SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2016; **9**:652–666
Published online 3 December 2015 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.1387

RESEARCH ARTICLE

Security approach to controlling access to personal health records in healthcare service

Tzer-Long Chen[1]*, Yu-Ting Liao[2], Yi-Fan Chang[3] and Jen-Hung Hwang[2]

[1] Department of Information Networking and System Administration, Ling Tung University, Taichung, Taiwan
[2] Department of Management Science, National Chiao Tung University, Hsinchu, Taiwan
[3] Department of Information Management, Tunghai University, Taichung, Taiwan

ABSTRACT

The changing information technology and the constant progress of medical technologies have gradually changed traditional paper-based medical records into low-cost electronic health records. The broad application of electronic health records allows a medical information exchange model being developed, called personal health records (PHR), which are the personal health medical information managed and maintained by the user. In consideration of PHR being a patient's health medical information, the privacy setting and the access authority have to be strictly controlled. In addition to providing users with reasonable access authorities, the PHR system has to avoid the illegal access of unauthorized single users or groups. The idea of public-key cryptosystems and Lagrange interpolating polynomial is applied to construct a high-security and efficient encryption scheme so that PHR users could execute the access system in a secure environment. Copyright © 2015 John Wiley & Sons, Ltd.

KEYWORDS

personal health records (PHR); public-key cryptosystems; Lagrange interpolating polynomial

***Correspondence**

Tzer-Long Chen, Department of Creative Product Design, Ling Tung University, Taichung, Taiwan.
E-mail: tlchen@teamail.ltu.edu.tw

1. INTRODUCTION

1.1. Preface

Paper-based patient records that were used in medical institutions occupied much space, wasted costs, and could not efficiently offer patients with perfect healthcare. Accordingly, traditional paper-based patient records are gradually developed into electronic medical records so that patients' medical data, including medical examinations and medical records, could be directly delivered by medical institutions through the electronic medical record exchange center of Ministry of Health and Welfare under the agreement of patients. It could avoid unnecessary examinations and reduce the waste of social resources [1] to largely reduce medical costs and enhance the patient healthcare efficiency.

Based on the advance of information technology and the popularity of the Internet, many medical services are completed with information technology for the continuous patient treatment and observation, rather than patient conditions being hard to be traced in the past [2]. Besides, in order to have patients manage their health conditions for actively guarding their health, Ming Li *et al*. proposed patient-centered personal health records (PHR) [3] in 2010 for patients self-managing their health records, which covered all past medical records, medical history, medication, or allergic history of patients, to assist the public in understanding health.

Although the management of personal health conditions could be convenient and rapid, the problem of privacy is worth noticing. The contents in PHR are related to patients; however, different from past medical records being managed by hospitals, patients' personal health information is self-managed. In other words, a patient's health information is controlled by the patient. The data security, integrity, and usability in the transformation process are important. In this case, this study would propose an effective and practicable solution for information security in order to prevent private information from being tampered, stolen, or lost and to reduce patient rights and medical loss.

1.2. Research motivation and objective

The emerging cloud computing, with the advantages of self-service, source pool share, and high flexibility of

redistribution [4], allows several electronic systems transferring the platforms to the cloud; medical systems appear no exception. Medical systems that are transferred to the cloud reveal the following advantages.

(1) The data share and convenient exchange allow rapidly retrieving patients' medical situations to reduce treatment delay.
(2) Data flow is more flexible.
(3) The rapid and effective access to medical files could largely reduce medical costs.
(4) It crosses the space limitation of hardware equipment.

Establishing medical systems on the cloud therefore presents great assistance on the users.

In addition to the convenience of sharing sources, cloud computing also allows simultaneous access of several users. In this case, when several users are allowed to access to the system, the efficiency and security to access confidential data and different authority settings become primary (e.g. authority settings for users with different access authority levels). As the confidential data in the system are patients' health records, patient privacy needs to be guaranteed when the users (either physicians or nurses) access medical information, so as to avoid illegal access.

Accordingly, this study intends to propose a practicable and secure approach to protect the system from illegal entry.

This study aims to establish a secure and efficient information security mechanism. Each authorized member of the system could assess distinct confidential files. The authority division has to be definite, and patients could determine the users (e.g. physicians or nurses) to access the personal health records. Such a model is expected to guarantee the privacy and security of personal medical information.

For system transaction, such as patient referral, changes of attending physician, nurses on duty, or family doctor engagement, the system adding or removing members or revising the access authority, and even updating confidential document would not appear as a loophole on the information security.

2. LITERATURE REVIEW

2.1. Electronic medical record, personal health record, and electronic health record

Safran and Goldberg defined electronic medical records in 2000 that could be accessed through computers or the Internet: they were patients' clinical diagnosis records and personal health treatment records, and each patient was an independent medical record system [5].

With electronic medical records, medical personnel could rapidly and efficiently master the complete medical history and medication records of patients; therefore, repeated medication or examinations could be avoided to avoid waste and offer patients with proper treatment.

Table I shows the comparison between traditional paper-based patient records and electronic medical records [5–11].

Electronic health records are electronic personal records, containing electrocardiogram, medical records, or medical images, that could be accessed through the Internet. In addition to electronic medical records, they could be used as the reference for medical data and demographic data. Nowadays, many definitions about electronic patient healthcare records are proposed, and there are some overlaps among them [12]. In general situations, the two could be regarded as the same; however, there are still differences in some professional fields (e.g. medical informatics).

In regard to current situations of introducing electronic health records to Taiwan, the investigation of Ministry of Health and Welfare, Executive Yuan, China, on electronic medical records of national medical institutions, including 538 hospitals and 4033 random check clinics, in 2005 showed the popularity of electronic health records in medical institutions [13]. However, the cases of exchanging electronic medical records among medical institutions are still rare. The exchange is currently experimented, but not comprehensively practiced, that the promotion of electronic health records still requires efforts to the public health policies [14].

Table I. Comparison between traditional paper-based patient records and electronic medical records.

Advantages and drawbacks of traditional paper-based patient records	Advantages and drawbacks of electronic medical records
It cannot be real-time or synchronically retrieved	The data could be directly inquired through the system to save search time
The handwriting data are hard to recognize	The reading is not affected by handwriting or broken paper
Medical records in various areas could merely be retrieved by authorized physicians	The medical records could be simultaneously retrieved by several physicians
The formats are different	The format could be uniformed to solve the reading difficulty
The space for storing paper-based patient records is inadequate after a long period	The space for storing medical records and the personnel expenses could be reduced
It is hard to preserve	It is not easily lost or damaged, and the complete medical records could be traced
Patients' medical data cannot be integrated so that the medical costs are enhanced and the medical quality is reduced	It allows medical personnel inquiring patient data and statistical analyses of relevant medical data to help medical research and development, reduce medical costs, and enhance medical quality

Kahn *et al.* defined PHR in 2009 that it could be used for sharing health information, increasing the understanding of health, and assisting patients in healthcare [15]. In the entire medical history, the practice and development of PHR are rather late. Comparing to electronic medical records and Electronic Health Record (EHR), PHR contains personal food habits, exercise habits, or behavioral activities and emotion of patients. In terms of management, it used to be uniformly managed in medical institutions but is gradually transferred to patients managing their own health records [16].

Personal health records are becoming more important in Taiwan, which is approaching aging society. PHR not only could record food and exercise habits, heartbeats, and blood pressure but also allows physicians or nurses master patient conditions in time. As the elderly suffering from Alzheimer's disease, dementia, or epilepsy seizure might not smoothly use information products to keep the recording conditions of PHR [17], it becomes a critical issue to implement PHR for the elderly.

2.2. Lagrange interpolating polynomial

Lagrange interpolation, a polynomial interpolation named by Joseph Lagrange who was a mathematician in the 18th century, could be used for rapidly calculating several specific dissimilarities on a plane.

Assuming $n+1$ dissimilarities on a plane $A_k(x_k, y_k)$, $k=0, 1, 2, 3, \ldots, n$, where any two x_k are different, the Lagrange interpolating polynomial appears as

$$L(x) := \sum_{j=0}^{n} y_j \ell_j(x)$$

where $\ell_j(x)$ is the Lagrange basic polynomial (or interpolation function), expressed as [18]

$$\ell_j(x) = \prod_{i=0, i\neq j}^{n} \frac{x - x_i}{x_j - x_i} = \left(\frac{x - x_0}{x_j - x_0}\right) \cdots \left(\frac{x - x_{j-1}}{x_j - x_{j-1}}\right)\left(\frac{x - x_{j+1}}{x_j - x_{j+1}}\right) \cdots \left(\frac{x - x_k}{x_j - x_k}\right)$$

$\ell_j(x)$ shows the characteristics that the value on x_j is 1, but 0 on other points $x_i (i \neq j)$. The expression is shown as in the succeeding text.

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

For example,
Assuming three dissimilarities $A_1(0\ ,\ 5)$, $A_2(2\ ,\ 7)$, $A_3(3\ ,\ 14)$ on a plane, the following are calculated.

$$\ell_1(x) = \left(\frac{x-2}{0-2}\right)\left(\frac{x-3}{0-3}\right) = \frac{x^2 - 5x + 6}{6}$$

$$\ell_2(x) = \left(\frac{x-0}{2-0}\right)\left(\frac{x-3}{2-3}\right) = \frac{-x^2 + 3x}{2}$$

$$\ell_3(x) = \left(\frac{x-0}{3-0}\right)\left(\frac{x-2}{3-2}\right) = \frac{x^2 - 2x}{3}$$

The Lagrange interpolating polynomial of the three points could be deducted as

$$\begin{aligned} y = f(x) &= 5\times\ell_1(x) + 7\times\ell_2(x) + 14\times\ell_3(x) \\ &= \frac{5x^2 - 25x + 30}{6} + \frac{-7x^2 + 21x}{2} + \frac{14x^2 - 28x}{3} \\ &= \frac{12x^2 - 18x + 30}{6} \\ &= 2x^2 - 3x + 5 \end{aligned}$$

2.3. T.S. Chen (2012) methodology

Personal health records are a system allowing several users accessing various confidential files; different users could append, delete, revise, and inquire the system; each PHR user does not necessarily have the same access authority to the same confidential files in the system; and the quantity of users and confidential files is huge. In other words, each user has different authority to access confidential files, and it is complicated.

