J Med Syst
DOI 10.1007/s10916-010-9595-8

ORIGINAL PAPER

A Study on Agent-Based Secure Scheme for Electronic Medical Record System

Tzer-Long Chen · Yu-Fang Chung · Frank Y. S. Lin

Received: 22 July 2010 / Accepted: 7 September 2010

Abstract Patient records, including doctors' diagnoses of diseases, trace of treatments and patients' conditions, nursing actions, and examination results from allied health profession departments, are the most important medical records of patients in medical systems. With patient records, medical staff can instantly understand the entire medical information of a patient so that, according to the patient's conditions, more accurate diagnoses and more appropriate in-depth treatments can be provided. Nevertheless, in such a modern society with booming information technologies, traditional paper-based patient records have faced a lot of problems, such as lack of uniform formats, low data mobility, slow data transfer, illegible handwritings, enormous and insufficient storage space, difficulty of conservation, being easily damaged, and low transferability. To improve such drawbacks, reduce medical costs, and advance medical quality, paper-based patient records are modified into electronic medical records and reformed into electronic patient records. However, since eletronic patient records used in various hospitals are diverse and different, in consideration of cost, it is rather difficult to establish a compatible and complete integrated electronic patient records system to unify patient records from heterogeneous systems in hospitals. Moreover, as the booming of the Internet, it is no longer necessary to build an integrated system. Instead, doctors can instantly look up patients' complete information through the Internet access to electronic patient recoreds as well as avoid the above difficulties. Nonetheless, the major problem of accessing to electronic patient records cross-hospital systems exists in the security of transmitting and accessing to the records in case of unauthorized medical personnels intercepting or stealing the information. This study applies the Mobile Agent scheme to cope with the problem. Since a Mobile Agent is a program, which can move among hosts and automatically disperse arithmetic processes, and moves from one host to another in heterogeneous network systems with the characteristics of autonomy and mobility, decreasing network traffic, reducing transfer lag, encapsulating protocol, availability on heterogeneous platforms, fault-tolerance, high flexibility, and personalization. However, since a Mobile Agent contacts and exchanges information with other hosts or agents on the Internet for rapid exchange and access to medical information, the security is threatened. In order to solve the problem, this study proposes a key management scheme based on Lagrange interpolation formulas and hierarchical management structure to make Mobile Agents a more secure and efficient access control scheme for electronic patient record systems when applied to the access of patients' personal electronic patient records cross hospitals. Meanwhile, with the comparison of security and efficacy analyses being the feasibility of validation scheme and the basis of better efficiency, the security of Mobile Agents in the process of operation can be guaranteed, key management efficacy can be advanced, and the security of the Mobile Agent system can be protected.

Keywords Electronic medical record · Lagrange's interpolation · Access control · Mobile agent · Information security

T.-L. Chen (✉) · F. Y. S. Lin
Information Management Department,
National Taiwan University,
Taipei, Taiwan
e-mail: d97725005@ntu.edu.tw

F. Y. S. Lin
e-mail: yslin@im.ntu.edu.tw

Y.-F. Chung
Electrical Engineering Department, Tunghai University,
Taichung, Taiwan
e-mail: yfchung@thu.edu.tw

Published online: 21 September 2010

Introduction

With the development of the Internet, the transmission of data has been greatly changed and the speed of data transmitting and spreading has also become faster. In medical organizations, medical personnel have to quickly understand the complete medical information of patients in order to make instant and accurate diagnoses as well as to provide appropriate treatments. Medical information is recorded in patient records which contain medical files of patients, observations, diagnoses, and treatments records of diseases, nursing actions from medical personnel, and various examination results from allied health profession departments. The purpose of medical records is to provide the continuity of care. Traditional paper-based patient records therefore appear the following drawbacks [1–6].

(1). Disorganization. Since there is no strictly uniform format of patient-record forms in various medical organizations, traditional paper-based patient records are lack of organization. With medical information from various sources keeping in one patient record, it would take time to analyze and obtain the systematical data that will be even more difficult as the data are likely to be damaged after being kept for a long period of time.
(2). Low data mobility. With traditional paper-based patient records, data are searched, transferred, and kept through man-carrying; and the same patient record cannot be simultaneously available for several people.
(3). Illegibility. Traditional paper-based patient records are marked with medical information in handwriting, which could result in illegibility after a long period of conservation in ill-conditions and further cause medical malpractice claims. In this case, not only is the patient's health not protected, but the medical cost is also lost.
(4). Space requirement and conservation difficulty. Traditional paper-based patient records are so easily affected by the external environment that the temperature, humidity, space, data access control of unauthorized personnel, and moreover natural disasters must be paid more attention to.
(5). Low Transferability. In such a high-mobility society, people hardly take all medical treatments in a single medical organization. However, the transfer of patient-record information among medical organizations is not so convenient that patients have to individually apply for personal patient records, copy the data, and bring them to other medical organizations. The low transferability could possibly also be at the risk of data security.

In order to solve the above problems as well as to reduce medical cost and to enhance medical quality, present patient records have gradually been transformed from paper-based patient records into electronic patient records with the following advantages [16].

(1). Accessibility: It can enhance the instantaneity of patient records and hasten the retrieving speed of patient records so as to promote the medical quality.
(2). Reduce costs: The operation cost and personnel expenses are reduced; and the manpower and space of medical records room are economized.
(3). Reporting: The recorded data in traditional paper-based patient records is disorganized, but the contents in electronic patient records are standarized and integrated. What is more, electronic patient records can satisfy the demands of medical personnel with the inquiry and analyses of patients' data as well as contribute to medical researches, communications, and statistics.
(4). Readability: With the illegibility of hand written traditional paper-based patient records, clerical errors are likely to happen on medical personnel, or the scripts are misunderstood because of different writing habits. On the contrary, the typeface in electronic patient records is unified, clear, and legible that the readability of information is advanced.
(5). Diagnostic support: With the complete medical information, medical personnel can make more appropriate diagnoses and treatments according to patients' conditions.

In such a society with fast changing environment and high population mobility, most patients take medical treatments in different medical organizations, where various medical records, including medical history, medication records, and clinical data, are remained. Furthermore, medical personnel can not quickly or instantly retrieve previous relevant patient records as electronic patient records in various medical organizations are with heterogeneous information systems or in long distance. With integrated electronic patient records systems, few more problems would still be derived. (1) Present information systems of electronic patient records are heterogeneous and diverse that it would be difficult and time consuming to integrate them into a single system. (2) All users have to re-adapt to and re-learn the new system. (3) The cost is too high. (4) All medical organizations will experience the transition period, which is not necessarily suitable for the structures and operation procedures of various medical organizations.

With the booming of the Internet and the universality of electronic patient records, this study proposes a solution to the above problems of having doctors access to electronic

patient records on the Internet. Nevertheless, a scheme is necessary for medical personnel being conveniently and legally authorized to access to patient records when retrieving patients' relevant medical records among various medical organizations, as well as to ensure the security of patients' privacy. This study therefore proposes the Mobile Agent scheme to solve the problems. A Mobile Agent is a program of disperse arithmetic process which can move from one host to another in heterogeneous network systems with the characteristics of autonomy and mobility, decreasing network traffic, reducing transfer lag, encapsulating protocol, fault-tolerance, high flexibility, and personalization [7, 8]. What is more, apart from transmitting information, a Mobile Agent is able to interact and allocate data with other mobile agents or disperse data systems. A Mobile Agent mainly receives and sends assigned missions to relevant service platforms on the Internet, searches or operates relevant data, and reports to the user after completing the missions. With the above characteristics, Mobile Agents can be applied to heterogeneous medical network systems, communicate and interact with other hosts from the host in one hospital information system migrating to another, as well as implement and complete the mission assigned from a legal user. Figure 1 shows the simple structure of Mobile Agents applied to the medical system.

