東海大學資訊管理研究所

碩士學位論文

基於個人健康紀錄的雲端健康照護服務之存取控制

Design of Secure Access Control Scheme for PHR-Based Cloud Healthcare Service

指導教授：陳澤雄 博士

劉嘉惠 博士

研 究 生：林峰祺 撰

中華民國 102 年 6 月

東海大學資訊管理學系碩士學位

考試委員審定書

資訊管理學系研究所 林峰祺 君所提之論文

基於個人健康紀錄的雲端健康照護服務之存取控制

經本考試委員會審查，符合碩士資格標準。

學位考試委員會 召集人：賴冰麗 (簽章)

委 員：鐘玉芳

劉嘉惠

陳文智

陳澤雄

中 華 民 國 102 年 6 月 1 日

誌　　謝

首先誠摯地感謝指導教授陳澤雄博士及劉嘉惠博士兩位老師悉心的教導，並且關心我的學業與生活，您們的提攜與栽培，使我在這兩年中獲益匪淺，能當您的學生，真的很幸福。峰祺在此感謝您！

峰祺能夠完成東海大學資訊管理研究所的碩士學位，乃是家人與朋友的一路扶持，感謝志賢老師、澤龍學長適時給予解惑，因您們傾囊相授，讓我在資訊安全領域，有更深入的認識。感謝偉琦學姊，您是我心靈的導師，在我困頓與迷惑的時候，給予我最溫暖的支持；感謝學弟耀民、培鑫、維勝、坤昊、富勝，在我緊急需要協助的時候給予我幫助，還有一起奮鬥的好夥伴健貿、智銘、郁婷、恩平，在我寫論文的過程中，一起在無數的會議中互相鼓勵與成長。也感謝東海資管所的全體同學彼此交流與切磋，你們都是峰祺生命中的天使，因為你們支持，使得我的論文能夠如期完成。

最後，要感謝我最親愛的家人，感謝您們這些年來辛苦的扶育我栽培長大，有你們的諄諄教誨的包容與支持，我才能順利完成學業，僅把這份喜悅與榮耀與您們分享。

林峰祺 謹誌

中華民國 102 年 6 月 01 日

論文名稱：基於個人健康紀錄的雲端健康照護服務之存取控制

校所名稱：東海大學資訊管理學系研究所

畢業時間：2013 年 06 月

研究生：林峰祺　　**指導教授**：陳澤雄 博士

論文摘要：

隨著資訊科技與醫療技術的發展，許多先進國家為了因應時代的改變以及資訊的應用，紛紛成立相關組織制訂電子病歷標準，然而隨著高齡化社會的來臨，老年人健康照護的興起，逐漸發展出新興型態的個人健康紀錄。個人健康紀錄可以整合不同來源的個人健康紀錄，利用網際網路或可攜式媒體，提供完整且正確的個人健康與醫療歷史摘要。透過個人健康紀錄的推動與實施，可以提高健康照護的品質，提供病人完整的連續性照護，並增加健康照護上的效率與促進個人健康。

而將個人健康紀錄系統實作在雲端運算環境下，可以降低基礎建設管理成本，並可視用戶端需求變化的狀況，即時進行資源動態調整等優點。但同時也帶來了新的挑戰，在雲端環境裡資訊安全性的確保對使用者來說是相當重要，因此，本論文提出有效且安全的存取管理機制解決個人健康紀錄系統實作在雲端環境中的安全性問題，避免可能因雲端中的資訊遭受安全性威脅，而造成的醫療照護中斷、病患資料被竊、個人隱私資訊或是財務損失等嚴重後果。

本論文提出以雙線性函數建構於雲端環境下新的個人健康紀錄存取控制機制，適合佈署大規模且具多使用者的個人健康紀錄系統，提供使用者安全且有效率的動態存取個人健康紀錄的機制。從研究結果得知，透過本研究建構的存取控制機制可以於雲端計算環境中有效抵擋方程式工程、外部攻擊、協同攻擊、內部攻擊。

關鍵詞：個人健康紀錄、雲端運算、存取控制、金鑰管理、雙線性配對

Title of Thesis: Design of Secure Access Control Scheme for PHR-Based Cloud Healthcare Service

Name of Institute: Tunghai University, Institute of Information Management

Graduation Time: 06/2013

Student Name: Fong-Ci Lin **Advisor Name**: Dr. Tzer-Shyong Chen

Dr. Chia-Hui Liu

Abstract:

With development of information technology and medical technology, many developed countries have been established organizations to develop electronic medical standards in response to apply the development of technology information and the changes of new generation, and they gradually develop the emerging patterns of personal health records "Personal Health Records (PHR)". PHR can integrate different kind of health information, with the Internet or portable devices, and offer the integrity and accuracy personal health and medical records. Through electronic medical records, we can evaluate the quality of health care, provide continuously care to patients, promote the medical efficiency and increase the accuracy of medical diagnosis.

Using the cloud computing environment to implement the PHR system; we can decrease the infrastructure management costs, adjust the dynamic resources immediately based on the changes of client's demand and other advantages. But it also brings a new challenge, to assure the security information in cloud computing environment is important to users, so this thesis provides efficient and safe access managing mechanism to solve PHR implement on cloud environment's security problem, avoiding possibility that the information security being threatened in the Cloud may lead to the collapse of medical care, patients' data stolen, loss of personal privacy and financial or other serious consequences.

This thesis presents Bilinear Pairing which constructed in the cloud computing environment of the new PHR access control mechanism which suited for deploying a large-scale and multiple identities of users, and users are safe and efficient in accessing the PHR information. As a result from the research, Access control scheme which implemented on cloud computing environments can be effectively resist equation attack, external attack, collaborative attack, and internal attack.

Keywords: Personal Health Records, Cloud Computing, Access Control, Key Management, Bilinear Pairing

Contents

List of Figures

List of Table

Chapter 1 – Introduction

1.1 Research Background

The popularity of computers and networks have promoted the implementation of the electronic medical records. In the past, hospitals used EMR (Electronic Medical Records) system, which includes past, present or future physical and mental patient status records, electronic digital format record of the patient status and check the test results, to replace the medical paper records, the main purpose is to assist the medical or related services to provide information to healthcare professionals in clinical use. After importing the EMR system to the hospital, the paper medical records will be replaced by electronic medical records, and providing the additional benefits that cannot be achieved by paper medical records. Such as to solve the problem of paper medical records storage and transmission, and directly through the EMR tracking, medical records can be well managed, not only to improve the medical administrative efficiency, but also reduce human error. However, the EMR system is LAN-based systems, the scope of application of the electronic case is still emphasis on electronic medical records management and data transfer, only part of the electronic medical record can exchange between medical institutions. Sharing between information is greatly restricted, real-time monitoring and quick response are difficult to meet the needs of the modern medical development. But this is from the point of view of the medical information providers who operates, manages, and non-patient-centered. The only source of patient's medical information is doctors, the patients does not have authority to edit the data so that the patient can not immediately grasp their own health status, which in the future can lead to insufficient medical information for patient's disease.