Before constructing encryption algorithms, the quantity of confidential files should be confirmed and numbered, and the users have to clearly set the access authority to confidential files. In T.S. Chen's (2012) methodology, partial order is utilized for setting the access authority, which is uniformly established by central authority (CA). Partial order is defined in the succeeding text. Given a set S, the binary relation $\lceil \preccurlyeq \rfloor$ on S presents reflexive, antisymmetric, and transitive characteristics [19] so that it is suitable for setting a user's access authority. In this method, CA records the access authority of a user S_i in a set J_i, which explains the access authority of the user S_i. In this case, when the access authority is acquired, the decryption key for confidential files could be acquired, expressed as $J_i = \{x | x$ is the number of confidential file *for* S_i with authority access$\}$, $i = 1, 2, 3, \ldots, n$, and $n \in N$ is acquired. For instance, the user S_2 could access confidential files numbered 1 and 3, and the user S_3 could access confidential files numbered 1, 3, and 4. The mathematical equation is shown as $J_2 = \{1, 3\}$, $J_3 = \{1, 3, 4\}$. With the characteristics of partial order, $J_2 = \{1, 3\} \preccurlyeq J_3 = \{1, 3, 4\}$ stands for S_3 being able to acquire the decryption keys of S_2 for accessing $file_1$ and $file_3$.

According to the users' authority accessing confidential files, an access control matrix, as Figure 1 access authority control matrix, is established, where the numerical meanings present 1 for the users with access authority and 0 for the ones without authority access. For example, S_2 has the access authority to $file_1$ and $file_3$, but not to $file_2$ and $file_4$.

	$file_1$	$file_2$	$file_3$	$file_4$
S_1	0	1	0	1
S_2	1	0	1	0
S_3	1	0	1	1
S_4	0	1	1	0
S_5	1	1	0	0

Figure 1. Access authority control matrix.

Applying the previous mechanism to medical institutions to construct the decryption keys (DK_1, DK_2, …, DK_5) that possess six independent users (S_1, S_2, …, S_6) with individual secret keys (H_1, H_2, …, H_6) and five accessible confidential files in the access control matrix has the correspondent decryption keys (DK_1, DK_2, …, DK_5). When the decryption key for the confidential files can be acquired, the confidential files would be accessed. Figure 2 shows the situations of the users' access authority to confidential files.

According to Figure 5 and T.S. Chen's (2012) methodology [20], CA establishes the polynomial $A_i(x)$ for each user S_i and calculates as in the succeeding text.

$$A_i(x) = \left\{ \prod_{\substack{k=1 \\ k\neq i}}^{m} \frac{(x-H_k)}{(H_i-H_k)} \right\} \times I_{\{H_1,\ \cdots,\ H_n\}}(x),\ for\ i = 1,\ 2,\ \cdots,\ n \wedge x \in R.$$

$$A_1(x) = \frac{x-H_2}{H_1-H_2} \times \frac{x-H_3}{H_1-H_3} \times \frac{x-H_4}{H_1-H_4} \times \frac{x-H_5}{H_1-H_5} \times \frac{x-H_6}{H_1-H_6} \times I_{H_1}(x)$$

$$A_2(x) = \frac{x-H_1}{H_2-H_1} \times \frac{x-H_3}{H_2-H_3} \times \frac{x-H_4}{H_2-H_4} \times \frac{x-H_5}{H_2-H_5} \times \frac{x-H_6}{H_2-H_6} \times I_{H_2}(x)$$

$$A_3(x) = \frac{x-H_1}{H_3-H_1} \times \frac{x-H_2}{H_3-H_2} \times \frac{x-H_4}{H_3-H_4} \times \frac{x-H_5}{H_3-H_5} \times \frac{x-H_6}{H_3-H_6} \times I_{H_3}(x)$$

$$A_4(x) = \frac{x-H_1}{H_4-H_1} \times \frac{x-H_2}{H_4-H_2} \times \frac{x-H_3}{H_4-H_3} \times \frac{x-H_5}{H_4-H_5} \times \frac{x-H_6}{H_4-H_6} \times I_{H_4}(x)$$

$$A_5(x) = \frac{x-H_1}{H_5-H_1} \times \frac{x-H_2}{H_5-H_2} \times \frac{x-H_3}{H_5-H_3} \times \frac{x-H_4}{H_5-H_4} \times \frac{x-H_6}{H_5-H_6} \times I_{H_5}(x)$$

$$A_6(x) = \frac{x-H_1}{H_6-H_1} \times \frac{x-H_2}{H_6-H_2} \times \frac{x-H_3}{H_6-H_3} \times \frac{x-H_4}{H_6-H_4} \times \frac{x-H_5}{H_6-H_5} \times I_{H_6}(x)$$

	$file_1(DK_1)$ Blood Pressure Record	$file_2(DK_2)$ Electrocardiogram	$file_3(DK_3)$ Major Surgery Records	$file_4(DK_4)$ Drug and Allergic Reaction	$file_5(DK_5)$ Health Insurance Records
$S_1(H_1)$ Patient	1	1	1	1	1
$S_2(H_2)$ Physician	1	1	1	1	0
$S_3(H_3)$ Nurse	1	0	0	1	0
$S_4(H_4)$ Medical Researcher	0	0	0	1	0
$S_5(H_5)$ Health Insurance Unit	0	0	0	0	1
$S_6(H_6)$ Kinship	1	0	0	0	0

Figure 2. The situations of the users' access authority to confidential files.

where $I_{\{H_1,\ \cdots,\ H_6\}} = \begin{cases} 1, & if\ x \in \{H_1,\ \cdots,\ H_6\} \\ 0, & o.w. \end{cases}$ is an indicator function to verify the legality of H_i.

Moreover, CA also establishes the polynomial $B_i(y)$ for each user S_i and calculates as follows.

$$B_i(y) = \left\{ \sum_{u \in J_i} DK_u \left[\prod_{\substack{t=1 \\ t\neq u}}^{m} \frac{(y-t)}{(u-t)} \right] \right\} \times I_{J_i}(y),\ y \in R.$$

$\wedge J_i = \{u | 1 \leq u \leq m,\ u$ is the number of confidential file f or the i user ' s authorized access$\}$

$$B_1(y) = \begin{bmatrix} DK_1 \times \frac{(y-2)(y-3)(y-4)(y-5)}{(1-2)(1-3)(1-4)(1-5)} \\ +DK_2 \times \frac{(y-1)(y-3)(y-4)(y-5)}{(2-1)(2-3)(2-4)(2-5)} \\ +DK_3 \times \frac{(y-1)(y-2)(y-4)(y-5)}{(3-1)(3-2)(3-4)(3-5)} \\ +DK_4 \times \frac{(y-1)(y-2)(y-3)(y-5)}{(4-1)(4-2)(4-3)(4-5)} \\ +DK_5 \times \frac{(y-1)(y-2)(y-3)(y-4)}{(5-1)(5-2)(5-3)(5-4)} \end{bmatrix} \times I_{J_1}(y)$$

$$B_2(y) = \begin{bmatrix} DK_1 \times \frac{(y-2)(y-3)(y-4)(y-5)}{(1-2)(1-3)(1-4)(1-5)} \\ +DK_2 \times \frac{(y-1)(y-3)(y-4)(y-5)}{(2-1)(2-3)(2-4)(2-5)} \\ +DK_3 \times \frac{(y-1)(y-2)(y-4)(y-5)}{(3-1)(3-2)(3-4)(3-5)} \\ +DK_4 \times \frac{(y-1)(y-2)(y-3)(y-5)}{(4-1)(4-2)(4-3)(4-5)} \end{bmatrix} \times I_{J_2}(y)$$

$$B_3(y) = \begin{bmatrix} DK_1 \times \frac{(y-2)(y-3)(y-4)(y-5)}{(1-2)(1-3)(1-4)(1-5)} \\ +DK_4 \times \frac{(y-1)(y-2)(y-3)(y-5)}{(4-1)(4-2)(4-3)(4-5)} \end{bmatrix} \times I_{J_3}(y)$$

$$B_4(y) = \left[DK_4 \times \frac{(y-1)(y-2)(y-3)(y-5)}{(4-1)(4-2)(4-3)(4-5)} \right] \times I_{J_4}(y)$$

$$B_5(y) = \left[DK_5 \times \frac{(y-1)(y-2)(y-3)(y-4)}{(5-1)(5-2)(5-3)(5-4)} \right] \times I_{J_5}(y)$$

$$B_6(y) = \left[DK_1 \times \frac{(y-2)(y-3)(y-4)(y-5)}{(1-2)(1-3)(1-4)(1-5)} \right] \times I_{J_6}(y)$$

where $I_{J_i}(y) = \begin{cases} 1, & if\ y \in J_i \\ 0, & o.w. \end{cases}$ is an indicator function to verify the user's access authority to the decryption key DK_u.

Finally, CA establishes the following equation and publishes the expansion.

$$G(x,\ y)=\sum_{i=1}^{n}A_i(x)B_i(y)\wedge x,\ y\in R.$$

2.3.1. Insecurity of T.S. Chen (2012) methodology with mathematical characteristics of polynomial $A_i(x)B_i(y)$

When the effects of $I_{H_i}(x)$ and $I_{J_i}(y)$ are removed, $A_i(x)$ and $B_i(y)$ present the mathematical characteristics.

Assuming $y=0$, the first-order polynomial $\prod_{\substack{k=1\\k\neq i}}^{n}(x-H_k)$ would be acquired through a series of deduction [21].