For instance, a patient's electronic patient records could possibly be dispersed in medical organizations in various regions because of moving so that doctors can hardly acquire the complete patient records and patients cannot possess continuous medical care. In this case, Mobile Agents can be applied to search the dispersed medical records in various medical organizations through roaming on the Internet, which provides medical personnel more complete information of patient records, helps doctors rapidly understand the medical information of the patient according to patients' conditions, assists medical personnel in controlling the conditions of the patient, as well as enhances the timeliness and accuracy of therapy.

A Mobile Agent exchanges information with different hosts or other agents through roaming on the Internet that could result in the threats to the security. Four major threats are classified as follows [9].

(1). Integrity attacks: Malicious hosts intending to increase, delete, or revise the data, executable codes, and the status of Mobile Agents, or not to completely run the program of Mobile Agents could cause threats to the completion of data and execution in Mobile Agents. In this case, patient records could be revised when those problems occur in the transmission of electronic patient records, so that the completion of the patient records would be damaged and serious medical malpractice claims between the patient and the doctor would occur as a result.

(2). Availability refusal of servers: In the process of Mobile Agents moving among hosts, malicious hosts refusing Mobile Agents accessing to data, delaying service time, or rejecting transmitting Mobile Agents to the next server platform could cause failure of patient records feedback.

(3). Confidentiality attacks on Mobile Agents: Malicious hosts monitor or analyze the data, executable codes, or the status of Mobile Agents in the process of operation so as to steal the confidential data.

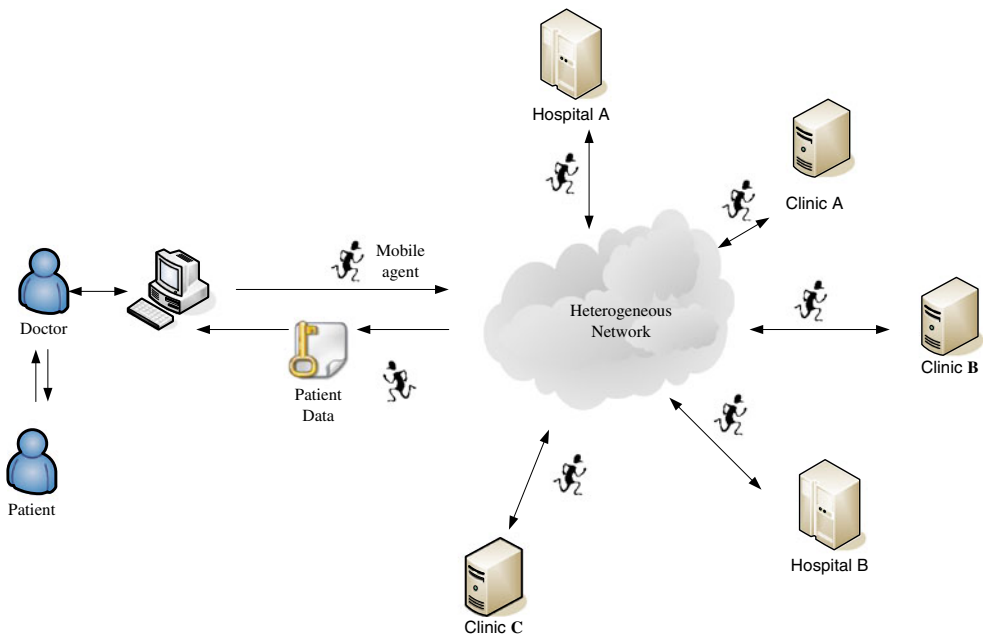


Fig. 1 Simple structure of Mobile Agents applied to the medical system

(4). Authentication risks of servers: Malicious hosts counterfeit the path of serve nodes and lead Mobile Agents to operate programs in other platform, or duplicate Mobile Agents to make them not be identified by other servers in implementing missions and not obtain the patient record information.

The above security threats result from Mobile Agents accessing to individual electronic patient records cross-medical organizations on the Internet. In this case, it is necessary to ensure that Mobile Agents not be intercepted or revised during moving as well as the confidential data in Mobile Agents can only be accessed by legally authorized persons so as to prevent the data from being falsified or counterfeited. In order to ensure the data in Mobile Agents being reasonably allocated and effectively protected, the establishment of access control schemes is inevitable. There have been several relevant studies in recent years. Corradi et al. proposed a Mobile Agent scheme, Secure and Open Mobile Agent (SOMA) [10], which contained agents, agent servers, management systems, and security policies. Karnik and Tripathi also proposed Ajanta system [11] for Mobile Agents with similar functions of SOMA. Volker and Mehrdad proposed a tree structure of Mobile Agents [12] with the functions of key management and access control. Nonetheless, with redundancy allocation of the key, the tree structure increased the size of Mobile Agents and enlarged the inducing calculation of the key. Based on hierarchical structure, key management scheme and access control scheme of Lagrange interpolation formula can improve the above drawbacks as well as make Mobile Agents be a more secure and effective electronic patient records access control scheme in the application cross medical organizations and access to patient electronic medical records. Furthermore, with the comparison of security and efficacy being the basis of feasibiltiy and better efficiency and the guarantee of secure environment during Mobile Agents implementing missions, the efficacy of key management can be promoted to protect the security of the system.

Related work

Transmission and access to electronic patient records on the internet

In present situations, the development of electronic patient records is necessary for the promotion of hospital competition. More importantly, statistical analyses of electronic data at any time could assist hospital managers to make the most appropriate decision support. With thousands of electronic patient records saved in the system, doctors can easily inquire the medication, medical history, various examination results, and allergic information of patients [15] through computers and the Internet so that the similar examinations and the waste of medical resources can be reduced, the instantaneity of medical data can be effectively enhanced, and the speed of retrieving patient records can also be hastened. According to present medical regulations, patient records must be kept for 10 years; but, they will be required of longer conservation with new medical practices. In this case, without electronic patient records, the medical records room in hospitals will not be able to load paper-based patient records. Consequently, not only do electronic patient records save human resource and space, but the data will not be lost or damaged after a long period of time so that they can be permanently conserved. Moreover, if any emergency happens to a person abroad, previous medication, medical history, and various records can be acquired on the Internet so that the time and medical resources are saved [1, 16]. The advantages include:

(1). Effectively advancing the instantaneity of medical patient records information, hastening the retrieval of patient records, and promoting medical quality.
(2). Reducing operation costs and personnel expenses, and saving space and manpower.
(3). Being helpful to medical research, statistics, and communications.
(4). Reducing errors by legible electronic patient records in comparison with traditional paper-based handwritings.
(5). Being able to be conserved permanently without being lost or damaged.
(6). Legally authorized persons being able to inquire patient records, on the Internet, for further examinations and analyses at any time and any place.