The aging society is now a feature of the evolution of the advanced countries family. [1]According to the World Health Organization (WHO), a national population over the age of 65 is more than 7%, on behalf of that country is the "aging society"; while the ratio is more than 14%, then it enters the "old-age society"; up to 21% or more, it can be referred to as "super-aged society". Many developed countries such as Japan, the total number of elderly whose age is over 65 is 21.2%, has reached super-aged society standards (March 2007), other countries such as Germany and Italy, the elderly population has reached old-aged society standards.

However, old-aged society also caused a rapid increase in the phenomenon of chronic disease cases, the demand of people to manage their health and prevent disease has increased, many medical services began to develop a patient-centered system. M. Li, S.Yu, et al. [2] proposed a patient-centered personal health information (Personal Health Record, PHR) switching architecture, PHR integration of medical records came from various medical institutions, such as drug use, allergies record, health insurance, patients can access and manage their health information. For example, patients with active role initiate the request of care, health care workers in the passive role based on requests do respond and provide services, so the patient will be more easy to grasp their own health status, to increase the interaction between doctors, and reduce the repeat testing and treatment medical costs, thus achieve more integrated continuity of remote care services. Therefore PHR got much national attention.

Such as [3] the U.S. Secretary of Health and Human Services, the National Coordinator for Health Information Technology, and the Administrator of the Centers for Medicare and Medicaid Services (CMS) have all identified PHRs as a top priority.

1.2 Research Motivations

Cloud computing can be distributed networks, servers, operating systems, storage,

applications etc. IT resources, through centralization, virtualization, forming a unified management of the resource pool, IT units can immediately service the clients based on their needs. Cloud computing has a cross-platform and the advantages are saving space, saving energy and reduce the budget. PHR implement on cloud computing environment can achieve a variety of flexible services to adjust according to the required computing power and storage space. The concept of sharing resources and services, besides it can significantly reduce the cost of IT investment, it also increases its overall efficiency, enhances system stability, and it can improve the previous level of service of the IT unit, enhances the hospital's service flexibility and hospital services. The MarketsandMarkets forecast report [4] pointed out that the Health IT running on the cloud will bring huge growth market revenue will grow to $ 5.4 billion in health care by 2017, users from 4% increased to 20.5%. More and more PHR providers are willing to transfer the application services and data storage to the cloud, such as Microsoft, IBM, SAP also had the PHR System on the cloud services.

The PHR System implemented on cloud computing environment can reduce infrastructure management costs, and can service the clients based on their demands, real time adjustment services, but it also brought new challenges, ensuring the information security is very important to users on cloud computing environment, therefore, we propose effective and secure access control mechanisms to solve the security issues of the PHR implement on cloud computing environment. To avoid the possibility of suffering security threat, this would lead to interruption, stolen data, privacy information, or financial loss and other serious consequences.

1.3 Research Objectives

PHR files stored in the cloud server, patients will be unable to control the medical information. Cloud computing has many security threats and behaviors such as illegal

access, internal staff malicious behavior, private information is stolen. We cannot fully ensure that the PHR service provider is safe and can be trusted. PHRs should be guarded through ownership controlled encryption, enabling secure storage, transmission, and access. The access and sharing of PHRs should provide end-to-end source verification through signatures and certification process against blind subpoena and unauthorized change in healthcare critical data content and user agreements.

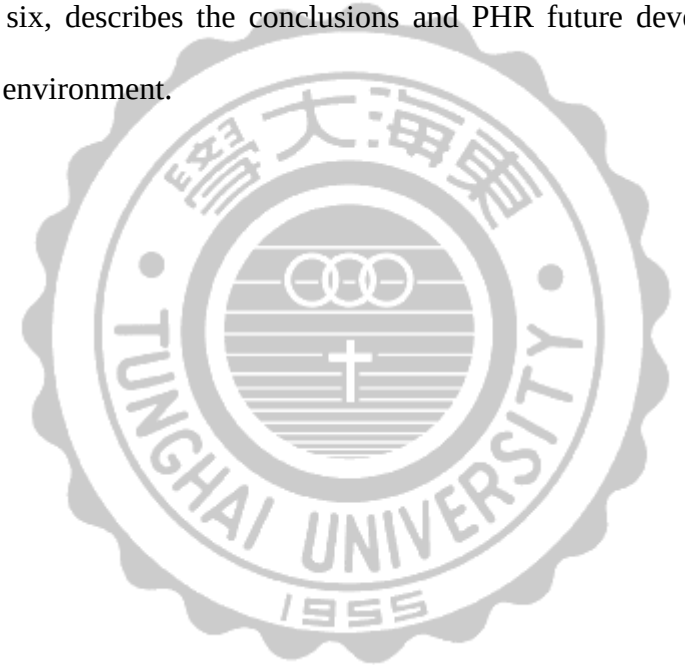
While building the "patient-centered" PHR system, we hope that when the legitimate user logged into the system, he will be able to manage their owned information. Especially the transfer of personal health information in the network, he can decide whether to allow other people to access the information. This can be reached through the authority, and PHR system will follow authentication scheme to ensure that the legitimate user access, and protect ownership of information, does not allow unauthorized access. Although an encryption scheme can ensure the confidentiality within PHRs, We still should strengthen the legitimate users when using the system, due to accidentally or maliciously operation which would lead to a confidential record to other illegal parties.

In this thesis, we propose a user identity-based cryptosystems in dynamic access architecture. In order to ensure that each patient self-management and share their medical records, we have designed a patient-centered access mechanism, patients can immediately add, revoke the user access privileges, and update the PHR record. And it offers multi-user access, reduce the complexity of key management solutions on the cloud environment.

1.4 Research Findings

This thesis is divided into six chapters: the first chapter is to study the background and motivation research purposes and the introduction of the paper structure. The

second chapter is the introduction of the research, including the introduction of the personal health record (PHR), cloud computing medical services, cryptography and Identity-Based Cryptography. Then enter the core of this thesis, this thesis uses Bilinear generate derivation key, which described in Chapter three, how to obtain PHR access on cloud computing environment, and the use of examples to illustrate the operation of the process of the function. Chapter four describes the PHR dynamic access control on cloud computing environment. And in the fifth chapter, the analysis of safety operation, lists four attacks, the safety authentication method. The final chapter, Chapter six, describes the conclusions and PHR future development on the cloud computing environment.



Chapter 2 – Literature Review

2.1 Personal Health Records

Because of Advances in information and communications technology, electrical health records become a trend around worldwide, however the traditional medical records of EMR mainly provide information for the professional nurses in clinical medical use, not the health care and manage on patients' view. Due to the higher percentage of self-consciousness and participation on patients, the concept of PHR continually defined. Now, we don't have pervasive definition of electrical health records. As defined by the National Alliance for Health Information Technology in a report to the National Coordinator for Health Information Technology (NCHIT), "a PHR is an individual's electronic record of health-related information that conforms to nationally recognized interoperability standards and that can be drawn from multiple sources while being managed, shared and controlled by the individual." [5].

American Health Information Management Association (AHIMA) considers the personal health record should be developed under protection. Defined PHR in their report on the subject as: "The personal health record (PHR) is an electronic, lifelong resource of health information needed by individuals to make health decisions. Individuals own and manage the information in the PHR, which comes from healthcare providers and the individual. The PHR is maintained in a secure and private environment, with the individual determining rights of access. The PHR does not replace the legal record of any provider." [6].

