prod_k \left(t - TS(k)\right) \bmod 24\right)\right)\right)$$

$$DK_5 = F_{DK_5}\left(24\left(g^{K_5\|ID_5} \bmod p\right) + \left(\left(\prod_k \left(t - TS(k)\right) \bmod 24\right)\right)\right)$$

$$DK_6 = F_{DK_5}\left(24\left(g^{K_6\|ID_6} \bmod p\right) + \left(\left(\prod_k \left(t - TS(k)\right) \bmod 24\right)\right)\right) \quad (4.3)$$

Since the specific time access management mechanism proposed in this paper selects an interpolation polynomial x_{ij} with time-limited parameters, according to the above equation, the cooperative attackers S_3, S_5, and S_6 must solve the server S_1 by calculating complex polynomial functions. The secret key K_1 of the server S_1 will be

relatively difficult to crack. It can be known from the above mathematical analysis that even if several access levels are relatively low, S_j, S_{j+1}, …, S_{j+k} cooperate together, and the secret key K_i of S_i which is relatively high in access level cannot be obtained. In addition, the decryption polynomial $F_{DKj}(x)$ has the limitation of access in a specific time range, and the probability of success of such an attack is greatly reduced. Therefore, the mechanism proposed in this paper is safe.

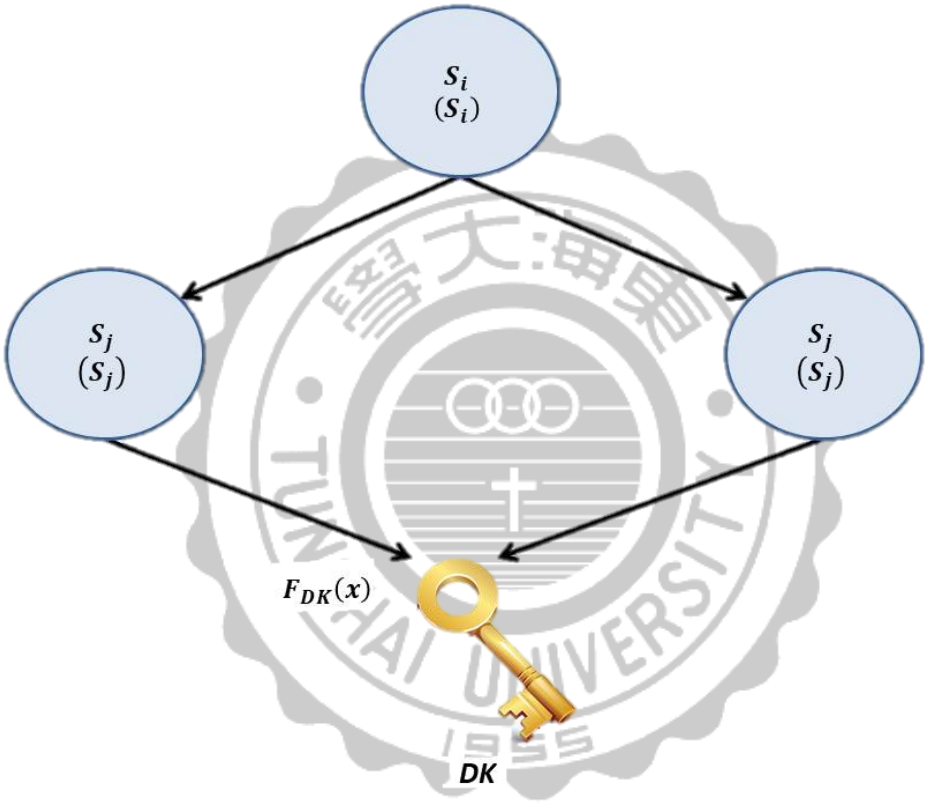

Figure - 5 Collusion attack

Section III Reverse Attack

A reverse attack is a secret key in which a relatively low access level wants to illegally obtain a relatively high access level. Take Figure- 6 for example, S_j represents a physician or a patient with a lower authority, and S_i represents a dean or any user who has a higher authority, if the doctor or the patient illegally obtains the upper secret key,

the key can be used for extra-privileged actions, such as illegal use of the authority's key, for all medical records or medical information. It is one of the necessary security analysis to prevent or reverse the attack by making major mistakes such as tampering or loss of data.