The insecurity is proven according to $A_i(x)B_i(y)$ polynomial in the previous section.

$$\begin{aligned}A_i(x)&=\frac{x-H_1}{H_i-H_1}\times\cdots\times\frac{x-H_{i-1}}{H_i-H_{i-1}}\\&\quad\times\frac{x-H_{i+1}}{H_i-H_{i+1}}\times\cdots\times\frac{x-H_n}{H_i-H_n}\times I_{H_i}(x)\\&=\left\{\prod_{\substack{k=1\\k\neq i}}^{n}\frac{(x-H_k)}{(H_i-H_k)}\right\}\times I_{\{H_i\}}(x)\end{aligned}$$

$$B_i(y)=\left[b_{m-1}^{(i)}y^{m-1}+b_{m-2}^{(i)}y^{m-2}+\cdots+b_1^{(i)}y+b_0^{(i)}\right]\times I_{J_i}(y)$$

$$\begin{aligned}A_i(x)B_i(y)&=\left[\prod_{\substack{k=1\\k\neq i}}^{n}\frac{(x-H_k)}{(H_i-H_k)}\right]\times I_{\{H_i\}}(x)\times\left[b_{m-1}^{(i)}y^{m-1}+\cdots+b_1^{(i)}y+b_0^{(i)}\right]\times I_{J_i}(y)\\&=\left\{\left[\prod_{\substack{k=1\\k\neq i}}^{n}\frac{(x-H_k)}{(H_i-H_k)}\right]\left[b_{m-1}^{(i)}y^{m-1}+\cdots+b_1^{(i)}y+b_0^{(i)}\right]\right\}\times I_{\{H_i\}}(x)\times I_{J_i}(y)\\&=\left\{\left[\prod_{\substack{k=1\\k\neq i}}^{n}\frac{(x-H_k)}{(H_i-H_k)}\right]\left[b_{m-1}^{(i)}y^{m-1}+\cdots+b_1^{(i)}y\right]+\left[\prod_{\substack{k=1\\k\neq i}}^{n}\frac{(x-H_k)}{(H_i-H_k)}\right]b_0^{(i)}\right\}I_{\{H_i\}}(x)I_{J_i}(y)\end{aligned}$$

Assuming

$$A_i^*(x)B_i^*(y)=\left\{\left[\prod_{\substack{k=1\\k\neq i}}^{n}\frac{(x-H_k)}{(H_i-H_k)}\right]\left[b_{m-1}^{(i)}y^{m-1}+\cdots+b_1^{(i)}y\right]+\left[\prod_{\substack{k=1\\k\neq i}}^{n}\frac{(x-H_k)}{(H_i-H_k)}\right]b_0^{(i)}\right\}$$

$$A_i(x)B_i(y)=A_i^*(x)B_i^*(y)I_{\{H_i\}}(x)I_{J_i}(y)$$

From the previous mathematical form $A_i(x)B_i(y)$, the expansion could be acquired, and then $I_{\{H_i\}}(x)I_{J_i}(y)$ could be neglected.

$$\text{Replacing } A_i^*(x)B_i^*(y) \text{ for } A_i(x)B_i(y)$$

and assuming $y=0$ to substitute $A_i^*(x)B_i^*(y)$

$$\begin{aligned}A_i^*(x)B_i^*(0)&=\left[\prod_{\substack{k=1\\k\neq i}}^{n}\frac{(x-H_k)}{(H_i-H_k)}\right]b_0^{(i)}\\&=\left[\prod_{\substack{k=1\\k\neq i}}^{n}b_0^{(i)}\frac{1}{(H_i-H_k)}\right]\left[\prod_{\substack{k=1\\k\neq i}}^{n}(x-H_k)\right]\end{aligned}$$

$$\text{Assuming } \alpha_i=\left[\prod_{\substack{k=1\\k\neq i}}^{n}b_0^{(i)}\frac{1}{(H_i-H_k)}\right]$$

$$A_i^*(x)B_i^*(0)=\alpha_i\left[\prod_{\substack{k=1\\k\neq i}}^{n}(x-H_k)\right]$$

When the equation is divided by the leading coefficient α_i, the first-order polynomial $\prod_{\substack{k=1\\k\neq i}}^{n}(x-H_k)$ is proven.

2.3.2. Decrypting polynomial $G(x, y)$ with the mathematical characteristics of $A_i(x)B_i(y)$

From the previous access authority control matrix, six users in the system could access five confidential files. The mathematical characteristics of $A_i(x)B_i(y)$ could be used for breaking the system and deducting the decryption key. The breaking process is described as in the succeeding text.

$$\text{Assuming } G_1(x,\ y)=\sum_{i=1}^{6}A_i(x)B_i(y)$$

When adding a new user $S_7(H_7)$ to the system, according to T.S. Chen's (2012) methodology, a new public polynomial $G_2(x, y)=G_1(x, y)+A_7(x)B_7(y)$ is acquired. When another new user $S_8(H_8)$ is added, another new public polynomial $G_3(x, y)=G_2(x, y)+A_8(x)B_8(y)$ is acquired.

Although $A_i(x)$ and $B_i(y)$ are not published, the published polynomials could be used for deducting;

$$A_7(x)B_7(y) = G_2(x,\ y) - G_1(x,\ y)$$

$$A_8(x)B_8(y) = G_3(x,\ y) - G_2(x,\ y)$$

With the properties introduced in previous section, $A_7(x)B_7(y)$ and $A_8(x)B_8(y)$ could be calculated:

$$A_7^*(x)B_7^*(0) = \alpha_7 \left[\prod_{\substack{k=1 \\ k\neq 7}}^{7} (x - H_k) \right]$$
$$= \alpha_7(x - H_1)(x - H_2)(x - H_3)(x - H_4)(x - H_5)(x - H_6)$$

$$zptA_8^*(x)B_8^*(0) = \alpha_8 \left[\prod_{\substack{k=1 \\ k\neq 8}}^{8} (x - H_k) \right]$$
$$= \alpha_8(x - H_1)(x - H_2)(x - H_3)(x - H_4)(x - H_5)$$
$$(x - H_6)(x - H_7)$$
$$\frac{A_8^*(x)B_8^*(0)}{A_7^*(x)B_7^*(0)} = \frac{\alpha_8}{\alpha_7}(x - H_7)$$

where α_7 and α_8 could be deducted.

$(x - H_7)$ is then acquired by dividing the two. Assuming it as 0, the secret key H_7 could then be easily acquired.

Similarly, when a new member $S_9(H_9)$ is added, the polynomial $(x - H_1)(x - H_2)(x - H_3)(x - H_4)(x - H_5)(x - H_6)(x - H_7)(x - H_8)$ could be acquired with the previous calculations. $(x - H_8)$ could also be acquired after dividing the two. That is, when two member data are continuously added to the system, the secret key of the $m - 1$ member could be acquired through the public polynomial and simple calculations once the m member joins in. Information insecurity therefore is easily generated.

3. RESEARCH METHODOLOGY

3.1. User authority setting

Public health records are a system that could establish and integrate each patient's records in different medical institutions. When the user needs to access to the records, he/she has to possess the access authority to the confidential files as well as the secret key. CA establishes an authority access control matrix that contains the user's access authority to confidential files and the file quantity and contents, where 0 stands for the user without the access authority and 1 for the user with the authority, as Figure 3 member authority access matrix.

	$file_1(DK_1)$ Blood Pressure Record	$file_2(DK_2)$ Electrocardiogram	$file_3(DK_3)$ Major Surgery Records	$file_4(DK_4)$ Drug and Allergic Reaction	$file_5(DK_5)$ Health Insurance Records
$S_1(H_1)$ Patient	1	1	1	1	1
$S_2(H_2)$ Physician	1	1	1	1	0
$S_3(H_3)$ Nurse	1	0	0	1	0
$S_4(H_4)$ Medical Researcher	1	1	0	1	0
$S_5(H_5)$ Health Insurance Unit	0	0	0	0	1
$S_6(H_6)$ Kinship	1	0	0	1	0

Figure 3. Member authority access matrix.

3.2. Improved T.S. Chen's (2012) methodology

T.S. Chen's approach in 2012 was a simple equation with the division of new-style and old-style derivative coefficients that a secret key could be easily acquired by making the equation zero. This proposed approach could exclude the effect of original parameters; when $y = 0$, the secret key still cannot be solved so that the security of decryption polynomial in dynamic update is ensured.

3.2.1. Methodology establishment

As described in Section 3, the mathematical characteristics of $A_i(x)B_i(y)$ result in the entire decryption polynomial being easily broken to cause the system insecurity that T.S. Chen's (2012) methodology is improved, and more secure encryption algorithms are proposed in this study to stabilize the system security.

The approaches are shown as following.

Step 1: According to the authority access matrix, CA establishes new polynomials $A_i^{(r)}(x)$ and $B_i^{(r)}(y)$ aiming at each PHR user (S_i).

Step 2: Establish a new private polynomial $A_i^{(r)}(x)$.

$$A_i^{(r)}(x) = \left\{ \prod_{\substack{1\leq k\leq n \\ k\neq i}} \left[\frac{x - H_k}{H_i - H_k} + (x - H_i) \right] \right\} \times I_{\{H_i\}}^{(x)},\ for\ i$$
$$= 1,\ 2,\ \cdots,\ n \wedge x \in R.$$

where $I_{\{H_i\}}^{(x)} = \begin{cases} 1, & if\ x \in \{H_1,\ \cdots,\ H_n\} \\ 0, & o.w. \end{cases}$ verifies the legality of H_i.

Step 3: Ensure the establishment of the following conditions.

(a): When H_i is a legal secret key, $\Theta_i^{(r)}(x)$ appears 1, or otherwise 0.

(b): $\Theta_i^{(r)}(x) = I_{\{1\}}^{\left(A_i^{(r)}(x)\right)}$, $\Theta_i^{(r)}(H_i) = 1$, $\Theta_i^{(r)}(\neq H_i) = 0$.

Step 4: Establish a new private polynomial $B_i^{(r)}(y)$.

$$B_i^{(r)}(y) = \left[b_{m-1}^{(i)} y^{m-1} + \cdots + b_1^{(i)} y + b_0^{(i)}\right] \times I_{J_i}^{(y)},\ y \in R.$$

$$\wedge J_i = \left\{ u \,\middle|\, \begin{array}{c} 1 \le u \le m,\ u \text{ is the number of confidential file for the } i \\ \text{user's access authority} \end{array} \right\}$$

where $I_{J_i}(y) = \begin{cases} 1, & \text{if } y \in J_i \\ 0, & \text{otherwise} \end{cases}$ verifies the user's access authority to the decryption key DK_u.