With electronic patient records, the privacy of patients [13, 14] has to be controlled, and related access schemes for the access authority of medical personnel have to be regulated in case of unauthorized persons randomly accessing to patients' information [17, 18] and causing the negligence of security and unnecessary medical malpractice claims. With national social welfare, many medical organizations apply smart cards to verify patients' identities through the operation of medical personnel that patient's data is still in risk as the verification is operated by another person. Nevertheless, if there is a doubled verification, the security will be solidified. For instance, in addition to the smart cards, the doctor re-confirms the identity of the patient or revises his/her data files with One-time Password (OTP) to prevent non-authorized persons accessing to the patient records at a different time. Face-based biometric authentication methods may also be considered for verification of patients' identities. For this reason, in the process of transmitting electronic patient records, several security-related issues are discussed as follows.

(1). Electronic patient records allow legally authorized persons accessing to certain data that is unreachable with paper-based patient records. However, single-layer passwords can be easily compromised in the process of encryption, so that multi-layer passwords can be utilized for encryption.
(2). It is essential to ensure that the electronic patient records not be stolen or revised in the process of transmission.
(3). If the data is stolen, the key can be prevented from being compromised so that the electronic medical records will not be revised and rejected so as to guard hackers and protect privacy.

Medical applications of mobile agents

Mobile Agents can automatically disperse arithmetic process when moving among computers so that, in medical applications, doctors can rapidly retrieve previous case history and effectively make medical integration and communication. This paper proposes to apply Mobile Agents to access to electronic patient records that can improve low mobility of paper-based patient records searching, delievering, and storing information through man-carrying. When two authorized medical personnel simultaneouly acquire the same patient record, individual mobile agents are sent to operate the mission that the same data is read seperately. However, the data is written in with hierarchic authorities in order to ensure the consistency of the patient information. The advantages of Mobile Agents include [19, 20]

(1). Reducing network load: In electronic patient records systems, there will be a large amount of data. With traditional disperse systems, communication as the media to exchange information is necessary; and, with security protocols, enormous network flow will further be generated. On the other hand, the Mobile Agent scheme does not require online connection with object computers, as it allows instructions being packaged and sent to the destination host as well as directly communicate and interact with the destination end so that the communication times between the source and the destination ends are reduced. What is more, Mobile Agents can remotely operate large amount of electronic patient record information from another host to decrease the communication times between the source and the destination ends. A Mobile Agent transmits data on the Internet merely when it is moving, and the transmitted data only contains the results of algorithm and the program in itself so that the consumed bandwidth is small and the network load is largely reduced.
(2). Reducing network lag: When accessing to large amount of electronic patient record information, network control is utilized for enormous instant reactions that would often cause network lag. With the technology of Mobile Agents, mobile agents are assigned to various computers from the central host and directly execute control instructions on each host. In the process of operation, the information is remotely exchanged by the central host so that the network lag is effectively reduced.
(3). Encapsulating protocol: Fixed protocols are applied to the exchange of information in traditional dispersed systems. Nevertheless, as the operation platforms are distinct in various hospitals, the hosts have to separately practice the protocol with individual program code. In this case, when the protocol requires reset for the sake of security or efficiency but one host can not synchronously renew, incompatibility or lag is therefore easily caused. With Mobile Agents, the protocol can be packaged so that Mobile Agents can, according to the protocol, establish a suitable protocol for communication, while moving to another host, without considering the problem of protocol.
(4). Allowing asynchronous and autonomic executions: Mobile Agents can asynchronously and automatically complete the missions, when the server is offline, as well as report the feedback after the completion that can reduce the connection time and enhance the convenience.
(5). Adapting to dynamic environment: According to the environment of the hospital, a Mobile Agent is able to adjust itself to adapt to the environment. Several mobile agents can maintain the best configurations anywhere in the network as well as solve specific problems simultaneously.
(6). Heterogeneity: Network environment, hardware, or software in each hospital are basically heterogeneous. Besides, the transmission among Mobile Agents and computers or the network is also independent, only related to the operation environmnet, so that Mobile Agents provide the best condition for system integration.
(7). Augmentability: The Mobile Agent scheme allows the function of flexible adjustment and augmentation for the source and destination ends of data.
(8). Solidity and fault-tolerance: With the ability of adapting to dynamic environment, Mobile Agents can remain the solidity and fault-tolerance in the unstably network so that loss and errors are preventable. This characteristic is important to the electronic patient record information.

Security of mobile agents

The Mobile Agent scheme proposed by Volker and Mehrdad was based on the tree structure [9], which was considered with the following drawbacks.

(1). With Mobile Agents, the interpreter or virtual machine in the computer is applied with common

program languages to describe the operation of Mobile Agents that would result in high cost.

(2). In the process of transmitting data with Mobile Agents, the operation of the key becomes an independent recording that cause the operation more complicated.

(3). Mobile Agents would save the key moving to various computers and choose a suitable key for the host of the destination end to execute, that would make the operation more efficient. Nonetheless, it would take a large space in the process of transmitting data and the size of the Mobile Agent would also be increased.

(4). More calculation for the public key – The decryption keys for confidential files are re-saved under the *static/sctx/acl/*folder, so that Mobile Agents would spend more time and cost on calculating and generating the key for the security of Mobile Agents.

For convenient transmission within the network, an ideal Mobile Agent acquires "the smaller, the better" to the space and the cost of the key calculation. For this reason, the refined Volder & Mehrdad security scheme, the key management and access control scheme of Mobile Agents based on hierarchy structure, is proposed in the following section in this paper. The recommended concepts are further demonstrated, as well as the operation procedure and applications are described in detail.

Lagrange interpolation

In numerical analyses, many practical problems are presented with functions for internal connections or regular patterns that can generally stand for certain correlations. However, the relationship correspondences of several functions are understood merely through experiments and observations. When observing a certain physical quantity in a practice and receiving the corresponding observed value, Lagrange interpolation can be applied to find a polynomial which is able to obtain the observed value at various observing points. This kind of polynomial is called Lagrange polynomial.

In mathematics, Lagrange interpolation can provide a polynomial function just through several known points on a two-dimensional plane. However, regarding the given points, such as n+1 points of (x_0, y_0), (x_1, y_1),…, (x_n, y_n), corresponding to the times, there is only one Lagrange polynomial (L) not exceeding n.

With higher-time polynomials, there will be infinite Lagrange polynomials (L), as all polynomials $\lambda(x\text{-}x_0)(x\text{-}x_1)\ldots(x\text{-}x_n)$ different from L are satisfied.

In defining Lagrange, k+1 data points, (x_0, y_0),…, (x_k, y_k), are given to certain polynomial function, where x_j responds to the location of independent variable and y_j to the data of the function being at the location. It represents that the known x_j and $f(x_j)$ can easily acquire y_j of the function corresponding to x_j. An n-polynomial passing these points will then be found, meaning function $y_j = f(x_j)$ can represent the polynomial $y = \sum_{j=0}^{K} a_j x^j = a_k x^k + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \ldots + a_1 x + a_0$· Besides, since y is the n-polynomial of x, the linear combination can be written as $l_j(x)$. With Lagrange interpolation, the acquired Lagrange polynomial is shown as

$$L(x) = \sum_{j=0}^{K} y_j l_j(x) \tag{1}$$

where each $l_j(x)$ is Lagrange basic polynomial or interpolation function, as

$$\begin{aligned} l_j(x) &= \prod_{i=0, i\neq j}^{k} \frac{x - x_i}{x_j - x_i} \\ &= \left(\frac{x - x_0}{x_j - x_0}\right)\ldots\left(\frac{x - x_{j-1}}{x_j - x_{j-1}}\right)\left(\frac{x - x_{j+1}}{x_j - x_{j+1}}\right)\ldots\left(\frac{x - x_k}{x_j - x_k}\right) \end{aligned} \tag{2}$$

The characteristic of Lagrange basic polynomial $l_j(x)$ is to take 1 at x_j and 0 at other points $x_i, i\neq j$, as $l_j(x) = \begin{cases} 0, & i \neq j \\ 1, & i = j \end{cases}$.