In the method proposed in this thesis, the Lagrange Interpolation function $l_{i,j}(x)$ in the equation is expanded as follows:

$$l_{ij}\left(b\left(x_{ij}\right)\right)=\prod_{t=1,t\neq i}^{m}\left(\frac{b\left(x\right)-b\left(x_{t,j}\right)}{b\left(x_{ij}\right)-b\left(x_{tj}\right)}\right)=1 \tag{4.4}$$

The server S_j and the server S_i are independent individuals. When there is a relationship of $S_j \leq S_i$, the server S_j cannot know the internal information possessed by the server S_i. The server S_j represents an unauthorized user who will pair or collide with information known by himself to find the secret key K_i of the server S_i. According to the access authority architecture, the server S_j can use $F_{DKr}(x)$ to obtain the decryption key DK_r within its authority, that is,

$$DK_r = F_{DK_r}\left(24\left(q^{k_j\|ID_r}\ mod\ p\right)\right) \tag{4.5}$$

But it is difficult that the server S_j wants to utilize the known key DK_r to derive the secret key K_i of the server S_i, because the mechanism proposed in this paper is to select a pair of interpolation polynomials x_{ij} containing time-limiting parameters. In the above expression, the secret key K_i must be based on complex polynomial functions. The calculation is obtained, so it is regarded as a difficult calculation problem in the arithmetic solution. It is very time-consuming to try to solve this function by the server S_j, and the accuracy is relatively low. From the above analysis, the server S_j cannot

know the secret key K_i of the server S_i and thus access the decryption key that the server S_i can access.

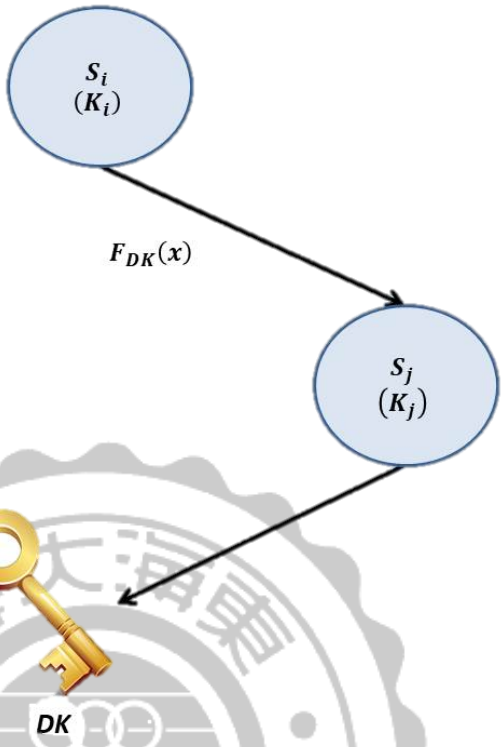

Figure - 6 Reverse attack

Section IV External Collective Attack

In common attacks, most of the attackers are usually not users in the system. The information such as personal data and medical records of patients is personal and accurate. Because of the valuable information and the potential for additional medical peripheral business opportunities, many attackers view medical information as a huge business opportunity, stealing or selling data, causing loss to hospitals or patients, so external attacks are an important security analysis when conducting security factor analysis. External attack refers to whether the outside system of the system intercepts the action agent and can obtain the K_i that you want to know through the system public parameters to access the decryption key to steal or tamper with the internal data. Because the mechanism proposed in this paper wants to know any decryption key DK_j, we must first try to obtain the secret key K_i. To obtain the secret key K_i, we must go

through the calculation of the discrete logarithm problem on the finite field $GF(P)$. So trying to solve this logarithm is very complicated and inefficient. On the other hand, to know that the decryption key must first be calculated by equation $F_{DKj}(x)$ to obtain DK, and because its Lagrange interpolation polynomial exists in the form of expansion, the original content of decryption polynomial $F_{DKj}(x)$ is difficult to be known. As can be seen from the above, the intruder cannot know the information of the secret key K_i and cannot use any of the decryption keys DK. In other words, the information owned by the intruder is not enough to know the secret key K_i or DK, so it is impossible to access the internal data through this information. The mechanism proposed in this paper can resist the attacks of external intruders.