Step 5 Finally, CA establishes the expansion of the decryption polynomial and publishes as in the previous text.

$$G^{(r)}(x,\ y) = \sum_{i=1}^{n} A_i^{(r)}(x) B_i^{(r)}(y) \wedge x,\ y \in R.$$

3.2.2. Security check of decryption polynomial

Regarding the removal of the effects of $I_{\{H_i\}}^{(x)}$ and $I_{J_i}^{(y)}$, assuming $y = 0$, the secret key H_k would not be broken to ensure the security of the decryption polynomial. It is proven as follows.

$$A_i^{(r)}(x) = \left\{ \prod_{\substack{1 \le k \le n \\ k \ne i}} \left[\frac{x - H_k}{H_i - H_k} + (x - H_i) \right] \right\} \times I_{\{H_i\}}^{(x)},\ \text{for } i = 1,\ 2,\ \cdots,\ n \wedge x \in R.$$

$$B_i^{(r)}(y) = \left[b_{m-1}^{(i)} y^{m-1} + \cdots + b_1^{(i)} y + b_0^{(i)}\right] \times I_{J_i}^{(y)},\ y \in R.$$

$$A_i^{(r)}(x) B_i^{(r)}(y) = \left\{ \left\{ \prod_{\substack{1 \le k \le n \\ k \ne i}} \left[\frac{x - H_k}{H_i - H_k} + (x - H_i) \right] \right\} \times I_{\{H_i\}}^{(x)} \times \left[b_{m-1}^{(i)} y^{m-1} + \cdots + b_1^{(i)} y + b_0^{(i)}\right] \times I_{J_i}^{(y)} \right\}$$

$$= \left\{ \left\{ \prod_{\substack{1 \le k \le n \\ k \ne i}} \left[\frac{x - H_k}{H_i - H_k} + (x - H_i) \right] \right\} \times \left[b_{m-1}^{(i)} y^{m-1} + \cdots + b_1^{(i)} y + b_0^{(i)}\right] \right\} \times I_{\{H_i\}}^{(x)} \times I_{J_i}^{(y)}$$

Assuming

$$A_i^{*(r)}(x) B_i^{*(r)}(y) = \left\{ \left\{ \prod_{\substack{1 \le k \le n \\ k \ne i}} \left[\frac{x - H_k}{H_i - H_k} + (x - H_i) \right] \right\} \left[b_{m-1}^{(i)} y^{m-1} + \cdots + b_1^{(i)} y + b_0^{(i)}\right] \right\}$$

$$A_i^{(r)}(x) B_i^{(r)}(y) = A_i^{*(r)}(x) B_i^{*(r)}(y) I_{\{H_i\}}^{(x)} I_{J_i}^{(y)}$$

According to the expansion of the polynomial, the characteristics of $I_{\{H_i\}}(x) I_{J_i}(y)$ could be ignored.

$$\text{Replacing } A_i^{*(r)}(x) B_i^{*(r)}(y) \text{ for } A_i^{(r)}(x) B_i^{(r)}(y)$$

and assuming $y = 0$ to substitute $A_i^{*(r)}(x) B_i^{*(r)}(y)$,

$$A_i^{*(r)}(x) B_i^{*(r)}(0) = \left\{ \prod_{\substack{1 \le k \le n \\ k \ne i}} \left[\frac{x - H_k}{H_i - H_k} + (x - H_i) \right] \right\} b_0^{(i)}$$

From the previous mathematical form, it could not be factorized that it could not acquire the first-order polynomial $\prod_{\substack{1 \le k \le n \\ k \ne i}}^{n} (x - H_k)$ as the previous, and the secret key H_k could not be solved. The system security is implemented.

3.2.3. Security check of decryption polynomial $G^{(r)}(x, y)$

As the example of the system with six users accessing five confidential documents, CA constructs the decryption polynomial as in the succeeding text.

$$\text{Assuming } G_1^{(r)}(x,\ y) = \sum_{i=1}^{6} A_i^{(r)}(x) B_i^{(r)}(y)$$

When a new user $S_7(H_7)$ is added to the system, a brand-new public polynomial $G_2^{(r)}(x,\ y) = G_1^{(r)}(x,\ y) + A_7^{(r)}(x) B_7^{(r)}(y)$ is acquired. Adding another new user $S_8(H_8)$ to the system, another new public polynomial $G_3^{(r)}(x,\ y) = G_2^{(r)}(x,\ y) + A_8^{(r)}(x) B_8^{(r)}(y)$ is also acquired, where $A_i^{(r)}(x)$ and $B_i^{(r)}(y)$ are private, while $G_1^{(r)}(x,\ y)$, $G_2^{(r)}(x,\ y)$, and $G_3^{(r)}(x,\ y)$ are public. The testing processes are shown as follows.

$$G_2^{(r)}(x,\ y) - G_1^{(r)}(x,\ y) = A_7^{(r)}(x) B_7^{(r)}(y)$$

$$G_3^{(r)}(x,\ y) - G_2^{(r)}(x,\ y) = A_8^{(r)}(x) B_8^{(r)}(y)$$

$A_7^{(r)}(x) B_7^{(r)}(y)$ and $A_8^{(r)}(x) B_8^{(r)}(y)$ could be calculated by the properties introduced in the previous section.

$$A_7^{*(r)}(x)B_7^{*(r)}(0) = \left\{ \prod_{\substack{1\le k\le 7\\ k\neq 7}} \left[\frac{x-H_k}{H_7-H_k} + (x-H_7)\right] \right\} b_0^{(7)}$$
$$= \left[\frac{x-H_1}{H_7-H_1} + (x-H_7)\right] \times \left[\frac{x-H_2}{H_7-H_2} + (x-H_7)\right]$$
$$\times \left[\frac{x-H_3}{H_7-H_3} + (x-H_7)\right] \times \left[\frac{x-H_4}{H_7-H_4} + (x-H_7)\right]$$
$$\times \left[\frac{x-H_5}{H_7-H_5} + (x-H_7)\right] \times \left[\frac{x-H_6}{H_7-H_6} + (x-H_7)\right]$$

$$A_8^{*(r)}(x)B_8^{*(r)}(0) = \left\{ \prod_{\substack{1\le k\le 8\\ k\neq 8}} \left[\frac{x-H_k}{H_8-H_k} + (x-H_8)\right] \right\} b_0^{(8)}$$
$$= \left[\frac{x-H_1}{H_8-H_1} + (x-H_8)\right] \times \left[\frac{x-H_2}{H_8-H_2} + (x-H_8)\right]$$
$$\times \left[\frac{x-H_3}{H_8-H_3} + (x-H_8)\right] \times \left[\frac{x-H_4}{H_8-H_4} + (x-H_8)\right]$$
$$\times \left[\frac{x-H_5}{H_8-H_5} + (x-H_8)\right] \times \left[\frac{x-H_6}{H_8-H_6} + (x-H_8)\right]$$
$$\times \left[\frac{x-H_7}{H_8-H_7} + (x-H_8)\right]$$

$$\frac{A_8^{*(r)}(x)B_8^{*(r)}(0)}{A_7^{*(r)}(x)B_7^{*(r)}(0)} = \frac{\left[\frac{x-H_1}{H_8-H_1} + (x-H_8)\right] \times \left[\frac{x-H_2}{H_8-H_2} + (x-H_8)\right] \times \cdots \times \left[\frac{x-H_7}{H_8-H_7} + (x-H_8)\right]}{\left[\frac{x-H_1}{H_7-H_1} + (x-H_7)\right] \times \left[\frac{x-H_2}{H_7-H_2} + (x-H_7)\right] \times \cdots \times \left[\frac{x-H_6}{H_7-H_6} + (x-H_7)\right]}$$

From previous deduction, merely a series of mathematical forms that could no longer be factorized are acquired after dividing $A_7^{*(r)}(x)B_7^{*(r)}(0)$ with $A_8^{*(r)}(x)B_8^{*(r)}(0)$, so that the secret keys H_7 and H_8 could not be acquired in order to prevent the decryption keys for S_7 and S_8 accessing files from being deducted.

Similarly, when a member $S_9(H_9)$ is added, the followings could be deducted.

$$A_9^{*(r)}(x)B_9^{*(r)}(0) = \left\{ \prod_{\substack{1\le k\le 9\\ k\neq 9}} \left[\frac{x-H_k}{H_9-H_k} + (x-H_9)\right] \right\} b_0^{(9)}$$
$$= \left[\frac{x-H_1}{H_9-H_1} + (x-H_9)\right] \times \left[\frac{x-H_2}{H_9-H_2} + (x-H_9)\right]$$
$$\times \left[\frac{x-H_3}{H_9-H_3} + (x-H_9)\right] \times \left[\frac{x-H_4}{H_9-H_4} + (x-H_9)\right]$$
$$\times \left[\frac{x-H_5}{H_9-H_5} + (x-H_9)\right] \times \left[\frac{x-H_6}{H_9-H_6} + (x-H_9)\right]$$
$$\times \left[\frac{x-H_7}{H_9-H_7} + (x-H_9)\right] \times \left[\frac{x-H_8}{H_9-H_8} + (x-H_9)\right]$$

A series of mathematical forms that could not be factorized anymore are still acquired after dividing two formulas. In this case, even though new members are continuously added, the secret key H_9 could not be deducted from the mathematical form, so that the system is secure.

3.3. Example

Aiming at the new public polynomial $G^{(r)}(x, y) = \sum_{i=1}^{n} A_i^{(r)}(x)B_i^{(r)}(y)$ established in the previous section, the member authority access matrix in Figure 3 is used for the illustration.

3.3.1. Example: legal access authority of user

Assuming that a medical researcher (S_4) possesses legal access authority to blood pressure record (*file*$_1$), electrocardiogram (*file*$_2$), and drug and allergic reaction (*file*$_4$), the secret key (H_4) is first substituted for $A_4^{(r)}(x)$.

$$A_4^{(r)}(x) = \left\{ \prod_{\substack{1\le k\le 6\\ k\neq 4}} \left[\frac{x-H_k}{H_i-H_k} + (x-H_4)\right] \right\} \times I^{(H_4)}_{\{H_1,\ \cdots,\ H_6\}}$$
$$= \left\{ \left[\frac{x-H_1}{H_4-H_1} + (x-H_4)\right] \times \left[\frac{x-H_2}{H_4-H_2} + (x-H_4)\right] \right.$$
$$\times \left[\frac{x-H_3}{H_4-H_3} + (x-H_4)\right] \times \left[\frac{x-H_5}{H_4-H_5} + (x-H_4)\right]$$
$$\left. \times \left[\frac{x-H_6}{H_4-H_6} + (x-H_4)\right] \right\} \times I^{(H_4)}_{\{H_1,\ \cdots,\ H_6\}}$$

Furthermore, $I^{(H_4)}_{\{H_1,\ \cdots,\ H_6\}} = 1$ and then $A_4^{(r)}(H_4) = 1$ are calculated; the result of $A_4^{(r)}(H_k)(\ k\in\{1,\ 2,\ 3,\ 5,\ 6\})$ is a series of random numbers; however, the final value appears as 0 because $\Theta_i^{(r)}(x) = I^{(A_i^{(r)}(x))}_{\{1\}}$, so that it does not present the access authority. The polynomial $A_i^{(r)}(x)$ could be utilized for verifying the user as well as the secret key H_i being on the legal list of CA.