The Markle Foundation's Connecting for Health Collaborative, a public-private endeavor working toward an interoperable health information infrastructures defined

PHR in their report on the subject as: "An electronic application through which individuals can access, manage and share their health information, and that of others for whom they are authorized, in a private, secure, and confidential environment."[3].

The purpose of PHR is to help people understand their health information and the way of managing their health for a lifetime. The value of PHR is accumulative long-term health records, improving personal health and enough information reference for nurses to fight for the coming diseases. Most standalone PHRs provide basic tools that help people collect, organize and store their health information [7]. These include medical history, medical and emergency contacts, outpatient and hospital visits, immunization tracking, insurance records, and health-related alerts and reminders. More advanced PHRs (particularly those with digitally-networked services) offer additional functions [8]:

1. Accessing medical records with capacity to offer amendments to add information (such as alternative treatments being pursued by the patient), or correct errors or incomplete information.
2. Adding information of primary interest to patients rather than providers, such as patient-relevant decision support.
3. Drug interaction checking (when a complete medication profile is available)
4. Home monitoring with recording or tele-reporting of data to the record.
5. Interactive health risk profiling and patient education resources.
6. Patient-physician secure e-mail.
7. Prevention and wellness reminders.
8. Processing of claims and payment.
9. Refilling of prescriptions.
10. Retrieving of laboratory and other tests.
11. Reviewing of insurance eligibility and benefits.

12. Scheduling appointments.

In summary, we know PHR is the health record switch model focus on patients which they manage on their own. An ideal PHR can integrate different personal health information; we use Internet or portable flash drive to transfer different medical records, also provide precise personal health record and medical records under the privacy and safety situation. PHR bring advantages like improving medical service and continually corporate with medical care service, therefore, professional nurses can check patients' medical information at the right moment so that we can decrease duplicated examination and cure on the cost.

2.2 Health Care Services and Cloud Computing

2.2.1 Introduction to Cloud Computing

According to National Institute of Standards and Technology (NIST), Information Technology Laboratory [9], the definition of cloud computing include three services, four models and five characters. As figure 1.

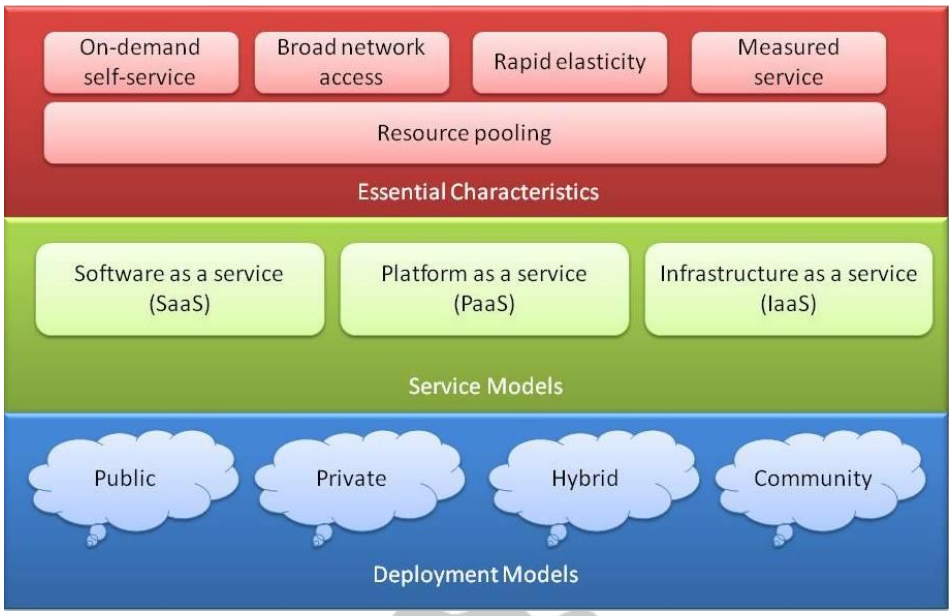


Figure 1: NIST Visual Model of Cloud Computing Definition

Cloud service delivery is divided among three archetypal models and various derivative combinations, respectively — defined thus:

1. *Infrastructure as a Services (IaaS):* Consumers with "infrastructure" such as storage space, network components and computing power. They can control storage space and network components (such as firewall and Load balancer, etc.), but they actually do not control cloud infrastructure. In other words, suppliers can provide the computing power and data storage space on clients' demand and then charging.
2. *Platform as a Service (PaaS):* Consumers use the host to operate application; they usually have a little authority on the host, but not on the operating system, hardware and the operation of the network infrastructure. Platform offers the infrastructure of the application, users can arrange their applications or writing code directly, they do not need to manage or control the cloud equipment themselves.
3. *Software as a Service (SaaS):* Consumers operate application; they do not control the operating system, hardware or the operation of the network infrastructure. It is

kind of a web-based software service mode, clients can regard their actual demand through the Internet to find the service mode and pay to manufacture on what they ordered and how long it took, and we do not need to the update the software, the manufacture will do it for you.

There are four deployment models for cloud services, with derivative variations that address specific requirements:

1. *Public Cloud:* Public cloud services are free for customers through the Internet or a third-party, but the public cloud does not mean that users' information is available for anyone. Public cloud providers usually take access control mechanisms on users.
2. *Private Cloud:* Data and programs on private cloud services are manage through organization. Unlike public cloud services, private cloud services don't influenced by network bandwidth, security concerns and regulations; besides that, private cloud services providers and users are more likely to understand the cloud infrastructure and improving security and flexibility problems.
3. *Community Cloud:* Community cloud operated by many similar organizations, such as the specific security requirements, common purposes and so on. Members share cloud data and application.
4. *Hybrid Cloud:* Hybrid cloud combined private cloud and public cloud; users usually do non business-critical information outsourcing and deal with them in the public cloud so that they can control business-critical services and information at the same time.

Cloud services exhibit five essential characteristics that demonstrate their relation to, and differences from, traditional computing approaches:

1. *On-demand self-service:* Clients can get computing resources on their need (such

as server or storage space), and the entire process is one-sided automation without interaction with resource providers.

2. *Broad network access:* Service is provided by the Internet and there is a standard mechanisms to clients widely use (such as smart phones and laptop).
3. *Resource pooling:* Services provide computing resources, such as storage space, network bandwidth, computing power, virtual machines and et cetera, which compare to a large pool that can redistribute to multiple users in different platforms anytime.
4. *Rapid elasticity:* Computing resources can not only provide fast and flexible to clients and the resources are inexhaustible and easily purchase.
5. *Measured service:* Both providers and users can oversee resource usage transparently.
6. In summary, cloud computing services provide management of software, hardware and maintenance. Users only need to care about what kind of service they desire and do not need to realize the principle and achievement. Cloud computing provides strong Distributed computing power, flexibility and variety of services base on computing power and storage to do adjustment.

Users save hardware maintenance, software maintenance and upgrade costs and even cloud services providers can handle the System Fault Tolerance, multi-tasking, data backup and more professional problems.