Taking the structure of hierarchical access from Figure- 3 as an example, if you want to obtain useful medical records or medical information, you need to use the obtained public parameters to derive the decryption key and decrypt it to obtain meaningful data or medical records. Suppose there is an external attacker who wants to obtain the decryption key DK_3, according to $F_{DK3}(x)$ and the structure of hierarchical access from Figure- 3.

$$
\begin{aligned}
&F_{DK_3}(x) \\
&= b(x) + DK_3 - \left\{ b(x_{ij}) \times \left(l_{1,3}(b(x)) + l_{3,3}(b(x)) + l_{5,3}(b(x)) \right) \right. \\
&\qquad \left. + \left[\prod_{DK_3 \le S_i} a\left(l_{i,3}(b(x)) \right) + (x_{ij} \bmod 24) \right] \right\} \\
&\neq DK_6
\end{aligned}
\tag{4.6}
$$

He must crack K_1 or K_2 or K_3 or K_5. It is very difficult to crack based on the difference input function x_i, mainly because the complexity of the interpolation function is high, and the attacker needs extra time to crack the time stamp parameters:

$$\left(\prod_{k}\left(t - TS\left(k\right)\right) \bmod 24\right) \tag{4.7}$$

So that the secret key can be effectively protected, and thus the correct decryption key *DK* cannot be derived, so it can be proved that the attacker cannot obtain medical information or medical records illegally by external attacks.

Chapter V Conclusion

This thesis integrates the concept of electronic informatization of medical records to create a safe environment for medical institutions to exchange the information, and then use the mobile agents' techniques to access them, so that medical personnel can effectively obtain patients with complete medical treatment. However, when data is transferred on the Internet, there is a potential risk of being stolen or falsified. Therefore, the restrictions such as hierarchical authority management and the monitoring of time access are added to the authority of the mobile agent which aims at ensuring the confidentiality of the patient information. Under the premise of security, it is effectively and safely provided to legally authorize medical personnel and will not be possessed by unauthorized persons. It can definitely ensure that patient privacy is not violated.

In addition, the research methods proposed in the third chapter of this thesis are particularly worthy of reference in terms of data protection, including solving the decryption key and deriving the time-limiting parameters through the decryption polynomial, and then verifying whether different attacks will caused the data to be stolen or lost by security analysis. Finally, we will check if the algorithm is logically operated, and prove that the data can be effectively protected and not easily stolen.

The methods provided in this paper can be applied not only to the medical records protection, but also to address the needs of medical system referrals, especially when patients are admitted to different medical institutions through emergency departments. In addition, when emergency surgery is required, the medical records can be considered as a reference for physician diagnosis. If the medical records are legally obtained, the patient can be exempted from repeated tests or the waitlist for drug allergy tests which will save the first aid time and it can also prevent the personal data loss and achieve data protection. Finally, it will achieve the initial goal of saving medical resources.

Reference

[1] Medinfo , Healthcare Information Management, http://elearning.hk.edu.tw/medinfo_4.pdf, 10, 2017[Jan. 13, 2018].

[2] E. Bierman, T. Pretoria and E. Cloete, “Classification of Malicious Host Threats in Mobile Agent Computing,” Proceedings of the 2002 annual research conference of the South African institute of computer scientists and information technologists on Enablement through technology, No. 5, pp. 34-49, 2002.

[3] M. h. Guo and D. J. Deng, "Centralised conference key mechanism with elliptic curve cryptography and lagrange interpolation for sensor networks," in IET Communications, vol. 5, no. 12, pp. 1727-1731, August 12 2011.

[4] Young Sil Lee, E. Alasaarela and Hoon Jae Lee, "Secure key management scheme based on ECC algorithm for patient's medical information in healthcare system," The International Conference on Information Networking 2014 (ICOIN2014), Phuket, 2014, pp. 453-457.