After confirming the medical researcher (S_4) being a legal user, the access authority to three confidential files of blood pressure record (*file*$_1$), electrocardiogram (*file*$_2$), and drug and allergic reaction (*file*$_4$) are further verified. Replacing $J_4 = \{1, 2, 4\}$ for $B_4^{(r)}(y)$,

$$B_4^{(r)}(y) = \left[\begin{array}{l} DK_1 \times \dfrac{(y-2)(y-3)(y-4)(y-5)}{(1-2)(1-3)(1-4)(1-5)} \\ +DK_2 \times \dfrac{(y-1)(y-3)(y-4)(y-5)}{(2-1)(2-3)(2-4)(2-5)} \\ +DK_4 \times \dfrac{(y-1)(y-2)(y-3)(y-5)}{(4-1)(4-2)(4-3)(4-5)} \end{array} \right] \times I_{J_4}(y)$$

After calculating $I_{J_4}(1) = 1, I_{J_4}(2) = 1$, and $I_{J_4}(4) = 1$, $B_4^{(r)}(1) = DK_1$, $B_4^{(r)}(2) = DK_2$, $B_4^{(r)}(3) = 0$, $B_4^{(r)}(4) = DK_4$, and $B_4^{(r)}(5) = 0$ are further calculated to prove the medical researcher's (S_4) access authority to acquire the decryption keys for blood pressure record (*file*$_1$), electrocardiogram (*file*$_2$), and drug and allergic reaction (*file*$_4$).

When the medical researcher (S_4) intends to access to a patient's electrocardiogram ($file_2$) for the research, the personal legal secret key H_4 and ID2 of the electrocardiogram ($file_2$) are substitute for the public polynomial $G^{(r)}(x, y)$ for the calculation.

$$\begin{aligned} G^{(r)}(H_4,\ 2) &= A_1^{(r)}(H_4)B_1^{(r)}(2) + A_2^{(r)}(H_4)B_2^{(r)}(2) \\ &\quad + A_3^{(r)}(H_4)B_3^{(r)}(2) + A_4^{(r)}(H_4)B_4^{(r)}(2) \\ &\quad + A_5^{(r)}(H_4)B_5^{(r)}(2) + A_6^{(r)}(H_4)B_6^{(r)}(2) \end{aligned}$$

The decryption key (DK_2) for the electrocardiogram ($file_2$) required by the medical researcher (S_4) is hidden in $A_4^{(r)}(H_4)B_4^{(r)}(2)$.

$$\begin{aligned} A_4^{(r)}(H_4) &= \left\{\left[\frac{H_4-H_1}{H_4-H_1}+(H_4-H_4)\right]\times\left[\frac{H_4-H_2}{H_4-H_2}+(H_4-H_4)\right]\right. \\ &\quad \times\left[\frac{H_4-H_3}{H_4-H_3}+(H_4-H_4)\right]\times\left[\frac{H_4-H_5}{H_4-H_5}+(H_4-H_4)\right] \\ &\quad \left.\times\left[\frac{H_4-H_6}{H_4-H_6}+(H_4-H_4)\right]\right\}\times I^{(H_4)}_{\{H_1,\ \cdots,\ H_6\}} \\ &= 1 \end{aligned}$$

$$\begin{aligned} B_4^{(r)}(2) &= \left[\begin{array}{l} DK_1\times\dfrac{(2-2)(2-3)(2-4)(2-5)}{(1-2)(1-3)(1-4)(1-5)} \\ +DK_2\times\dfrac{(2-1)(2-3)(2-4)(2-5)}{(2-1)(2-3)(2-4)(2-5)} \\ +DK_4\times\dfrac{(2-1)(2-2)(2-3)(2-5)}{(4-1)(4-2)(4-3)(4-5)} \end{array}\right]\times I_{J_4}(2) \\ &= [DK_1\times 0 + DK_2\times 1 + DK_4\times 0]\times 1 \\ &= DK_2 \end{aligned}$$

The rest shows 0 because of inadequate information.

$$\begin{aligned} A_1^{(r)}(H_4) &= \left\{\left[\frac{H_4-H_2}{H_1-H_2}+(H_4-H_1)\right]\times\left[\frac{H_4-H_3}{H_1-H_3}+(H_4-H_1)\right]\right. \\ &\quad \times\left[\frac{H_4-H_4}{H_1-H_4}+(H_4-H_1)\right]\times\left[\frac{H_4-H_5}{H_1-H_5}+(H_4-H_1)\right] \\ &\quad \left.\times\left[\frac{H_4-H_6}{H_1-H_6}+(H_4-H_1)\right]\right\}\times I^{(H_4)}_{\{H_1,\ \cdots,\ H_6\}} \\ &= m \end{aligned}$$

$$\begin{aligned} A_2^{(r)}(H_4) &= \left\{\left[\frac{H_4-H_1}{H_2-H_1}+(H_4-H_2)\right]\times\left[\frac{H_4-H_3}{H_2-H_3}+(H_4-H_2)\right]\right. \\ &\quad \times\left[\frac{H_4-H_4}{H_2-H_4}+(H_4-H_2)\right]\times\left[\frac{H_4-H_5}{H_2-H_5}+(H_4-H_2)\right] \\ &\quad \left.\times\left[\frac{H_4-H_6}{H_2-H_6}+(H_4-H_2)\right]\right\}\times I^{(H_4)}_{\{H_1,\ \cdots,\ H_6\}} \\ &= m \end{aligned}$$

$$\begin{aligned} A_3^{(r)}(H_4) &= \left\{\left[\frac{H_4-H_1}{H_3-H_1}+(H_4-H_3)\right]\times\left[\frac{H_4-H_2}{H_3-H_2}+(H_4-H_3)\right]\right. \\ &\quad \times\left[\frac{H_4-H_4}{H_3-H_4}+(H_4-H_3)\right]\times\left[\frac{H_4-H_5}{H_3-H_5}+(H_4-H_3)\right] \\ &\quad \left.\times\left[\frac{H_4-H_6}{H_3-H_6}+(H_4-H_3)\right]\right\}\times I^{(H_4)}_{\{H_1,\ \cdots,\ H_6\}} \\ &= m \end{aligned}$$

$$\begin{aligned} A_5^{(r)}(H_4) &= \left\{\left[\frac{H_4-H_1}{H_5-H_1}+(H_4-H_5)\right]\times\left[\frac{H_4-H_2}{H_5-H_2}+(H_4-H_5)\right]\right. \\ &\quad \times\left[\frac{H_4-H_3}{H_5-H_3}+(H_4-H_5)\right]\times\left[\frac{H_4-H_4}{H_5-H_4}+(H_4-H_5)\right] \\ &\quad \left.\times\left[\frac{H_4-H_6}{H_5-H_6}+(H_4-H_5)\right]\right\}\times I^{(H_4)}_{\{H_1,\ \cdots,\ H_6\}} \\ &= m \end{aligned}$$

$$\begin{aligned} A_6^{(r)}(H_4) &= \left\{\left[\frac{H_4-H_1}{H_6-H_1}+(H_4-H_6)\right]\times\left[\frac{H_4-H_2}{H_6-H_2}+(H_4-H_6)\right]\right. \\ &\quad \times\left[\frac{H_4-H_3}{H_6-H_3}+(H_4-H_6)\right]\times\left[\frac{H_4-H_4}{H_6-H_4}+(H_4-H_6)\right] \\ &\quad \left.\times\left[\frac{H_4-H_5}{H_6-H_5}+(H_4-H_6)\right]\right\}\times I^{(H_4)}_{\{H_1,\ \cdots,\ H_6\}} \\ &= m \end{aligned}$$

m acquired from the previous equations appears as a huge disordered number; however, $A_4^{(r)}(H_k)(\ k\in\{1,\ 2,\ 3,\ 5,\ 6\})$ does not have the access authority that $\Theta_i^{(r)}(x) = I^{\left(A_i^{(r)}(x)\right)}_{\{1\}}$ could be utilized for transforming the invalid value m to 0 in order to avoid invalid operation.

Accordingly, the medical researcher (S_4) could successfully deduct the decryption key (DK_2) for the electrocardiogram ($file_2$) with the following equations.

$$\begin{aligned} G^{(r)}(H_4,\ 2) &= A_1^{(r)}(H_4)B_1^{(r)}(2) + A_2^{(r)}(H_4)B_2^{(r)}(2) \\ &\quad + A_3^{(r)}(H_4)B_3^{(r)}(2) + A_4^{(r)}(H_4)B_4^{(r)}(2) \\ &\quad + A_5^{(r)}(H_4)B_5^{(r)}(2) + A_6^{(r)}(H_4)B_6^{(r)}(2) \\ &= 0 + 0 + 0 + 1\times DK_2 + 0 + 0 \\ &= DK_2 \end{aligned}$$

4. DYNAMIC ACCESS CONTROL

The so-called user or file transaction indicates the addition and removal of members and the authority revision in the system, or the appending or removal of confidential files. Because PHR systems could be transacted any time in daily life, for example, a medical researcher can no longer operate the confidential file of the patient's electrocardiogram after completing the research project, the medical researcher's access authority to the electrocardiogram needs to be revised to disable the access. The responses to the user or file transaction in the system are described as in the succeeding text.

4.1. User modification: member adding

When adding a new member to the system, CA establishes the access authority to the confidential files as well as updates the old public polynomial $G^{(r)}(x, y)$ to publish it. The steps to add a member are shown as following.

Step 1: Adding a new member S_{n+1}, CA establishes a private secret key H_{n+1}.