2.2.2 Cloud Computing Application in Health Care Services

Cloud computing provides a strong distributed computing power, flexibility, and a variety of services base on computing power and storage to do adjustment. The combinations of cloud computing and medical care service bring new possibilities,

such as easy and ubiquitous access to Personal Health Record, and opportunities for new business models. Personal health records have been positioned as a tool to empower consumers to play a larger and more active role in wellness and self-care. Microsoft HealthVault and ICW Life Sensor use personal health record as medical application in industry. In these systems patients store their own health-related data on certain web servers.

Recently, it becomes more common to use cloud technology in medical care industry, Carlos and others [10] propose a system to automate the process of collecting patient's vital data via a network of sensors connected to legacy medical devices, and deliver this information to the medical center's "cloud" for storage, processing, and distribution.

With information and communication technology, it automatically get patients' physiological data and doctors can realize their health condition though remote monitoring. For chronic disease patients and old people with disabilities in remote areas, especially patients who need long-term care, they do not need to hospitalize and go to the hospital frequency. Doctors master patients' health record with remote medical care system uploading PHR to the Cloud not only re-integrate medical resources but greatly decrease the medical expenditures.

The U.S. military hospital set telephone-based computer system for chronic patients; they monitor Blood sugar, blood pressure, heart rate, electrocardiogram and other physiological data at home, what more, nurses can read data with personal health record via the Internet, if there is anything unusual, we will give them medical support on telephone or video. These result in 85% cutting down in the days of hospital, 26% lower calling for emergency, meanwhile, the visits of nurses also decrease 21%, although only 47 patients take experiment, it sure save 200 million dollars in medical costs a year[11].

When doctors diagnose chronic diseases, they can check long-term and continuously personal health record as reference. Besides accuracy on medical treatment, patients can manage their personal health more proactive even through the history of personal health record to find unusual physiological conditions earlier; this is a concept of prevention than medication. More ever, we can call for collaboration with neighbor medical institutions at the time physiological problems coming out in the Cloud. Doing Health analysis and feedback through Cloud computing we can provide Prevention, medical, rehabilitation and follow-up services, which not only lower health care costs, but improving the quality of medical care.

Doan and other experts [12] propose a Mobile Cloud for Assistive Healthcare infrastructure. They make use of Cloud computing such as user easy access, elasticity of resources demands, scalability of infrastructure, and metered usage and accounting of resources on healthcare systems. Download patients' data with smart phone from Cloud bring lots of advantages, for example, when the context-aware module detects serious anomalous behave that may affect the life of patients, sensible decision must be made that may compromise the patient's privacy as a nurse or a doctor requires immediately authority to access the "private" data to provide appropriate emergency response. [13] Emergency access to health information has long been held out as a pivotal expectation of personal health records by patients and clinicians.

However, medical care service on the Cloud also bears new risks and raise challenges with respect to security and privacy aspects. Access control of data should be flexible and fine grained depending on the dynamic nature of the health care system as multiple entities will interact with the data. Access rights to resources must be granted to users only for the amount of time that is necessary. [14], according to some researches [15], we abstract threats that PHR now facing under the development as follow:

1. Abuse and Nefarious Use of Cloud Computing
2. Insecure Interface and APIs
3. Malicious Insiders
4. Shared Technology Issues
5. Data Loss or Leakage
6. Account or Service Hijacking
7. Unknown Risk Profile

Base on the Cloud's security reasons, we think we should take reliable encryption mechanisms and appropriate access control system to protect user's privacy. When establishing PHR system which "centered on patients", we hope legitimate users are able to manage their own information. Especially personal health record on the Internet, he or she can make decision whether allow others to access or not. So our purpose is to provide effective and safe access mechanisms to solve security problems with PHR implement on cloud Environment. So we can prevent threats on information security that cause interruption of medical care, patients' information be stolen, loss of personal privacy information or financial loss and other serious consequences.

2.3 Cryptography and Encryption Systems

Cryptography is mainly used to protect secret communications, the message through some special methods in order to make the message difficult to interpret, such as mathematic. So that others cannot read the contents of the message. With encryption, the message will from proclamation into ciphertext to protect important message, and someone who has ciphertext can use decryption to reverse it, others who lacks of interceptors or eavesdroppers cannot read it. Cryptography steps up computer science, especially the technology use in computer and network security, like access control and

confidentiality of the information. Cryptography has already widely used in daily life: including bank account identity, entrance security system, electronic commerce and so on. This information not only has personal information in our life, but important trade secrets. Therefore, we need a safe access control mechanisms to store PHR data in the Cloud that each patient's medical record can be encrypted, and ensure the data be stored safely in the Cloud server.

2.3.1 Identity-Based Cryptography

In the traditional public key cryptosystem, it is mainly based on the certificate issued by certificate authority (CA) as to verify the user's identity. In accordance with each user’s identity and public key, CA issues verifiable identity certificate. Other users can via this certificate to confirm the identity of users and its corresponding relationship of public key. Since all user authentication and management key must be centrally managed through the CA, it must spend a large amount of computing time and storage space for issuance as well as custody of certificate, which are serious shortcomings of the traditional public key cryptosystem.

In order to improve the shortcomings of traditional public key cryptosystem, Shamir [16] proposed the concept of identity-based cryptography in 1984 for the first time. In the identity-based cryptography, the public key of users can directly use the sole and representative information of users that is personal information, such as identity card number, E-mail, etc., as the user's public key. The private key of user is generated through the private key generator which is responsible for generating its corresponding private key according to identification code. Based on simple and straightforward design concept, it’s not necessary for other users to additionally verify the relationship between the public key and the user that they can directly use. But this

system has not been an efficient decryption method so it's not widely used by the general public.

In 1985, Koblitz and Miller [17] sequentially proposed to build the password system through the discrete logarithm of elliptic curves. Elliptic curve cryptography system has the advantages of shorter key length, so it is suitable for use in resource-limited mobile devices, conducting the work of added decryption or signature verification. However, in 1993, Menezes, Okamoto, and Vanstone [18] when the three scholars were analyzing the computing features of Weil Pairing function by mathematics, they found that the discrete logarithm problem on the elliptic curve or hyperelliptic curve can be summarized as a discrete logarithm problem which is on finite field of multiplication group that is discrete logarithm problem already converts to the discrete logarithm problem on generally known finite field. This also means that to solve the discrete logarithm problem in finite field is relatively easy and using the password system designed by some specific elliptic curve is not safe, that is so called MOV attack. But owing to this finding, the pairing-based cryptosystem had flourishing development subsequently. Until 2001, Boneh and Franklin [19] jointly proposed identity-based encryption system which is secure and efficient, using the identity code as recognizable base. They use the bilinear pairing (Weil and Tate pairing) on the super singular elliptic curve as the operation base, prompting an ID password system to have rapid development of application.