For example, to obtain $f(18)$ in $f(4) = 1\ f(5) = 5\ f(6) = 10$, first write down each Lagrange basic polynomials,

$$l_1(x) = \left(\frac{x-5}{4-5}\right)\left(\frac{x-6}{4-6}\right)$$

$$l_2(x) = \left(\frac{x-4}{5-4}\right)\left(\frac{x-6}{5-6}\right)$$

$$l_3(x) = \left(\frac{x-4}{6-4}\right)\left(\frac{x-5}{6-5}\right)$$

with Lagrange interpolation, the expression $L(x)$, the interpolation function of f, is acquired

$$\begin{aligned} L(x) &= f(4)l(1) + f(5)l(2) + f(6)l(3) \\ &= 1 \times \left(\tfrac{x-5}{4-5}\right)\left(\tfrac{x-6}{4-6}\right) + 5 \times \left(\tfrac{x-4}{5-4}\right)\left(\tfrac{x-6}{5-6}\right) \\ &\quad + 10 \times \left(\tfrac{x-4}{6-4}\right)\left(\tfrac{x-5}{6-5}\right) \\ &= \tfrac{1}{2}x^2 - \tfrac{1}{2}x - 5 \\ &=> L(x) = f(4)l(1) + f(5)l(2) + f(6)l(3) \end{aligned}$$

and then substitute 18 to get the value, $f(18) = L(18) = 148$.

The proposed scheme

This paper mainly applies formulas and Mobile Agents. When there are too many members, mobile agents are spread among various hosts for data exchange. It indirectly disperses the load among hosts as well as directly exchange with mobile agents to save the communication time with the hosts. In the formula of polynomial, only the host with access is real, or the others are zero, in the process of substitution. When the negative item is known by the formula in advance, the calculation will be faster to advance the efficacy of the system so that the system is successfully operated with the possibility of dispersing loads. The hierarchy concept applied in this paper aims to improve the problem of too many members resulting in larger load to the system as in the original tree structures.

Besides, the application of Lagrange interpolation polynomials allows Mobile Agents substituting the key for the server to obtain the decrytion key, which can reduce calculations and save time. Moreover, with the characteristics of Mobile Agents being not necessarily connected with the end device, the information exchange is merely operated in the end host that can effectively decrease network delay. In this case, it will not take long for medical personnel to wait for returning information.

With the understanding of the difficulty in integrating different systems in various medical organizations, the proposed Mobile Agent scheme is applied to overcome the difficulty of integrating heterogeneous systems as well as to be successfully operated cross systems. With the characteristics of Mobile Agents having the ability of crossing heterogeneous systems, which is able to develop its own protocol to communicate or exchange data between hosts or agents without any communication problem among heterogeneous systems.

Key generation

In medical sectors, not every hospital has definite relations of hierarchy. Some hospitals only deploy a principal and others belonging to different departments without hierarch relation. In this case, when the operation is executed only among departments, the hierarchy of Mobile Agent users would hardly be established. The Lagrange method, therefore, introduces Lagrange polynomials to the environment with hierarchy but without hierarchy authority, so that Mobile Agents can be applied to medical sectors without hierarchy authorities. Without hierarchic authorities, the method can still be utilized as the entire structure is established with formulas whose parameters do not possess authority relations so that the hierarchic structure will not be affected. Although it is mentioned that hierarchic authorities are not necessary, the method with hierarchic structure is still applied in this paper for easy demonstration. With the characteristics of formulas, which can be applied in both with and without authorities, hierarchy authorities are referred in this paper for more appropriate expression. The primary model is to remain authority relation among departments, but has no mutual access between the key and individuals. With the decryption key DK_t for encryption and the establishment of function $F_{DKt}(x)$, doctors in various departments can obtain the corresponding DK_t by decrypting $F_{DKt}(x)$ with the authorized access.

Step 1: The Mobile Agent randomly selects a big prime number $P = 2P'+1$, where P' is a big prime number. Then, choose g as the root of Galois Field $GF(P)$ and make g, P, and P' public.

Step 2: The Mobile Agent selects different decryption keys DK_t (t =1, 2, …, m; m is the number of decryption keys in the Mobile Agent) for each confidential document, where DK_t and P-1 are relatively prime.

Step 3: Mobile Agent select different secret keys SK_i (i =1, 2, …, n; n is the number of visited hosts), where SK_i and P-1 are relatively prime and SK_i is private.

Step 4: With the set of interpolation polynomials $\{(ID_j \| (g^{SKi} \bmod P), DK_t)\}$, the function $F_{DKt}(x)$ is established as followed, where $\|$ is the continuous operator, $DK_t \le SC_i$ stands for SC_i with decryption key of authorized access DK_t, and ID_j is the identity of decryption key. Finally, $F_{DKt}(x)$ is made public as

$$F_{DK_t}(x) = x \times DK_t \times \sum_{DK_t \le SC_i} x_{i,j}^{-1} l_{i,j}(x) \tag{3}$$

where $l_{i,j}(x)$ is the Lagrange polynomial or the interpolation function

$$l_{i,j}(x) = \prod_{t=1, t\neq i}^{n} \frac{x - x_{t,j}}{x_{i,j} - x_{t,j}} = \left(\frac{x - x_{1,j}}{x_{i,j} - x_{1,j}}\right) \ldots \left(\frac{x - x_{i-1,j}}{x_{i,j} - x_{i-1,j}}\right) \left(\frac{x - x_{i+1,j}}{x_{i,j} - x_{i+1,j}}\right) \ldots \left(\frac{x - x_{n,j}}{x_{i,j} - x_{n,j}}\right)$$

that i stands for the visited host number, j is the number of decryption keys, and $x_{i,j} = ID_j \| (g^{SKi} \bmod P)$.

Key derivation

Step 1: Set the right of the host SC_i to access a certain DK_t.

Step 2: The security classes SC_i can use its secret key SK_i and the public $F_{DKt}(x)$ to derive and obtain DK_t.

Example

Suppose that a confidential document is kept in a Mobile Agent with DK_5 encryption and transmitted to the assigned

department, a person with authorized access can substitute the decryption key to the function to obtain the corresponding decryption key. The detailed procedure of encryption and decryption is shown as follows.