Step 2: CA updates the private polynomial $A_{n+1}^{(r)}(x)$ and the verification indicator $I^{(x)}_{\{H_{n+1}\}}$.

$$A_{n+1}^{(r)}(x)=\left\{\prod_{\substack{1\le k\le n+1\\ k\neq n+1}}\left[\frac{x-H_k}{H_{n+1}-H_k}+(x-H_{n+1})\right]\right\}\times I_{\{H_{n+1}\}}^{(x)}$$

Step 3: When H_{n+1} is a legal secret key, $A_{n+1}^{(r)}(H_{n+1})$ appears as 1, or otherwise 0, revealing

$$\Theta_{n+1}^{(r)}(x)=I_{\{1\}}^{\left(A_{n+1}^{(r)}(x)\right)},\ \Theta_{n+1}^{(r)}(H_{n+1})=1,\ \text{and}\ \Theta_{n+1}^{(r)}(\neq H_{n+1})=0.$$

Step 4: CA updates the private polynomial $B_{n+1}^{(r)}(y)$ and the verification indicator $I_{J_{n+1}}(y)$.

$$B_{n+1}^{(r)}(y)=\left\{\sum_{u\in J_{n+1}}DK_u\left[\prod_{\substack{t=1\\ t\neq u}}^{m}\frac{(y-t)}{(u-t)}\right]\right\}\times I_{J_{n+1}}(y),\ y\in R.$$

$\wedge J_{n+1}=\{u|1\le u\le m,\ u$ is the number of the confidential file the $n+1$ user's access authority$\}$

where $I_{J_{n+1}}(y)=\begin{cases}1, & \text{if } y\in J_{n+1}\\ 0, & \text{otherwise}\end{cases}$.

Step 5: The original public polynomial $G^{(r)}(x,\ y)$ is updated as $\overline{G^{(r)}(x,\ y)}$.

$$\overline{G^{(r)}(x,\ y)}=G^{(r)}(x,\ y)+A_{n+1}^{(r)}(x)B_{n+1}^{(r)}(y)$$

From the previous member adding steps, CA would establish $A_{n+1}^{(r)}(x)$, $B_{n+1}^{(r)}(y)$, and J_{n+1} as well as update the verification indicators $I_{\{H_{n+1}\}}^{(x)}$, $\Theta_{n+1}^{(r)}(x)$, and $I_{J_{n+1}}(y)$ for the new member S_{n+1} and finally update such information to the original public polynomial $G^{(r)}(x,\ y)$. The entire adding process merely requires few costs for updating S_{n+1}; besides, merely addition is applied to the final $G^{(r)}(x,\ y)$ updating so that the calculation cost is largely reduced.

4.2. User modification: member removal

When a member no longer participates in the work related to the PHR system, the relevant operations would be prohibited. The member's access authority to confidential files would be removed to avoid having the member steal the confidential data illegally.

Assuming to remove the member S_k, two methods are used by CA. One is to remove the relevant parameters $A_k^{(r)}(x)$ and $B_k^{(r)}(y)$ to the member S_k from the public polynomial.

$$\overline{\overline{G^{(r)}(x,y)}}=G^{(r)}(x,y)-A_k^{(r)}(x)B_k^{(r)}(y)$$

The other is to directly destroy the member's access authority to confidential document and update $J_k^{'}=\{\}$.

4.3. Modification of user access authority

When a PHR system user's access authority is modified (added or removed), CA would adjust the authority access matrix and revise the relevant parameters with the following steps.

Step 1: CA resets the verification indicator J_i of the user's decryption key DK_u for the access authority

$J_i^{'}=\{u|1\le u\le m,\ u$ is the number of confidential file the i user's access authority$\}$

$J_i^{'}$ is the new authority set after the user S_i modified the access authority and CA recalculating the member authority access matrix.

Step 2: Because updating the verification indicator J_i is closely related to $B_i^{(r)}(y)$, the polynomial $B_i^{(r)}(y)$ has to be updated as $B_i^{'(r)}(y)$ when CA updates the verification indicator J_i as $J_i^{'}$. Finally, the updated public polynomial is shown as in the succeeding text.

$$\widetilde{G^{(r)}(x,\ y)}=G^{(r)}(x,\ y)-A_i^{(r)}(x)B_i^{(r)}(y)+A_i^{(r)}(x)B_i^{'(r)}(y)$$

The modification of the user's authority is completed after previous steps.

4.4. Modification of confidential file: appending file

When the confidential files in the system need to be appended, CA would distribute the access authority to new files to each PHR user and resets the verification indicator J_i as $J_i^{'}$, and the polynomial $B_i^{(r)}(y)$ is also updated as $B_i^{'(r)}(y)$. Finally, we update the public polynomial, as in the succeeding text, to complete the file appending.

$$G^{*(r)}(x,\ y)=\sum_{i=1}^{n}A_i^{(r)}(x)B_i^{'(r)}(y)\wedge x,\ y\in R.$$

4.5. Modification of confidential file: file removal

When the confidential files in the system need to be removed, CA would remove each PHR user's access authority to such files and reset the verification indicator J_i as $J_i^{''}$, and the polynomial $B_i^{(r)}(y)$ is also updated as $B_i^{''(r)}(y)$. Finally, the public polynomial is updated to complete the file removal.

$$G^{**(r)}(x,\ y)=\sum_{i=1}^{n}A_i^{(r)}(x)B_i^{''(r)}(y)\wedge x,\ y\in R.$$

5. SECURITY ANALYSIS

Public health records are the data with high personal privacy, and a cloud system is the tool to store and share data. The security in the sharing is therefore questioned. In this study, public-key cryptography, interpolating polynomial, and access matrix are utilized for accessing data. When the mechanism is placed on the cloud system as the access control mechanism, the symmetric encryption is used to

encrypt the data for protecting the key. The access control is protected with Lagrange operation and the public-key system, where the members must be approved by CA to pass through the access matrix for accessing. Besides, each member has the accessible matrix authority; when they intend to attack or simulate the others' matrices, they would have to crack the access polynomial, solve Lagrange and public-key cryptosystem, and face the decryption of symmetric cryptosystem. The security is achieved as what is spent would be more than the security request.

The past approach mostly established a user's access polynomial, representing that the authorized person with the key to access to encrypted files could apply the key to access confidential files. The access polynomial needs to be recalculated for dynamic update, and the more members would affect the calculation complexity. This study proposes to apply an access matrix to the dynamic update so that the altered calculation is relatively easier. Moreover, access polynomial often encounters the operation security of mathematical equations. However, new parameters are added to the calculation formula with an access matrix such that there is no such a problem.

In this section, the responses to the user or file transaction analyzed the security, and the common attacks (external attack, insider attack, coordinative attack, and equation breaking attack) are examined in the actual conditions to implement the system security. The four attacks proposed in this study are described as following.

5.1. External attack

External attack refers to an attacker attempting to illegally acquire the user's secret key and steal confidential data through the public information in the system.

As the example of this study, an attacker has to work on the sole public decryption polynomial $G^{(r)}(x, y)$ of the system for the external attack. Because each user (S_i) could substitute a personal private key (H_i) for the public decryption polynomial $G^{(r)}(x, y)$ to deduct the decryption key (DK_u) for authorized confidential files, both $A_i^{(r)}(x)$ and $B_i^{(r)}(y)$ have to be broken when attempting to illegally acquire the decryption key. Nonetheless, an external attacker could merely acquire the public decryption polynomial $G^{(r)}(x, y)$ and the number of the confidential file; with inadequate decryption information and the huge computations, the decryption key could not be effectively deducted with mathematical calculations. Even when two users are continuously added, the decryption key would not be acquired because of the mathematical form not being factorized (referring to Section 3.2.3). As a consequence, an illegal attacker cannot acquire a patient's medical records and some medical information through external attack.

5.2. Insider attack

Such an attack is common among system members; it usually occurs when a legal user (S_i) with lower authority utilizes the public decryption polynomial $G^{(r)}(x, y)$ and the personal secret key (H_i) to illegally acquire the secret keys of other legal users with higher authority so as to illegally acquire an unauthorized confidential document.

Based on such situations, it is assumed that a nurse (S_3) intends to access the electrocardiogram ($file_2$) and major surgery records ($file_3$) to which a physician (S_2) could access; Figure 4 shows member authority access matrix.

In general situations, a physician (S_2) and a nurse (S_3) show the partial order relationship, denoted as $S_3 \preccurlyeq S_2$, meaning that physicians have higher access authority ($S_2 = \{1, 2, 3, 4\}$; $S_3 = \{1, 4\}$) than nurses do. For this reason, a nurse (S_3) becomes an attacker for a physician (S_2), who attempts to substitute the personal secret key (H_3) for the public decryption polynomial $G^{(r)}(x, y)$ to deduct the physician's (S_2) secret key (H_2) and further acquire the electrocardiogram ($file_2$) and major surgery records ($file_3$) to which merely the physician (S_2) could access.

In the deduction process, a nurse (S_3) could substitute (H_3, 1) and (H_3, 4) for the public polynomial $G^{(r)}(x, y)$ to acquire the decryption keys DK_1 and DK_4 for the blood pressure records ($file_1$) and the drug and allergic reaction ($file_4$). Nevertheless, the decryption key for the electrocardiogram ($file_2$) and major surgery records ($file_3$) could not be acquired by substituting (H_3, 2) and (H_3, 3) for $G^{(r)}(x, y)$. That is, a nurse (S_3) cannot acquire the decryption keys DK_2 and DK_3 for a physician's (S_2) access.