2.3.2 Bilinear Pairing

Bilinear pairing means the corresponding bilinear map relationship between two cyclic groups. Since the set formed by all points on the elliptic curve will form the relationship of group in algebraic geometry, therefore the operation of bilinear pairing

function just can apply to the operation of elliptic curve. Weil and Tate pairing associated with supersingular elliptic curves or abelian varieties can be modified to create such bilinear map. Bilinear has the following features:

Let G_1 is an additive cyclic group. Its order is a prime number q. Let G_2 is a multiplicative cyclic group. Its order is q. The bilinear map $\hat{e}: G_1 \times G_1 \rightarrow G_2$ has the following properties:

1. Bilinear: let $P, Q, R \in G_1$, thus

   $\hat{e}(P+Q, R)=\hat{e}(P, R)\bullet\hat{e}(Q, R)$

   $\hat{e}(P, Q+R)=\hat{e}(P, Q)\bullet\hat{e}(P, R)$

   $\hat{e}(aP, bQ)=\hat{e}(bP, aQ)=\hat{e}(P, Q)^{ab}$, where a and $b \in Z_q^*$
2. Non-degeneracy: $P \in G_1 \Rightarrow \hat{e}(P,P) \neq 1$
3. Computable: if $P, Q \in G_1 \Rightarrow \hat{e}(P, Q)$ can be computed within polynomial time.

A bilinear map satisfying the three properties above is said to be an admissible bilinear map.

The following is the basic algorithm of identity-based encryption based on Bilinear pairing:

Setup: Given a security parameter $k \in z^+$, the algorithm works as follows:

Step1: Run g on input k to generate a prime q, *two group* G_1, G_2 *of order* q, and an admissible bilinear map $\hat{e}: G_1 \times G_1 \rightarrow G_2$. Choose a random generator $P \in G_1$.

Step2: Pick a random $s \in Z_q^*$ and set $P_{pub} = sP$.

Step3: Choose a cryptographic hash function $H_1: \{0,1\}^* \rightarrow G_1$.Choose a cryptographic hash $H_2 : G_2 \rightarrow \{0,1\}^n$ for some n. The security analysis will view H_1, H_2 as random oracles.

The message space is $M = \{0,1\}^n$. The ciphertext space is $C = G_1^* \times \{0,1\}^n$. The system parameters are params = $(q, G_1, G_2, \hat{e}, n, P, P_{pub}, H_1, H_2)$ The master-key is $s \in Z_q^*$.

Extract:

For a given string ID $\in\{0,1\}^*$ the algorithm does: (1) computes $Q_{ID} = H_1(ID) \in G_1^*$, and (2) sets the private key d_{ID} to be $d_{\mathrm{ID}} = sQ_{ID}$ where s is the master key.

Encrypt:

To encrypt $M \in M$ under the public key ID do the following: (1) compute $Q_{ID} = H_1(ID) \in G_1^*$ (2) choose a random $r \in Z_q^*$, and (3) set the ciphertext to be $C = (rP, M \oplus H_2(g_{\mathrm{ID}}^{r}))$ where $g_{ID} = \hat{e}(Q_{ID}; P_{pub}) \in G_2^*$

Decrypt:

Let $C = (U,V) \in C$ be a ciphertext encrypted using the public key ID. To decrypt C using the private key $d_{ID} \in G_1^*$ compute:

$$V \oplus H_2(\hat{e}(d_{ID}, U)) = M$$

Chapter 3 – Proposed Scheme

This thesis presents a safe and efficient access mechanism on cloud computing environment, also a patient-centered, patient self-management, access or share the Personal Health Record. PHR is not only for medical records. It included food, clothing, housing, behavior, and education, daily activities can be documented and be applied. The different sources of PHR integration of patient health information, including the record of the patient's own measurements (blood pressure, diet, exercise habits, etc.), clinic physician records (patient allergic reactions, EMR), hospital records (ECG medical advice, etc.), health records, drug research center.

On Cloud computing environment, the use of health care PHR will bring many advantages, besides we can use the cloud computing service to do a cross-platform, space-saving, energy-saving, reduce the budget, and according to the required computing power, flexible adjustment storage space, also patients can record their own physiological records through the cloud computing, active role interactions with the medical staff. Also the personal health history can be beneficial to the doctors in judging the basis of chronic diseases and improve the assistance of healthcare in a long distance term. Especially when emergency conditions occur, under the agreements of the person who is being cared, the medical staff can immediately access the information on the cloud computing to increase the medical services response.

In PHRs, personal medical records may come from different medical units, and the content of the message contains the physical information, medical report, drug records, and there are patients, physicians, health care professionals, medical research institutions etc. and other multi-user, with different permission to access the individual authorized file. The PHR dynamic access mechanism involves multiple users, and complex access control mechanisms need to ensure real-time updates and

completeness of the information and verify the true identity of the user to ensure that the user transfers information in safety and reliable conditions. This thesis presents the PHR which can be more efficient on the cloud computing server in providing a large number of multi-user access control mechanisms such as shown in Figure 2.