In the process of encryption, CA firstly establishes the function $F_{DK5}(x)$ of DK_5 and makes it public, then calculates the interpolation function with the authority of security classes, and finally substitute $x_{i,j}=ID_j\|(g^{SKi} \bmod P)$ for the function.

$$l_{1,5}(x) = \left(\frac{x-x_{2,5}}{x_{1,5}-x_{2,5}}\right)\left(\frac{x-x_{3,5}}{x_{1,5}-x_{3,5}}\right)\left(\frac{x-x_{4,5}}{x_{1,5}-x_{4,5}}\right)\left(\frac{x-x_{5,5}}{x_{1,5}-x_{5,5}}\right)\left(\frac{x-x_{6,5}}{x_{1,5}-x_{6,5}}\right)$$
$$= \frac{x-ID_5||(g^{SK_2} \bmod P)}{ID_5||(g^{SK_1} \bmod P)-ID_5||(g^{SK_2} \bmod P)} \times \frac{x-ID_5||(g^{SK_3} \bmod P)}{ID_5||(g^{SK_1} \bmod P)-ID_5||(g^{SK_3} \bmod P)}$$
$$\times \frac{x-ID_5||(g^{SK_4} \bmod P)}{ID_5||(g^{SK_1} \bmod P)-ID_5||(g^{SK_4} \bmod P)} \times \frac{x-ID_5||(g^{SK_5} \bmod P)}{ID_5||(g^{SK_1} \bmod P)-ID_5||(g^{SK_5} \bmod P)}$$
$$\times \frac{x-ID_5||(g^{SK_6} \bmod P)}{ID_5||(g^{SK_1} \bmod P)-ID_5||(g^{SK_6} \bmod P)}$$

$$l_{3,5}(x) = \left(\frac{x-x_{1,5}}{x_{3,5}-x_{1,5}}\right)\left(\frac{x-x_{2,5}}{x_{3,5}-x_{2,5}}\right)\left(\frac{x-x_{4,5}}{x_{3,5}-x_{4,5}}\right)\left(\frac{x-x_{5,5}}{x_{3,5}-x_{5,5}}\right)\left(\frac{x-x_{6,5}}{x_{3,5}-x_{6,5}}\right)$$
$$= \frac{x-ID_5||(g^{SK_1} \bmod P)}{ID_5||(g^{SK_3} \bmod P)-ID_5||(g^{SK_1} \bmod P)} \times \frac{x-ID_5||(g^{SK_2} \bmod P)}{ID_5||(g^{SK_3} \bmod P)-ID_5||(g^{SK_2} \bmod P)}$$
$$\times \frac{x-ID_5||(g^{SK_4} \bmod P)}{ID_5||(g^{SK_3} \bmod P)-ID_5||(g^{SK_4} \bmod P)} \times \frac{x-ID_5||(g^{SK_5} \bmod P)}{ID_5||(g^{SK_3} \bmod P)-ID_5||(g^{SK_5} \bmod P)}$$
$$\times \frac{x-ID_5||(g^{SK_6} \bmod P)}{ID_5||(g^{SK_3} \bmod P)-ID_5||(g^{SK_6} \bmod P)}$$

$$l_{6,5}(x) = \left(\frac{x-x_{1,5}}{x_{6,5}-x_{1,5}}\right)\left(\frac{x-x_{2,5}}{x_{6,5}-x_{2,5}}\right)\left(\frac{x-x_{3,5}}{x_{6,5}-x_{3,5}}\right)\left(\frac{x-x_{4,5}}{x_{6,5}-x_{4,5}}\right)\left(\frac{x-x_{5,5}}{x_{6,5}-x_{5,5}}\right)$$
$$= \frac{x-ID_5||(g^{SK_1} \bmod P)}{ID_5||(g^{SK_6} \bmod P)-ID_5||(g^{SK_1} \bmod P)} \times \frac{x-ID_5||(g^{SK_2} \bmod P)}{ID_5||(g^{SK_6} \bmod P)-ID_5||(g^{SK_2} \bmod P)}$$
$$\times \frac{x-ID_5||(g^{SK_3} \bmod P)}{ID_5||(g^{SK_6} \bmod P)-ID_5||(g^{SK_3} \bmod P)} \times \frac{x-ID_5||(g^{SK_4} \bmod P)}{ID_5||(g^{SK_6} \bmod P)-ID_5||(g^{SK_4} \bmod P)}$$
$$\times \frac{x-ID_5||(g^{SK_5} \bmod P)}{ID_5||(g^{SK_6} \bmod P)-ID_5||(g^{SK_5} \bmod P)}$$

The function is therefore obtained as

$$F_{DK_5}(x) = x \times DK_5 \times \left\{(x_{1,5})^{-1} l_{1,5}(x) + (x_{3,5})^{-1} l_{3,5}(x) + (x_{6,5})^{-1} l_{6,5}(x)\right\}$$

When security class 3 tends to obtain the decryption key DK_5, substitute $x_{3,5} = ID_5||(g^{SK_3} \bmod P)$ for $l_{i,j}(x)$

$$l_{1,5}(x_{3,5}) = \left(\frac{x_{3,5}-x_{2,5}}{x_{1,5}-x_{2,5}}\right)\left(\frac{x_{3,5}-x_{3,5}}{x_{1,5}-x_{3,5}}\right)\left(\frac{x_{3,5}-x_{4,5}}{x_{1,5}-x_{4,5}}\right)\left(\frac{x_{3,5}-x_{5,5}}{x_{1,5}-x_{5,5}}\right)\left(\frac{x_{3,5}-x_{6,5}}{x_{1,5}-x_{6,5}}\right)$$
$$= \frac{x_{3,5}-ID_5||(g^{SK_2} \bmod P)}{ID_5||(g^{SK_1} \bmod P)-ID_5||(g^{SK_2} \bmod P)} \times \frac{ID_5||(g^{SK_3} \bmod P)-ID_5||(g^{SK_3} \bmod P)}{ID_5||(g^{SK_1} \bmod P)-ID_5||(g^{SK_3} \bmod P)}$$
$$\times \frac{x_{3,5}-ID_5||(g^{SK_4} \bmod P)}{ID_5||(g^{SK_1} \bmod P)-ID_5||(g^{SK_4} \bmod P)} \times \frac{x_{3,5}-ID_5||(g^{SK_5} \bmod P)}{ID_5||(g^{SK_1} \bmod P)-ID_5||(g^{SK_5} \bmod P)}$$
$$\times \frac{x_{3,5}-ID_5||(g^{SK_6} \bmod P)}{ID_5||(g^{SK_1} \bmod P)-ID_5||(g^{SK_6} \bmod P)} = 0$$

$$l_{3,5}(x_{3,5}) = \left(\frac{x_{3,5}-x_{1,5}}{x_{3,5}-x_{1,5}}\right)\left(\frac{x_{3,5}-x_{2,5}}{x_{3,5}-x_{2,5}}\right)\left(\frac{x_{3,5}-x_{4,5}}{x_{3,5}-x_{4,5}}\right)\left(\frac{x_{3,5}-x_{5,5}}{x_{3,5}-x_{5,5}}\right)\left(\frac{x_{3,5}-x_{6,5}}{x_{3,5}-x_{6,5}}\right)$$
$$= \frac{ID_5||(g^{SK_3} \bmod P)-ID_5||(g^{SK_1} \bmod P)}{ID_5||(g^{SK_3} \bmod P)-ID_5||(g^{SK_1} \bmod P)} \times \frac{ID_5||(g^{SK_3} \bmod P)-ID_5||(g^{SK_2} \bmod P)}{ID_5||(g^{SK_3} \bmod P)-ID_5||(g^{SK_2} \bmod P)}$$
$$\times \frac{ID_5||(g^{SK_3} \bmod P)-ID_5||(g^{SK_4} \bmod P)}{ID_5||(g^{SK_3} \bmod P)-ID_5||(g^{SK_4} \bmod P)} \times \frac{ID_5||(g^{SK_3} \bmod P)-ID_5||(g^{SK_5} \bmod P)}{ID_5||(g^{SK_3} \bmod P)-ID_5||(g^{SK_5} \bmod P)}$$
$$\times \frac{ID_5||(g^{SK_3} \bmod P)-ID_5||(g^{SK_6} \bmod P)}{ID_5||(g^{SK_3} \bmod P)-ID_5||(g^{SK_6} \bmod P)} = 1$$