[5] Y. Ling, Y. An, M. Liu and X. Hu, "An error detecting and tagging framework for reducing data entry errors in electronic medical records (EMR) system," 2013 IEEE International Conference on Bioinformatics and Biomedicine, Shanghai, 2013, pp. 249-254.

[6] Y. Wan and W. Perry, "Lessons from method: A successful Electronic Medical

Record (EMR) system implementation," Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics, Beijing, 2011, pp. 248-251.

[7] N. Keller and Xiaolin Hu, "Data driven simulation modeling for mobile agent-based systems," 2016 Symposium on Theory of Modeling and Simulation (TMS-DEVS), Pasadena, CA, 2016, pp. 1-8.

[8] D. Patel and J. S. Shah, "Mobile agent and distributed data mining," 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Bangalore, 2016, pp. 548-550.

[9] Y. Jin, Y. Wang, W. Xia, L. Deng and H. He, "A Data Hiding Scheme Based on Lagrange Interpolation Algorithm and Multi-clouds," 2015 Seventh International Symposium on Parallel Architectures, Algorithms and Programming (PAAP), Nanjing, 2015, pp. 210-216.

[10] M. h. Guo and D. J. Deng, " Centralised conference key mechanism with elliptic curve cryptography and lagrange interpolation for sensor networks," in IET Communications, vol. 5, no. 12, pp. 1727-1731, August 12 2011.

[11] A. Castiglione et al., " Hierarchical and Shared Access Control," in IEEE Transactions on Information Forensics and Security, Vol. 11, no. 4, pp. 850-865, April 2016.

[12] S. G. Antoshchuk, A. A. Blazhko and E. Saoud, " Automated design method

of hierarchical access control in database,& quot; 2009 IEEE International Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Rende, 2009, pp. 360-363.

[13] V. El-khoury, N. Bennani and A. M. Ouksel, " Distributed Key Management in Dynamic Outsourced Databases: A Trie-Based Approach," 2009 First International Conference on Advances in Databases, Knowledge, and Data Applications, Gosier, 2009, pp. 56-61.

[14] T. T. Tsai and Y. M. Tseng, "Revocable Certificateless Public Key Encryption," in IEEE Systems Journal, vol. 9, no. 3, pp. 824-833, Sept. 2015.

[15] M. Mahdavian, H. Nazarian, M. Mahdavian and N. Wattanapongsakorn, "An investigation of the success of hospital information systems implementation: A case study," 2014 International Computer Science and Engineering Conference (ICSEC), Khon Kaen, 2014, pp. 329-333.

[16] Z. M. Ozsoyoglu and J. Wang, " A keying method for a nested relational database management system," [1992] Eighth International Conference on Data Engineering, Tempe, AZ, 1992, pp. 438-446.

[17] W. Shoukun, W. Kaigui and W. Changze, "Attribute-Based Solution with Time Restriction Delegate for Flexible and Scalable Access Control in Cloud Storage," 2016 IEEE/ACM 9th International Conference on Utility and Cloud

Computing (UCC), Shanghai, 2016, pp. 392-397.

[18] A. Castiglione, A. De Santis, B. Masucci, F. Palmieri, A. Castiglione and X. Huang, "Cryptographic Hierarchical Access Control for Dynamic Structures," in IEEE Transactions on Information Forensics and Security, vol. 11, no. 10, pp. 2349-2364, Oct. 2016.

[19] Gang Hu, "Study of file encryption and decryption system using security key," 2010 2nd International Conference on Computer Engineering and Technology, Chengdu, 2010, pp. V7-121-V7-124.

[20] V. Odelu, A. K. Das and A. Goswami, "LHSC: An effective dynamic key management scheme for linear hierarchical access control," 2013 Fifth International Conference on Communication Systems and Networks (COMSNETS), Bangalore, 2013, pp. 1-9.

[21] J.H.P. Eloff, M.M. Eloff, 2005, “Information Security Architecture”, Computer Fraud & Security, pp.10-16.

[22] Mikko T. Sipone, Harri Orinas-Kukkonen, 2007, “A Review of Information Security Issues and Respective Research Contributions”, The Database for advance information systems. pp. 60-80.