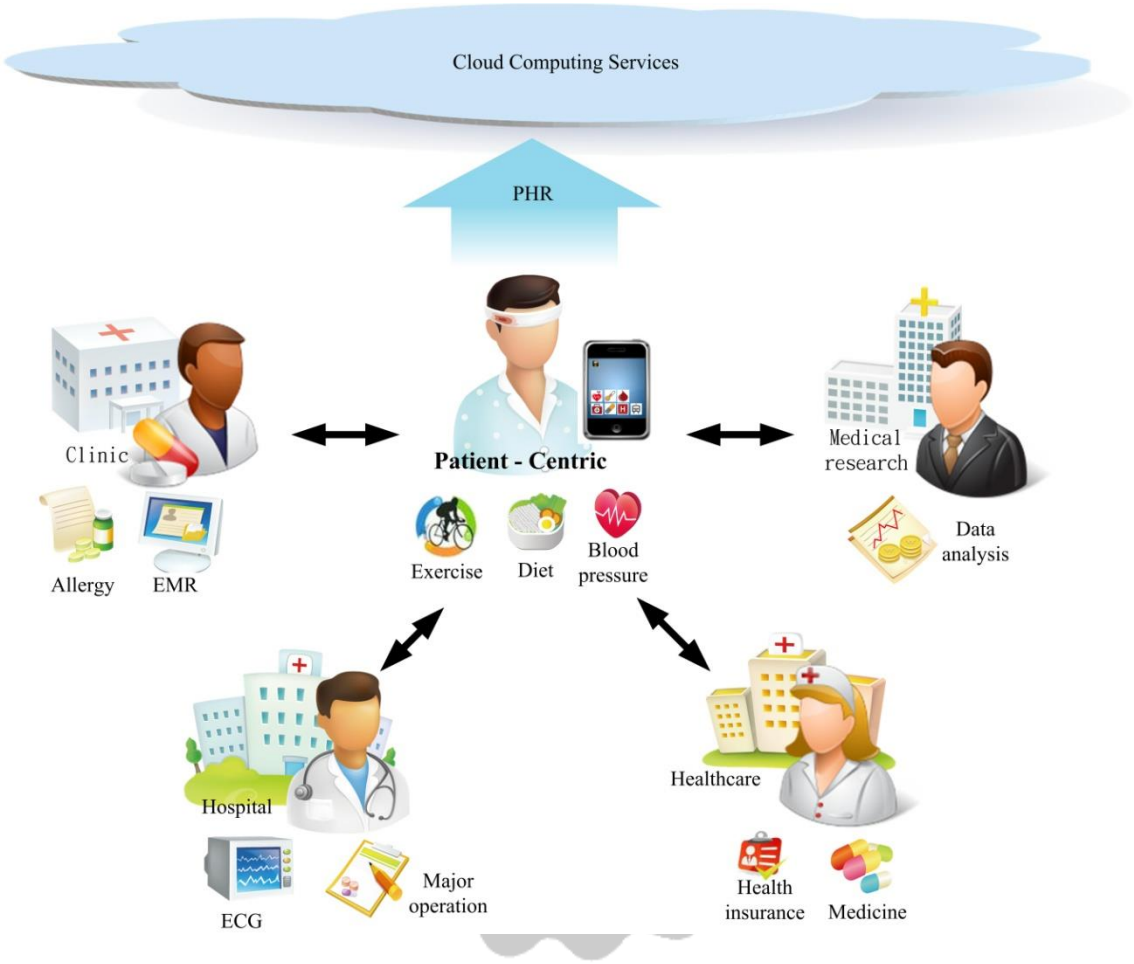


Figure 2: PHR Services in Cloud Environment

In this research, we use identity-based cryptographic system as the system design of the core, all parameters defined below:

Table 1 : The Defined Symbols and Parameters

Symbol	Definition
G_1	A finite cyclic additive group
G_2	A finite cyclic multiplicative group

Symbol	Definition
$\hat{e}$	A bilinear map ê :$G_1 \times G_1 \rightarrow G_2$
H_1、H_2	Hash functions
P_0	A generator of G_1
s_0	The master key
U_i	User U_i for $i = 1,2,\ldots, n$
P_{pub}	Public key
r	Random value
f_j、f_k	File ID
DK_j	Decryption key, for $j = 1, 2, ..., m$
D_{U_i}	The private key of user U_i
Q_{U_i}	The public key of user U_i
ID_{U_i}	The ID of user U_i
J_i	J_i={j,A(i,j) =1},the set of subscript j of filename f_j to which $U_i$has access.

Let U be a set of the user, D is a set of the data, assuming there are n users and m files. Therefore |*U*|=n, |*D*|=m. The matrix A is access control matrix of order n×m as follows:

$$\mathrm{A}\left[U_i, D_j\right] = \begin{cases} 1, \text{user } U_i \text{ can access } D_j \\ 0, \text{otherwise} \end{cases}$$

for i=1 to n；j=1 to m

This access control matrix can be clearly expressed the user and the file access permissions, the i-th column represents the identity of the user and the j-th row indicates data; if A [i, j] is equal to 1, which means that user i can access data j, if A [i, j] is equal to 0, which means that user i cannot access data j. For example, in the health care , the health care professionals U_2 want to obtain the patient's physiological

information *file*1, then A [U_2, D_1] is equal to 1, which means that health care professionals can access the file, if A [U_2, D_1] is equal to 0 then the health care professionals cannot access the file. This is the identity-based access control policy (Identification - Based Access of Control Policy IDBACP), through access control matrix it filters the user to access the data. Only through a trusted authority (TA) or Certification authority (CA) users can access the data. That is, each user can only access the files authorized by him. This can avoid the unexpected events, errors and unauthorized events which may bring the risk for the user.

3.1 Key Generation Phase

Step1: CA definds a set D as m confidential files $D = \{D_1, D_2, \ldots, D_m\}$ and selects non-repeated random integers $\{DK_1, DK_2, \ldots\ldots, DK_m\}$ as the decryption key for decrypting confidential files. Let G_1 be an additive cyclic group. Its order is a prime number q. Let G_2 be a multiplicative cyclic group of the same order q and chooses a bilinear map $\hat{e}: G_1 \times G_1 \rightarrow G_2$ and $P_0 \in G_1$.

Step2: CA generates two hash functions:

$$H_1 : \{0,1\}^* \rightarrow G_1$$

$$H_2 : G_2 \rightarrow \{0,1\}^l, \text{ for some } l$$

and randomly selects $s_0 \in Z_q^*$, and calculate $P_{pub} = s_0 * P_0$.

Secret parameter (Master key): s_0

Public parameters: G_1, G_2, $\hat{e}$, P_0, P_{pub}, H_1, H_2

Step3: CA for each user U_i calculates $D_{U_i} = s_0 * (Q_{U_i})$; $Q_{U_i} = H_1(ID_{Ui})$, where D_{U_i} is secret, and Q_{U_i} is private.

Step4: CA chooses a random value r and calculates $V = r * P_0$, CA based access control matrix, constructs the function given below for each user U_i.

$$F_{U_i}(\mathrm{x},\mathrm{y}) = \frac{x}{H_2(g_{U_i}^{r})}\left[\sum_{j\in J_i} DK_j \times \prod_{\substack{k\in J_i \\ k\neq j}}\left(\frac{y-f_k}{f_j-f_k}\right)\right]$$

Where $g_{U_i} = \hat{e}(Q_{U_i}, P_{pub})$, $x = H_2(\hat{e}(D_{U_i}, V))$, f_k as file ID and y is user U_i for access to file identity of the confidential files.

Example:

The PHRs may come from different medical units, and the content of the message contains the physical information, medical report, drug records, and there are patients, physicians, health care professionals, medical research institutions etc. and other multi-user with different permissions to access authorized individual files. Therefore for each user when accessing PHR, you must make sure that the sources of information and the integrity of the content, and make sure the user permission to access the PHR, and then encrypted and stored it on the Cloud computing server.

Assuming each user in the health care system, such as: patients, health care professionals, medical research institutions, physicians, etc. are different users U_1, U_2, U_3, U_4. The patient's physiological information, major surgery records, medication records, health insurance are $file_1$, $file_2$, $file_3$, $file_4$. Because of the different access permissions for each identity, CA based on access control matrix to the compute $F_{U_i}(\mathrm{x},\mathrm{y})$ function and make identity encryption. Its corresponding decryption keys are DK_1 , DK_2, DK_3, DK_4.

$$\mathrm{A}_{4\mathrm{x}4} = \begin{array}{c} \\ U_1 \\ U_2 \\ U_3 \\ U_4 \end{array}\begin{array}{c} \begin{array}{cccc} DK_1 & DK_2 & DK_3 & DK_4 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

$\mathrm{A}[\mathrm{a}_{11}] = 1$, which means that the patient U_1 has legal authority to get DK_1, and the patient can decrypts physiological information $file_1$. $\mathrm{A}[\mathrm{a}_{13}] = 0$, the medical research unit U_3 is not given the DK_3 permissions, $file_1$ does not decrypt. Assuming the health care staff U_2 granted access as shown in the access control matrix, that is, health

care staff U_2 can access physiological information, medication records, health insurance information DK_1, DK_3, DK_4. Then the health care professionals U_2 can access his own secret key file ID_j using the following public function to get DK_m.

$$F_{U_2}(\mathrm{x},\mathrm{y}) = \frac{x}{H_2(g_{U_2}^r)}\left[\sum_{j\in J_2} DK_j \times \prod_{\substack{k\in J_2=\{1,3,4\}\\ k\neq \mathrm{j}}}\left(\frac{y-f_k}{f_j-f_k}\right)\right]$$

$$= \frac{x}{H_2(g_{U_2}^r)}\left[DK_1 \times \frac{(y-f_3)(y-f_4)}{(f_1-f_3)(f_1-f_4)} + DK_3 \times \frac{(y-f_1)(y-f_4)}{(f_3-f_1)(f_3-f_4)} + DK_4 \times \frac{(y-f_1)(y-f_3)}{(f_4-f_1)(f_4-f_3)}\right]$$

3.2 Key Derivation Phase

Step1: Under the system environment which this paper proposes, the legal user U_i, can obtain the decryption key DK to solve the corresponding confidential information.