$$l_{6,5}(x_{3,5}) = \left(\frac{x_{3,5}-x_{1,5}}{x_{6,5}-x_{1,5}}\right)\left(\frac{x_{3,5}-x_{2,5}}{x_{6,5}-x_{2,5}}\right)\left(\frac{x_{3,5}-x_{3,5}}{x_{6,5}-x_{3,5}}\right)\left(\frac{x_{3,5}-x_{4,5}}{x_{6,5}-x_{4,5}}\right)\left(\frac{x_{3,5}-x_{5,5}}{x_{6,5}-x_{5,5}}\right)$$
$$= \frac{x_{3,5}-ID_5||(g^{SK_1} \bmod P)}{ID_5||(g^{SK_6} \bmod P)-ID_5||(g^{SK_1} \bmod P)} \times \frac{x_{3,5}-ID_5||(g^{SK_2} \bmod P)}{ID_5||(g^{SK_6} \bmod P)-ID_5||(g^{SK_2} \bmod P)}$$
$$\times \frac{ID_5||(g^{SK_3} \bmod P)-ID_5||(g^{SK_3} \bmod P)}{ID_5||(g^{SK_6} \bmod P)-ID_5||(g^{SK_3} \bmod P)} \times \frac{x_{3,5}-ID_5||(g^{SK_4} \bmod P)}{ID_5||(g^{SK_6} \bmod P)-ID_5||(g^{SK_4} \bmod P)}$$
$$\times \frac{x_{3,5}-ID_5||(g^{SK_5} \bmod P)}{ID_5||(g^{SK_6} \bmod P)-ID_5||(g^{SK_5} \bmod P)} = 0$$

Finally, substitute $F_{DK_5}(x)$ for the decryption key DK_5

$$F_{DK_5}(x_{3,5}) = x_{3,5} \times DK_5 \times \left\{(x_{1,5})^{-1} l_{1,5}(x) + (x_{3,5})^{-1} l_{3,5}(x) + (x_{6,5})^{-1} l_{6,5}(x)\right\}$$
$$= ID_5||(g^{SK_3} \bmod P) \times DK_5 \times \begin{Bmatrix} (ID_5||(g^{SK_1} \bmod P))^{-1} \times 0 \\ +(ID_5||(g^{SK_3} \bmod P))^{-1} \times 1 \\ +(ID_5||(g^{SK_6} \bmod P))^{-1} \times 0 \end{Bmatrix}$$
$$= ID_5||(g^{SK_3} \bmod P) \times DK_5 \times (ID_5||(g^{SK_3} \bmod P))^{-1} = DK_5$$

Security analyses

This section aims to precede security analyses of the Lagrange method with common external attacks, reversed attacks, and cooperative attacks, as well as to discuss possible attacks from the viewpoint of attackers and to seek for compromising the method proposed in this paper in order to prove the proposed method with certain security.

External attacks

Within common attacks, most attackers are not personnel in medical organizations, i.e. not internal attackers. These attackers are often interested in valuable medical information, such as patient conditions of famous people or the president's health, and tend to steal or sell the information that could result in the divulgence of confidential information and damages. This kind of attacks therefore becomes an essential analysis in the process of security analyses.

Regarding external attacks, attackers can only obtain protected meaningless documents or public parameters in Mobile Agents when the internal medical information is illegally acquired. For valuable patient records or medical information, attackers have to derive decryption key from the obtained public parameters, decrypt the encrypted information, and obtain valuable and meaningful information or patient records. Regarding security analyses, the analyses of both external and internal attacks are based on the parameters in the formula with solutions to discrete lognormal. Moreover, the formula is applied to effectively prevent from attacks and, in operation, is convenient for the members in the structure to calculate, while both external and internal non-members will face the problem and difficulty of solving discrete lognormal. In addition to data encryption, user authentication and access control may also be applied simultaneously to strengthen the overall security level.

When the public parameters are obtained by external attackers, the function in the method plays an important role, as the function $F_{DK_t}(x) = x \times DK_t \times \sum_{DK_t \le SC_i} x_{i,j}^{-1} l_{i,j}(x)$ contains the decryption key. For this reason, the function must have sufficient security. Referring to Fig. 2, if an attacker tries to obtain the decryption key DK_5, the decryption key has to be compromised from interpolation function. In this case, the first interpolation function $l_{1,5}(x)$ is substituted and analyzed.

$$
\begin{aligned}
l_{1,5}(x) &= \left(\frac{x - x_{2,5}}{x_{1,5} - x_{2,5}}\right)\left(\frac{x - x_{3,5}}{x_{1,5} - x_{3,5}}\right)\left(\frac{x - x_{4,5}}{x_{1,5} - x_{4,5}}\right)\left(\frac{x - x_{5,5}}{x_{1,5} - x_{5,5}}\right)\left(\frac{x - x_{6,5}}{x_{1,5} - x_{6,5}}\right) \\
&= \frac{x - ID_5||(g^{SK_2} \bmod P)}{ID_5||(g^{SK_1} \bmod P) - ID_5||(g^{SK_2} \bmod P)} \times \frac{x - ID_5||(g^{SK_3} \bmod P)}{ID_5||(g^{SK_1} \bmod P) - ID_5||(g^{SK_3} \bmod P)} \\
&\quad \times \frac{x - ID_5||(g^{SK_4} \bmod P)}{ID_5||(g^{SK_1} \bmod P) - ID_5||(g^{SK_4} \bmod P)} \times \frac{x - ID_5||(g^{SK_5} \bmod P)}{ID_5||(g^{SK_1} \bmod P) - ID_5||(g^{SK_5} \bmod P)} \\
&\quad \times \frac{x - ID_5||(g^{SK_6} \bmod P)}{ID_5||(g^{SK_1} \bmod P) - ID_5||(g^{SK_6} \bmod P)}
\end{aligned}
$$

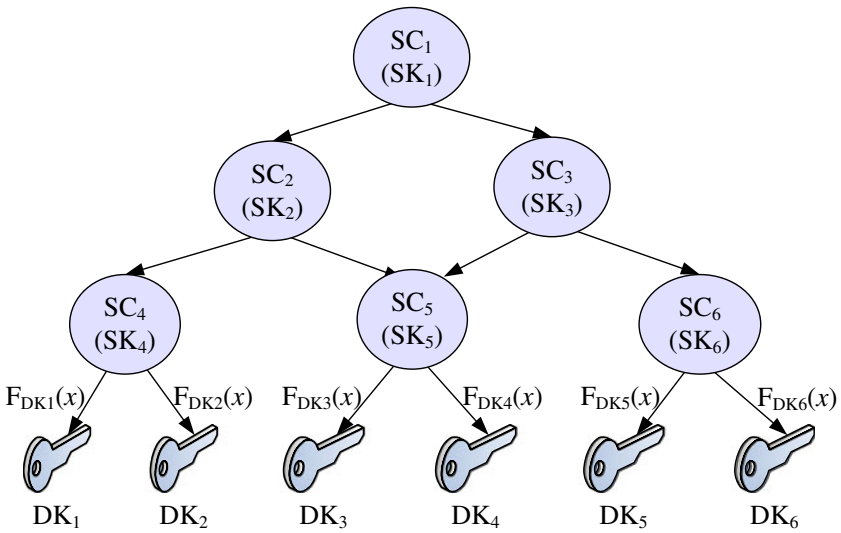


Fig. 2 Hierarchy structure in the access control

In the function, with known numbers P and g but others being unknown, the key will not be effectively derived as there have been too many unknown numbers. What is more, the attackers will face the problem of solving discrete lognormal, that could ensure the medical information or patient records not being acquired by external attacks.