When a nurse (S_3) intends to acquire the decryption keys DK_2 and DK_3 for the access of a physician (S_2), the attacked targets are hidden in H_2 in $A_2^{(r)}(x)$ and DK_2 and DK_3 hidden in $B_2^{(r)}(y)$. As a nurse (S_3) could acquire the decryption keys DK_1 and DK_4 by substituting (H_3, 1) and (H_3, 4) for $G^{(r)}(x, y)$, the attacker attempts to calculate the following.

$$
\begin{aligned}
&G^{(r)}(H_3,\ 1) = DK_1\\
&\Rightarrow G^{(r)}(H_3,\ 1) - DK_1 = 0\\
&\Rightarrow A_1^{(r)}(H_3)B_1^{(r)}(1) + A_2^{(r)}(H_3)B_2^{(r)}(1)\\
&+\cdots + A_6^{(r)}(H_3)B_6^{(r)}(1) - DK_1 = 0
\end{aligned}
$$

	$file_1(DK_1)$ Blood Pressure Record	$file_2(DK_2)$ Electrocardiogram	$file_3(DK_3)$ Major Surgery Records	$file_4(DK_4)$ Drug and Allergic Reaction	$file_5(DK_5)$ Health Insurance Records
$S_1(H_1)$ Patient	1	1	1	1	1
$S_2(H_2)$ Physician	1	1	1	1	0
$S_3(H_3)$ Nurse	1	0	0	1	0
$S_4(H_4)$ Medical Researcher	1	1	0	1	0
$S_5(H_5)$ Health Insurance Unit	0	0	0	0	1
$S_6(H_6)$ Kinship	1	0	0	1	0

Figure 4. Member authority access matrix.

$$
\begin{aligned}
&G^{(r)}(H_3,\ 4) = DK_4\\
&\Rightarrow G^{(r)}(H_3,\ 4) - DK_4 = 0\\
&\Rightarrow A_1^{(r)}(H_3)B_1^{(r)}(4) + A_2^{(r)}(H_3)B_2^{(r)}(4)\\
&+\cdots + A_6^{(r)}(H_3)B_6^{(r)}(4) - DK_4 = 0
\end{aligned}
$$

According to the previous deduction, the items, except $A_3^{(r)}(H_3)B_3^{(r)}(1)$ and $A_3^{(r)}(H_3)B_3^{(r)}(4)$, are a series of huge numerical values that could not be calculated (referring the calculation process to example 1 in Section 3.3.1) so that the attacker could not analyze H_2 from such numerical values to acquire DK_2 and DK_3.

Assuming that an attacker (S_3) acquires $A_2^{(r)}(x)B_2^{(r)}(y)$, it could not be easily broken as $A_2^{(r)}(x)$ and $B_2^{(r)}(y)$ are protected by individual verification indicators.

(1) An attacker (S_3) intends to acquire H_2-related information hidden in the polynomial $A_2^{(r)}(x)$.

$$
\begin{aligned}
A_2^{(r)}(x) = \Bigg\{ &\left[\frac{x-H_1}{H_2-H_1} + (x-H_2)\right] \times \left[\frac{x-H_3}{H_2-H_3} + (x-H_2)\right]\\
&\times \left[\frac{x-H_4}{H_2-H_4} + (x-H_2)\right] \times \left[\frac{x-H_5}{H_2-H_5} + (x-H_2)\right]\\
&\times \left[\frac{x-H_6}{H_2-H_6} + (x-H_2)\right] \Bigg\} \times I^{(x)}_{\{H_1,\ \cdots,\ H_6\}}
\end{aligned}
$$

The polynomial $A_2^{(r)}(x)$ could verify the user and confirm the secret key H_i being on the CA's legal list. A user not legally authorized by CA could not pass the calculation of the verification indicator $I^{(x)}_{\{H_1,\ \cdots,\ H_n\}}$. Even if the user is legally authorized by CA, the secret key not being confirmed by the owner would not succeed. In other words, assuming that a nurse (S_3) substitutes the personal secret key (H_3) for $A_2^{(r)}(x)$, a series of disordered numerical values would be acquired; being computed with $\Theta_i^{(r)}(x) = I^{\left(A_i^{(r)}(x)\right)}_{\{1\}}$, it appears as 0, presenting the failure in breaking.

(2) An attacker (S_3) intends to acquire DK_2- and DK_3-related information hidden in the polynomial $B_2^{(r)}(y)$.

$$
B_2^{(r)}(y) = \begin{bmatrix}
DK_1 \times \dfrac{(y-2)(y-3)(y-4)(y-5)}{(1-2)(1-3)(1-4)(1-5)}\\
+DK_2 \times \dfrac{(y-1)(y-3)(y-4)(y-5)}{(2-1)(2-3)(2-4)(2-5)}\\
+DK_3 \times \dfrac{(y-1)(y-3)(y-4)(y-5)}{(3-1)(3-2)(3-4)(3-5)}\\
+DK_4 \times \dfrac{(y-1)(y-2)(y-3)(y-5)}{(4-1)(4-2)(4-3)(4-5)}
\end{bmatrix} \times I_{J_2}(y)
$$

The user has to be authorized by CA to legally access the confidential document so as to successfully pass the confirmation with $I_{J_i}(y)$; otherwise, the result appears as 0, revealing not being broken. A nurse ($S_3 = \{1, 4\}$) not in the authority list of CA to access the electrocardiogram ($file_2$) and major surgery record ($file_3$) would not pass the confirmation of $I_{J_2}(y)$ ($J_2 = \{1, 2, 3, 4\}$) to acquire DK_2 and DK_3. The final result appears as 0, showing not successfully acquiring the decryption key.

In sum, the decryption information cannot be illegally acquired by reversely deducting the polynomial. Such a method therefore could effectively stop the attack from insider attacks to achieve the system security.

5.3. Collaborative attack

The difference between coordinative attack and insider attack lies in the quantity of attackers. Insider attackers refer to a legally authorized user attempting to illegally acquire the decryption key, while coordinative attackers are two or more legally authorized users cooperatively using the secret keys to deduct other system members' secret keys and confidential document to which an access attacker could not access.

In the member authority access matrix established by CA, the partial order relationship exists among users; therefore, two possible attacks are taken into account in collaborative attack. One is the partial order relationship between at least two and more conspired attackers and internal members who intend to attack, and the other is no partial order relationship among internal members who intend to attack.

(1) Partial order relationship among at least two and more conspired attackers and internal members who intend to attack:

It is assumed that a nurse (S_3) and a medical researcher (S_4) intend to access major surgery records ($file_3$) to which merely a physician (S_2) could access, and the attackers (S_3 and S_4) do not have any access authority to the major surgery records ($file_3$).

From Figure 5, the attackers' authorities are $S_3 = \{1, 4\}$ and $S_4 = \{1, 2, 4\}$, while the authority of the attacked is

	$file_1(DK_1)$ Blood Pressure Record	$file_2(DK_2)$ Electrocardiogram	$file_3(DK_3)$ Major Surgery Records	$file_4(DK_4)$ Drug and Allergic Reaction	$file_5(DK_5)$ Health Insurance Records
$S_1(H_1)$ Patient	1	1	1	1	1
$S_2(H_2)$ Physician	1	1	1	1	0
$S_3(H_3)$ Nurse	1	0	0	1	0
$S_4(H_4)$ Medical Researcher	1	1	0	1	0
$S_5(H_5)$ Health Insurance Unit	0	0	0	0	1
$S_6(H_6)$ Kinship	1	0	0	1	0

Figure 5. The conspired attackers and the attacked present partial order relationship.

$S_2 = \{1, 2, 3, 4\}$. In other words, the access authority of a physician (S_2) is higher than that of a nurse (S_3) and a medical researcher (S_4). In this case, an attacker intends to attack the physician (S_2) with personal decryption information to acquire the decryption key (DK_3) for major surgery records ($file_3$), where the information related to the decryption key DK_3 is hidden in $A_2^{(r)}(x)B_2^{(r)}(y)$.

$$A_2^{(r)}(x) = \left\{ \left[\frac{x - H_1}{H_2 - H_1} + (x - H_2) \right] \times \left[\frac{x - H_3}{H_2 - H_3} + (x - H_2) \right] \times \left[\frac{x - H_4}{H_2 - H_4} + (x - H_2) \right] \times \left[\frac{x - H_5}{H_2 - H_5} + (x - H_2) \right] \times \left[\frac{x - H_6}{H_2 - H_6} + (x - H_2) \right] \right\} \times I^{(x)}_{\{H_1, \ldots, H_6\}}$$

$$B_2^{(r)}(y) = \begin{bmatrix} DK_1 \times \dfrac{(y-2)(y-3)(y-4)(y-5)}{(1-2)(1-3)(1-4)(1-5)} \\ +DK_2 \times \dfrac{(y-1)(y-3)(y-4)(y-5)}{(2-1)(2-3)(2-4)(2-5)} \\ +DK_3 \times \dfrac{(y-1)(y-3)(y-4)(y-5)}{(3-1)(3-2)(3-4)(3-5)} \\ +DK_4 \times \dfrac{(y-1)(y-2)(y-3)(y-5)}{(4-1)(4-2)(4-3)(4-5)} \end{bmatrix} \times I_{J_2}(y)$$

Nonetheless, a nurse (S_3) and a medical researcher (S_4) merely have the personal secret keys H_3 and H_4, which could not be used for acquiring the desired H_2 with $A_2^{(r)}(x) \setminus$ but a series of disordered and huge numerical values. Eventually, the result appears as 0 because of $\Theta_i^{(r)}(x) = I_{\{1\}}^{\left(A_i^{(r)}(x)\right)}$ so that the result of $A_2^{(r)}(x)B_2^{(r)}(y)$ also appears as 0.

Apparently, conspired attack, similar to a single attacker, could not successfully break the desired decryption information.

(2) No partial order relationship between at least two and more conspired attackers and internal members who intend to attack:

It is assumed that a nurse (S_3) and a medical researcher (S_4) intend to access health insurance records ($file_5$) to which merely a health insurance unit (S_5) can access, and the attackers (S_3 and S_4) do not have any access authorities to the health insurance records ($file_5$).

From Figure 6, the attackers' authorities are $S_3 = \{1, 4\}$ and $S_4 = \{1, 2, 4\}$, and the authority of the attacked is $S_5 = \{5\}$. That is, the access authority of a health insurance unit (S_5) is not related to the nurse (S_3) and the medical researcher (S_4). In this case, attackers attempt to enhance the probability of attacking the health insurance unit (S_5) with the decryption information to acquire the decryption key (DK_5) for the health insurance records ($file_5$), where the information related to the decryption key DK_5 is hidden in $A_5^{(r)}(x)B_5^{(r)}(y)$.