Step2: A legal user U_i takes his own private key D_{U_i} and the public parameters ID_{Ui} as input to the function $F_{Ui}(x, y)$ for obtaining the decryption key of the confidential file. where $x = H_2(\hat{e}(D_{U_i}, V))$, y= user ID_{Ui} can access the file identity of confidential files.

Example:

If the health care professionals U_2 want to decrypt the medication record $file_3$, then the health care professionals U_2 must get decryption key DK_3 to decrypt $file_3$, and need to take his own private key D_{U_2} and public V and $file_3$ are substituted into $F_{U_2}(x,y)$, $x = H_2(\hat{e}(D_{U_2}, V))$, $y = f_3$, Its access control matrix is shown below:

$$\begin{array}{c} \\ U_1 \\ U_2 \\ U_3 \\ U_4 \end{array}\begin{array}{c} \begin{array}{cccc} DK_1 & DK_2 & DK_3 & DK_4 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

U_1: patient, U_2: health care professionals, U_3: Medical Research Unit, U_4: physicians, U_5: pharmacists. DK_1: To decrypt $file_1$ the decryption key of physiological information. DK_2: To decrypt $file_2$ the decryption key of major surgery record. DK_3: To decrypt $file_3$ the decryption key of the medication record. DK_4: To decrypt $file_4$ the decryption key of health insurance.

The health care professionals U_2 has three decryption key DK_1, DK_3, DK_4. If the health care professionals U_2 wants to obtain the medication record then substitutes ID from $file_3$ into y, so y = f_3. The health care professionals can be successfully derived DK_3. The decryption process is shown below:

$$F_{U_2}(\mathrm{x},\mathrm{y}) = \frac{x}{H_2(g_{U_2}^r)}\left[\sum_{j\in J_2} DK_j \times \prod_{\substack{k\in J_2=\{1,3,4\}\\ k\neq \mathrm{j}}}\left(\frac{y-f_k}{f_j-f_k}\right)\right]$$

When $\mathrm{x} = \mathrm{H}_2(\hat{e}(D_{U_2}, V))\mathrm{y} = f_3$,then

$$= \frac{x}{H_2(g_{U_2}^r)}\left[DK_1 \times \frac{(y-f_3)(y-f_4)}{(f_1-f_3)(f_1-f_4)} + DK_3 \times \frac{(y-f_1)(y-f_4)}{(f_3-f_1)(f_3-f_4)} + DK_4 \times \frac{(y-f_1)(y-f_3)}{(f_4-f_1)(f_4-f_3)}\right]$$

$$= \frac{x}{H_2(g_{U_2}^r)}\left[DK_1 \times 0 + DK_3 \times \frac{(f_3-f_1)(f_3-f_4)}{(f_3-f_1)(f_3-f_4)} + DK_4 \times 0\right]$$

$$= \frac{x}{H_2(g_{U_2}^r)}\left[DK_3 \times \frac{(f_3-f_1)(f_3-f_4)}{(f_3-f_1)(f_3-f_4)}\right]$$

$$= \frac{H_2(\hat{e}(D_{U2}, r\times P_o))}{H_2\left(\hat{e}(Q_{U2}, P_{pub})^r\right)} \times DK_3$$

$$= \frac{H_2(\hat{e}(s_0\times Q_{U2}, P_0)^r)}{H_2(\hat{e}(Q_{U2}, s_0\times P_0)^r)} \times DK_3$$

$$= \frac{H_2(\hat{e}(Q_{U2}, P_0)^{s_0\times r})}{H_2(\hat{e}(Q_{U2}, P_0)^{s_0\times r})} \times DK_3$$

$$= DK_3$$

Chapter 4 – Solution to Key Management of Dynamic Access Problems

PHR integrates different sources of health information, such as the record of the patient's own measurements (blood pressure, diet, exercise habits, etc.) the clinic physician records (patient allergic reactions, EMR, etc.), hospital records (ECG, doctor, etc.). The personal health information was stored in the appropriate encryption on cloud computing server, in order to ensure the security, the cloud computing storage access control mechanisms must be dependent on the encryption algorithm. We believe that user-transparent encryption mechanism should minimize the involving in key generating and key releasing. This research also assumes the CA as a trusted institution, it can provide a legal mechanism to encrypt data, CA is a trusted space which used to store access control information, access control information is cipher text plus the form of a signature stored. In the actual medical environment, when the doctor wants the patient data access request, the doctor first obtained the patients access control information from CA, and then stores the cipher text on cloud computing space, and finally the doctors use their own private key and access control information to calculate the decryption key to decrypt the data, and obtained the information.

The actual PHRs, users often due to changes in events or time, the access rights need to be updated. For example, the patient Alice goes to the hospital. The doctor Bob need to access the patient physiological information, such as blood pressure, pulse, weight information, etc. That is, the patient Alice can add a new authorized user. Then doctor Bob need to request permissions from CA to access Alice's physiological information. Through the CA certification, Doctor Bob can own the private key to decrypt and obtain Alice's physiological information.

In terms of health care, the blood pressure, pulse, weight record of patients will change in their daily life, so it will keep maintaining and updating. Personal medical records may be with the different access requirements to add, modify, and delete, such as changes in patients, health care professionals, medical research institutions, and physicians permissions. However, storage on cloud computing environments is dynamic and easy to expand, sharing and providing a lot of advantages to meet the PHR integration, which purposes are sharing and exchanging. Therefore, as long as we build a complete PHR which has dynamic access mechanism, we can surely offer a real-time and fulltime service. The dynamic access mechanism patterns are described below:

1. Adding a new authorized user
2. Updating access control matrix

4.1 Adding a New Authorized User

PHR integrate different health information, patients manage and share their own medical records. So they can authorize PHR to legitimate users on themselves, we take following steps to add a new authorized user:

Step1: Let the new authorized user U_{n+1} is added to the new system, $D_{U_{n+1}}$ means who owned the Private Key. CA will adjust access control matrix $A_{n\times m}$ into $A_{(n+1)\times m}$.

Step2: CA generates private $D_{U_{n+1}}$ for the new user U_{n+1}.

Step3: CA computes the new function as following equation.

$$F_{U_{n+1}}(x,y) = \frac{x}{H_2(g_{U_i}^{r})}\left[\sum_{j\in J_{n+1}} DK_j \times \prod_{\substack{k\in J_{n+1}\\ k\neq j}} \left(\frac{y-f_k}{f_j-f_k}\right)\right]$$

The three steps above describe about adding a new authorized user, and the CA will create a new $F_{Un+1}(x, y)$, then add a new row in the access control matrix and give

the access rights. The access control is based on each row of the matrix to describe the access control message, other established $F_{U_{n+1}}$(x, y) function and not because of the new user, affecting other users access control or producing an additional amount of calculation, therefore it is suitable to use on cloud computing environments. New user U_{n+1} can use their private key $D_{U_{n+1}}$, and public key $Q_{U_{n+1}}$ to obtain the legally authorized DK_j.