Reversed attacks

Simply speaking, reversed attacks present that doctors or patients with lower authority intend to obtain decryption keys of the chairman or the principal with higher authority. Referring to Fig. 3, SC_j stands for doctors or patients with lower authority while SC_i represents the chairman or the principal with higher authority. When doctors or patients obtain the decryption key with higher authority, they are likely to precede actions out of their authority, such as retrieving or revising patient records or medical information with the principal's decryption key. In this case, the system will record the illegal actions of the principal which could result in some loss. Preventing form reversed attacks therefore becomes an essential security analysis.

Regarding the method proposed in this paper, the interpolation function $l_{i,j}(x)$ is opened as

$$l_{i,j}(x) = \prod_{t=1,t\neq i}^{n} \frac{x - x_{t,j}}{x_{i,j} - x_{t,j}} = \left(\frac{x - x_{1,j}}{x_{i,j} - x_{1,j}}\right)\ldots\left(\frac{x - x_{i-1,j}}{x_{i,j} - x_{i-1,j}}\right)\left(\frac{x - x_{i+1,j}}{x_{i,j} - x_{i+1,j}}\right)\ldots\left(\frac{x - x_{n,j}}{x_{i,j} - x_{n,j}}\right)$$

where there is no relation among x's in $x_{i,j}$=ID_j||(g^{SKi} mod P). The benefit of this method is that there is no relation among the keys that all security classes are independent without mutual correlation. In this case, doctors or patients do not have available parameters or relations to derive the decryption key of the principal.

Cooperative attacks

Cooperative attacks mean that many doctors or patients intend to cooperatively obtain the principal's decryption key. Referring to Fig. 4, SC_j and SC_k stand for doctors or patients with lower authority and SC_i for the chairman or the principal with higher authority. Cooperative attacks therefore is considered as several reversed attacks assembled together. Comparing reversed attacks with cooperative attacks, there are more internal personnel attending at cooperative attacks, so that the compromise opportunity is increased as more keys are referred to. In this case, the threat of cooperative attacks is much higher than that of reversed attacks.

To solve the problem, randomized derivations of keys eliminate the regularity and the corresponding relations, so that doctors cannot directly derive the decryption key from several keys. Besides, with the features of Lagrange polynomials, there is no correlation between hierarchies, which avoids the system from being compromised and the principal's decryption key being obtained. Security classes are separated as independent units in this paper so that the decryption key of the higher authority cannot be effectively acquired no matter with reversed attacks from a single person or cooperative attacks from many people.

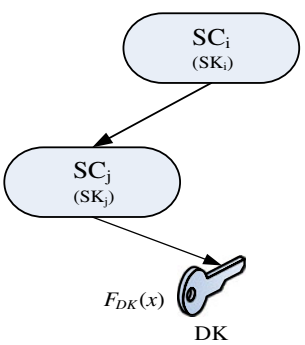
From the analysis of function $F_{DK_t}(x) = x \times DK_t \times \sum_{DK_t \le S_i} x_{i,j}^{-1} l_{i,j}(x)$, $l_{i,j}(x)$ is the key of compromise. In the process of opening, the above example of $l_{1,5}(x)$ is taken for demonstration.

$$l_{1,5}(x) = \left(\frac{x - x_{2,5}}{x_{1,5} - x_{2,5}}\right)\left(\frac{x - x_{3,5}}{x_{1,5} - x_{3,5}}\right)\left(\frac{x - x_{4,5}}{x_{1,5} - x_{4,5}}\right)\times \left(\frac{x - x_{5,5}}{x_{1,5} - x_{5,5}}\right)\left(\frac{x - x_{6,5}}{x_{1,5} - x_{6,5}}\right)$$

$$= \frac{x - ID_5||(g^{SK_2} \bmod P)}{ID_5||(g^{SK_1} \bmod P) - ID_5||(g^{SK_2} \bmod P)} \times \frac{x - ID_5||(g^{SK_3} \bmod P)}{ID_5||(g^{SK_1} \bmod P) - ID_5||(g^{SK_3} \bmod P)} \times \frac{x - ID_5||(g^{SK_4} \bmod P)}{ID_5||(g^{SK_1} \bmod P) - ID_5||(g^{SK_4} \bmod P)} \times \frac{x - ID_5||(g^{SK_5} \bmod P)}{ID_5||(g^{SK_1} \bmod P) - ID_5||(g^{SK_5} \bmod P)} \times \frac{x - ID_5||(g^{SK_6} \bmod P)}{ID_5||(g^{SK_1} \bmod P) - ID_5||(g^{SK_6} \bmod P)}$$

According to $l_{1,5}(x)$, SK_2~SK_6 are unknown numbers. If SK_2 stands for the decryption key of the principal and others for the keys of participating doctors, SK_2 becomes the only unknown number. According to g^{SK_2} mod P, the

Fig. 3 Reversed attacks



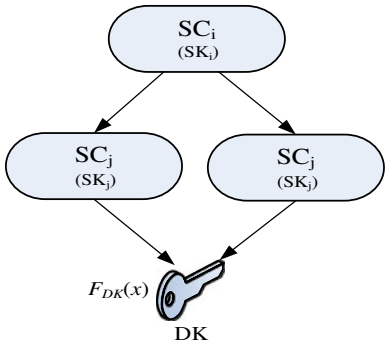


Fig. 4 Cooperative attacks

security is based on solving the problem of discrete lognormal, whose security has been proved to depend on the number and strength of primes [21]. In other words, if the prime is big enough, the security is confirmed, proving that the attack can be effectively prevented.

Equation attacks

In equation attacks, attackers tend to directly derive the decryption key from a known equation so that the security of the equation is the point in this section.