	$file_1(DK_1)$ Blood Pressure Record	$file_2(DK_2)$ Electrocardiogram	$file_3(DK_3)$ Major Surgery Records	$file_4(DK_4)$ Drug and Allergic Reaction	$file_5(DK_5)$ Health Insurance Records
$S_1(H_1)$ Patient	1	1	1	1	1
$S_2(H_2)$ Physician	1	1	1	1	0
$S_3(H_3)$ Nurse	1	0	0	1	0
$S_4(H_4)$ Medical Researcher	1	1	0	1	0
$S_5(H_5)$ Health Insurance Unit	0	0	0	0	1
$S_6(H_6)$ Kinship	1	0	0	1	0

Figure 6. No partial order relationship between conspired attackers and the attacked revealed.

$$A_5^{(r)}(x) = \left\{ \left[\frac{x - H_1}{H_5 - H_1} + (x - H_5) \right] \times \left[\frac{x - H_2}{H_5 - H_2} + (x - H_5) \right] \times \left[\frac{x - H_3}{H_5 - H_3} + (x - H_5) \right] \times \left[\frac{x - H_4}{H_5 - H_4} + (x - H_5) \right] \times \left[\frac{x - H_6}{H_5 - H_6} + (x - H_5) \right] \right\} \times I^{(x)}_{\{H_1, \ldots, H_6\}}$$

$$B_5^{(r)}(y) = \left[DK_5 \times \frac{(y-1)(y-2)(y-3)(y-4)}{(5-1)(5-2)(5-3)(5-4)} \right] \times I_{J_5}(y)$$

Nonetheless, a nurse (S_3) and a medical researcher (S_4) merely have the personal secret keys H_3 and H_4, which could not be used for acquiring H_5 through $A_5^{(r)}(x)$ but a series of disordered and huge numerical values. Eventually, it appears as 0 because of $\Theta_i^{(r)}(x) = I_{\{1\}}^{\left(A_i^{(r)}(x)\right)}$, and the result of $A_5^{(r)}(x)B_5^{(r)}(y)$ also appears as 0.

In conclusion, in the situations of the partial order relationship among system members and the quantity of attackers, an attacker cannot deduct the secret key of the attacked and the decryption key for the confidential document with known decryption information. This method therefore could not achieve the breaking with coordinative attack.

5.4. Equation attack

The fourth attack, equation attack, means that an attacker attempts to break mathematically with the public decryption polynomial $G^{(r)}(x, y)$ to further illegally acquire the secret key.

Such an attack is frequently used during the transaction of a system member's authority. As mentioned in Section 5 , when a system is adding members, removing members, or transacting the member's access authority to confidential document, any attackers could look for feasible breaking opportunities from the transaction of public polynomial. Consequently, the public polynomial security during the authority transaction is discussed in this section. The

transaction types of user authority mentioned in the previous section is further explained.

(1) Adding member: $\overline{G^{(r)}(x,\ y)} = G^{(r)}(x,\ y) + A_{n+1}^{(r)}(x) B_{n+1}^{(r)}(y)$

When a new member is added to the system, any attacker could deduct the original public polynomial $G^{(r)}(x, y)$ with the updated public polynomial $\overline{G^{(r)}(x,\ y)}$ to acquire $A_{n+1}^{(r)}(x)B_{n+1}^{(r)}(y)$. As discussed previously, useful information related to the decryption could not be acquired from $A_{n+1}^{(r)}(x)B_{n+1}^{(r)}(y)$. Moreover, the decryption information still cannot be acquired even though new members are continuously added to the system (referring to Section 3.2.3). As a result, an equation attacker could not break useful decryption information from the member addition.

(2) Member removal: $\overline{\overline{G^{(r)}(x,\ y)}} = G^{(r)}(x,\ y) - A_k^{(r)}(x) B_k^{(r)}(y)$

When a member is removed from the system, any attacker could deduct the original public polynomial $G^{(r)}(x, y)$ with the updated public polynomial $\overline{\overline{G^{(r)}(x,\ y)}}$ to acquire $A_k^{(r)}(x)B_k^{(r)}(y)$, which could not be used for breaking, even though members are continuously removed. Useful information therefore would not be acquired.

(3) Modification of authority: $\widetilde{G^{(r)}(x,\ y)} = G^{(r)}(x,\ y) - A_i^{(r)}(x)B_i^{(r)}(y) + A_i^{(r)}(x)B_i^{'(r)}(y)$

Different from the previous two attacks, the new public polynomial is deducted from the original one for $A_i^{(r)}(x)B_i^{(r)}(y) - A_i^{(r)}(x)B_i^{'(r)}(y)$. Although the results are different, the principle for not being broken is similar; that is, when $x = 0$ or $y = 0$ is assumed, a series of huge numerical values would be acquired. Accordingly, an attacker could not break the relevant decryption information even when working on the transaction of the changing user authority.

Summing up the previous security analysis, the four common attacks could not successfully break the decryption information in this study so that the methods proposed in this study could effectively protect the system from being attacked to successfully achieve system security.

6. CONCLUSION

In the access control mechanism, the process with larger computation appears on dynamic update. Several approaches were used for the past access control mechanism to establish access polynomial, including the operation of participation members with the authority to access to confidential files and keys, where the relationship between participation members is closely related to the authority operation. Ones with large authority could access several files, while the others with small authority could merely access some files. An access matrix is proposed in this study, in which the members are equally authorized. In comparison with other access mechanisms, it is simpler, and the computation is smaller in dynamic update, as the matrix does not consider the relationship between members, but merely the quantity of files, in the operation. Accordingly, the application of access matrix presents the advantage.

Patient referral and attending physician changes appear on dynamic update. In the dynamic update process, the approach proposed by T.S. Chen in 2012 is applied to this study. Nevertheless, as T.S. Chen's approach would appear as calculation weakness on the security in the dynamic update process, new parameters and operations are added to the approach proposed in this study to improve the operation drawbacks and enhance the security. Besides, the established access matrix presents no different authority between members; all legal members have accessible authority but do not know the other members' authority. It therefore could enhance the security in the dynamic update by a avoiding united attack.

Improving T.S. Chen (2012) methodology and consolidating the security, applying PHR to cloud computing environments, and considering different access authorities of each user in the system to confidential files, the methods proposed in this study not only could protect the system members and patients' privacy of personal health records but could also stop the entry of illegal attackers.

So far, many literatures have pointed out the convenience of PHR; however, they are not broadly practiced in medical institutions in Taiwan. Many medical clinics still use traditional paper-based patient records to keep patients' medical records, which is considered as the waste of cost. The possible factors in not being practiced are summarized as in the succeeding text.

(1) Capital problem: Large hospitals present adequate capitals to establish platforms, but small clinics could not so they still remain at the stage of traditional paper-based patient records.
(2) Platform establishment problem: Current platforms for PHR have not been uniformed so that the transformation among platforms might result in confidential data lost or error.
(3) Regulation problem: Regulations related to PHR have not been made in Taiwan. It not only involves legislation but also relates to national public health policies that the promotion is rather difficult.

Once PHR could be actually practiced in various medical institutions, and the secure, effective, and reliable encryption is constructed to prevent the cloud computing from the threat of uncertainty as well as to guarantee each user's information security and privacy, the public welfare would be promoted.

REFERENCES

1. Seung LP, Anil VP, Pantanowitz L. Electronic medical records, *Practical Informatics for Cytopathology* 2014; **14**: 121–127.
2. Corrigan JM, Donaldson MS, Kohn LT. *Crossing the Quality Chasm: A New Health System for the 21st Century*. National Academy Press: Washington, DC, 2001.
3. Li M, Yu S, Ren K, Lou W. Securing personal health records in cloud computing: patient-centric and fine-grained data access control in multi-owner settings, *Security and Privacy in Communication Networks* 2010; **50**: 89–106.
4. Mell P, Grance T. *Effectively and Securely Using the Cloud Computing Paradigm*, National Institute of Standards and Technology, 2009.
5. Safran C, Goldberg H. Electronic patient records and the impact of the internet, *International Journal of Medical Informatics* 2000; **60**(2): 77–83.
6. Wang NY. Computer-based patient record system, *The Journal of Taiwan Association for Medical informatics* 1994; **3**: 29–33.
7. Fan BY. Health information management, Taipei: Ho-Chi Book Publishing Co, 2008.
8. Dimitropoulos LL. Privacy and security solutions for interoperable health information exchange, http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_241358_0_0_18/IAVR_ExecSumm.pdf, 2006.
9. Ray P, Wimalasiri J. The need for technical solutions for maintaining the privacy of EHR, *Engineering in Medicine and Biology Society* 2006; **1**: 4686–4689.
10. Becker MY, Sewell P. Cassandra: flexible trust management, applied to electronic health records, Proceedings of the 17th IEEE Computer Security Foundations Workshop, 2004.
11. Jin J, Ahn GJ, Hu H, Covington MJ, Zhang X. Patient-centric authorization framework for sharing electronic health records, Proceedings of the 14th ACM Symposium on Access Control Models and Technologies SACMAT 09, 125–134, 2009.
12. Waegemann CP, Status report 2002: electronic health records: Medical Records Institute; 2002.
13. Ministry of Health and Welfare in Taiwan. Electronic medical records adoption in hospital, http://www.mohw.gov.tw/CHT/Ministry/, 2005.
14. Ministry of Health and Welfare in Taiwan. The plan of internet healthy service promotion. http://www.mohw.gov.tw/CHT/Ministry/, 2015.
15. Kahn JS, Aulakh V, Boswort A. What it takes: characteristics of the ideal personal health record, *Health Affairs* (Millwood) 2009; **28**(2): 369–376.
16. Iakovidis I. Towards personal health record: current situation, obstacles and trends in implementation of electronic healthcare record in Europe, *International Journal of Medical Informatics* 1998; **52**(1): 105–115.
17. Lober WB, Zierler B, Herbaugh A, Shinstrom SE, Stolyar A, Kim EH, Kim Y, Barriers to the use of a personal health record by an elderly population 2006; 514–518.
18. Smith III JO. Lagrange interpolation, center for computer research in music and acoustics (CCRMA), Stanford University.
19. Deshpande JV. On continuity of a partial order, *Proceedings of the American Mathematical Society* 1968; **19**(2): 383–386.
20. Chen TS, Liu CH, Chen TL, Chen CS, Bau JS. Secure dynamic access control scheme of PHR in cloud computing, *Journal of Medical Systems* 2012; **36**(6): 4005–4020.
21. Cheng JS. An application of public key cryptosystem on personal health records, National Chiayi University Department of Applied Mathematics 2014; **1–30**.