If authorized users SC_1 and SC_3 can derive the key DK_5 through function $F_{DK_5}(x)$, SC_3 can derive the secret parameters of SC_1 with the secret parameter SK_3, public parameters, and the function $F_{DK_5}(x)$, further obtain other information which can only be accessed with SC_1, and calculate the result through the following deriving steps.

$$F_{DK_5}(x_{3,5}) = x_{3,5} \times DK_5 \times \sum_{DK_j \le SC_i} x_{i,j}^{-1} l_{i,j}(x_{3,5})$$

$$\Rightarrow F_{DK_5}(x_{6,53}) \times DK_5^{-1} = x_{3,5} \times \sum_{DK_j \le SC_j} x_{i,j}^{-1} l_{i,j}(x_{3,5})$$

$$\Rightarrow F_{DK_5}(x_{3,5}) \times DK_5^{-1} = x_{3,5} \times \left\{ (x_{1,5})^{-1} l_{1,5}(x_{3,5}) \times (x_{3,5})^{-1} l_{3,5}(x_{3,5}) \times (x_{6,5})^{-1} l_{6,5}(x_{3,5}) \right\}$$

On the left of the equation, SC_3 can legally derive the key DK_5 with function $F_{DK_5}(x)$. Therefore, substitute DK_5 for the left of the equality as

$$\Rightarrow DK_5 \times DK_5^{-1} = x_{3,5} \times \left\{ \ldots (x_{3,5})^{-1} \times \left(\frac{x_{3,5} - x_{1,5}}{x_{3,5} - x_{1,5}} \right) \left(\frac{x_{3,5} - x_{2,5}}{x_{3,5} - x_{2,5}} \right) \left(\frac{x_{3,5} - x_{4,5}}{x_{3,5} - x_{4,5}} \right) \left(\frac{x_{6,5} - x_{5,5}}{x_{6,5} - x_{5,5}} \right) \left(\frac{x_{6,5} - x_{6,5}}{x_{6,5} - x_{6,5}} \right) \times \ldots \right\}$$

$$\Rightarrow 1 = x_{3,5} \times \{0 + (x_{3,5})^{-1} \times \frac{ID_5 || (g^{SK_3} \bmod P) - ID_5 || (g^{SK_1} \bmod P)}{ID_5 || (g^{SK_3} \bmod P) - ID_5 || (g^{SK_1} \bmod P)} \times \ldots + 0\} \Rightarrow 1 = x_{3,5} \times x_{3,5}^{-1} \times 1$$

On the right hand side of the equation, in addition to the number of function $l_{1,5}(x_{3,5})$ being 1 in the Lagrange polynomial, others are zero. In this case, even though the authorized user can derive to this step with known parameters, the polynomial can not be reversed from 1. Besides, there is discrete lognormal problem in the decryption key that can effectively prevent equation attacks.

Conclusion

Paper-based patient records have long been used with disadvantages of wasting large space, being easily damaged or lost, not being easily kept, not being able to retrieved by several doctors for united therapy, a large amount of management cost, not easily retrieving patient records, easily delaying treatments, transmitting difficulty of patient record information, difficulty in compilation of patient records, and too many patient records. With the progress of the time, paper-based patient records and traditional medical operations have been transformed into digital forms to advance the medical efficiency and information instantaneity. There have been many relevant medical organizations promoting the operation of electronic patient records at present. An acceptable electronic patient record must focus on the protection of information security, particularly on the protection of patient privacy. In the process of implementing electronic patient records, planning the

management of information security to conform to the requirements of present medical management has become primary on the promotion of electronic patient records to the public and medical organizations. A complete information security scheme will be the prior consideration of electronic patient record system. Presently, frequent network attacks make the electronic patient records among hospitals encounter many security threats in transmitting confidential documents, as electronic patient records frequently flow and exchange on the Internet. For this reason, this paper aims to improve the above drawbacks, to transform paper-based patient records into electronic patient records, and to apply the benefits of electronic patient records with the technology of Mobile Agents to construct a hierarchy access control system. With the key management capability in Lagrange interpolation and access control scheme, the classification and control of secure hierarchy are preceded. Moreover, with the benefits of easy calculation but difficult compromise of Lagrange interpolation, Mobile Agents can be applied to access to individual electronic patient records cross hospitals, to promote medical standards, and to provide safer and more efficient medical services. What is more, security analyses to the hierarchy system are preceded and several typical attacks are simulated in order to demonstrate the security of the constructed electronic patient record system, so that doctors and patients can instantly obtain the patient records to help the efficiency and accuracy of clinic and reduce unnecessary delay-time. For patients, they will not need to worry about patient records being divulged, as the secret of patient records is guaranteed.

References

1. Safran, C., and Goldberg, H., Electronic patient records and the impact of the Internet. *Int. J. Med. Inform.* 60(2):77–83, 2000.
2. Calcote, S., Developing a secure healthcare information network on the Internet. *Healthc. Financ. Manage.* 51(1):68, 1997.
3. Uslu, A. M., and Stausberg, J., Value of the electronic patient record: An analysis of the literature. *J. Biomed. Inform.* 41 (4):675–682, 2008.
4. Dujat, C., Haux, R., Schmucker, P., and Winter, A., Digital optical archiving of medical records in hospital information systems-a practical approach towards the computer-based patient record. *Meth. Inf. Med.* 34(5):487–497, 1995.
5. Rind, D. M., and Safran, C., Real and imagined barriers to an electronic medical record. *Proceedings of the Annual Symposium on Computer Application in Medical Care*, pp. 74-78, 1993.
6. van Ginneken, A. M., The computerized patient record: Balancing effort and benefit. *Int. J. Med. Inform.* 65(2):97–119, 2002.
7. Picco, G. P., Mobile agents: an introduction. *J. Microprocess. Microsyst.* 25(2):65–74, 2001.
8. Chen, T. S., Chung, Y. F., and Tian, C. S., A novel key management scheme for dynamic access control in a user hierarchy. *Proc. IEEE Annu. Int. Comput. Softw. Appl. Conf.* 1:396–401, 2004.
9. Bierman, E., Pretoria T., Cloete, E., 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*, pp. 141-148, 2002.
10. Corradi, A., Montanari, R., Stefanelli, C., Security issues in mobile agent technology. *Proceedings of the 7th IEEE Workshop on Future Trends of Distributed Computing System*, Cape Town, South Africa, pp. 3-8, 1999.
11. Karnik, N. M., Tripathi,, A. R. A security architecture for mobile agents in Ajanta. *Proceedings of the International Conference on Distributed Computing Systems*, Taipei, Taiwan, pp. 402-409, 2000.
12. Volker, R., and Mehrdad, J. S., Access control and key management for mobile agents. *Comput. Graph.* 22(4):457–461, 1998.
13. The State of HIPAA Privacy and Security Compliance. *AHIMA*, April 2006.
14. Rash, M. C. Privacy concerns hinder electronic medical records. *The Business Journal of the Greater Triad Area*, 2005.
15. Halamka, J. D., Szolovits, P., Rind, D., and Safran, C., A WWW implementation of national recommendations for protecting electronic health information. *J. Am. Med. Inform. Assoc.* 4 (6):258–464, 1997.
16. Lovis, C., Baud, R. H., and Scherrer, J. R., Internet integrated in the daily medical practice within an electronic patient record. *Comput. Biol. Med.* 28(5):567–579, 1998.
17. Safran, C., Rind, D., Citroen, M., Bakker, A. R., Slack, W. V., and Bleich, H. L., Protection of confidentiality in the computer-based patient record. *MD Computing* 12(3):187–192, 1995.
18. Barrows, R. C., Jr., and Clayton, P. D., Privacy, confidentiality, and electronic medical records. *J. Am. Med. Inform. Assoc.* 3 (2):139–148, 1996.
19. Borselius, N., Mobile agent security, electronics and communication. *Eng. J.* 14(5):211–218, 2002.
20. Maes, P., Guttman, R. H., and Moukas, A. G., Agents that buy and sell. *Commun. ACM* 42(3):81–91, 1999.
21. Nechaev, V. I., Complexity of a determinate algorithm for the discrete logarithm. *Math. Notes* 55:165–172, 1994.