Example 4.1

Assuming the PHRs already had four users, patients, health care professionals, medical research institutions and physicians, U_1 to U_4. Now we want to add a new user pharmacist, U_5, and have permissions to access the physiological information DK_1, medication record DK_3, health insurance DK_4. The scenario is shown in Figure 3:

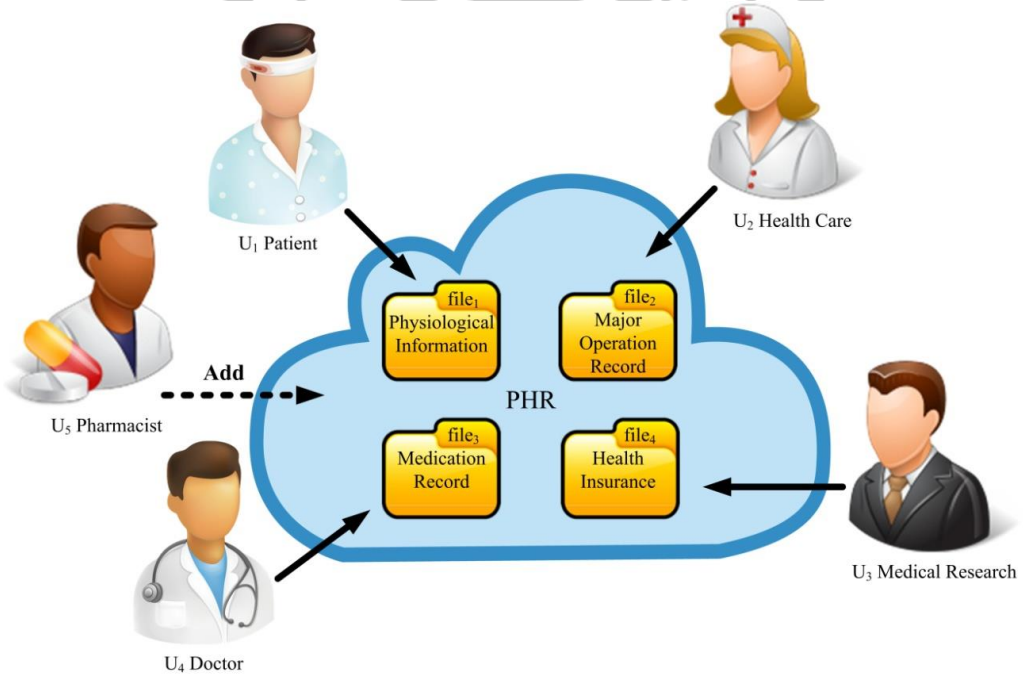


Figure 3: Adding A New User to Access Control Matrix

The relationship of storing its access control matrix is shown below:

$$\begin{array}{c} \\ U_1 \\ U_2 \\ U_3 \\ U_4 \\ U_5 \end{array} \begin{array}{c} \begin{array}{cccc} DK_1 & DK_2 & DK_3 & DK_4 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix} \end{array}$$

U_1: patient, U_2: health care professionals, U_3: Medical Research Unit, U_4: physicians, U_5: pharmacists. DK_1: To decrypt $file_1$ the decryption key of physiological information. DK_2: To decrypt $file_2$ the decryption key of major surgery record. DK_3: To decrypt $file_3$ the decryption key of the medication record. DK_4: To decrypt $file_4$ the decryption key of health insurance.

First of all, CA will add a new row in access control matrix which will change the access matrix from $A_{4\times4}$ to $A_{5\times4}$. Then it will establish a set which can be accessed for the user, J_5={1,3,4}, and calculate the following function.

When x = $H_2(\hat{e}(D_{U_5}, V))$, y = f_1,then

$$F_{U_5}(x,y) = \frac{x}{H_2(g_{U_5}^r)}\left[\sum_{j\in J_5} DK_j \times \prod_{\substack{k\in J_5=\{1,3,4\}\\ k\neq j}}\left(\frac{y-f_k}{f_j-f_k}\right)\right]$$

$$= \frac{x}{H_2(g_{U_5}^r)}\left[DK_1 \times \frac{(f_1-f_3)(y-f_4)}{(f_1-f_3)(f_1-f_4)} + DK_3 \times \frac{(f_1-f_1)(f_1-f_4)}{(f_3-f_1)(f_3-f_4)} + DK_4 \times \frac{(f_1-f_1)(f_1-f_3)}{(f_4-f_1)(f_4-f_3)}\right]$$

$$= \frac{x}{H_2(g_{U_5}^r)}\left[DK_1 \times \frac{(f_1-f_3)(y-f_4)}{(f_1-f_3)(f_1-f_4)} + DK_3 \times 0 + DK_4 \times 0\right]$$

$$= \frac{H_2(\hat{e}(D_{U5}, r\times P_o))}{H_2\left(\hat{e}(Q_{U5}, P_{pub})^r\right)} \times DK_1$$

$$= \frac{H_2(\hat{e}(s_0\times Q_{U5}, P_0)^r)}{H_2(\hat{e}(Q_{U5}, s_0\times P_0)^r)} \times DK_1$$

$$= \frac{H_2(\hat{e}(Q_{U5}, P_0)^{s_0\times r})}{H_2(\hat{e}(Q_{U5}, P_0)^{s_0\times r})} \times DK_1$$

$$= DK_1$$

When x = $H_2(\hat{e}(D_{U_5}, V))$, y = f_3, then

$$F_{U_5}(x,y) = \frac{x}{H_2(g_{U_5}^r)}\left[\sum_{j\in J_5} DK_j \times \prod_{\substack{k\in J_5=\{1,3,4\}\\ k\neq j}}\left(\frac{y-f_k}{f_j-f_k}\right)\right]$$

$$= \frac{x}{H_2(g_{U_5}^r)}\left[DK_1 \times \frac{(f_3-f_3)(f_3-f_4)}{(f_1-f_3)(f_1-f_4)} + DK_3 \times \frac{(f_3-f_1)(f_3-f_4)}{(f_3-f_1)(f_3-f_4)} + DK_4 \times \frac{(f_3-f_1)(f_3-f_3)}{(f_4-f_1)(f_4-f_3)}\right]$$

$$= \frac{x}{H_2(g_{U_5}^r)}\left[DK_1 \times 0 + DK_3 \times \frac{(f_3-f_1)(f_3-f_4)}{(f_3-f_1)(f_3-f_4)} + DK_4 \times 0\right]$$

$$= \frac{H_2(\hat{e}(D_{U5}, r \times P_o))}{H_2\left(\hat{e}(Q_{U5}, P_{pub})^r\right)} \times DK_3$$

$$= \frac{H_2(\hat{e}(s_0 \times Q_{U5}, P_0)^r)}{H_2(\hat{e}(Q_{U5}, s_0 \times P_0)^r)} \times DK_3$$

$$= \frac{H_2(\hat{e}(Q_{U5}, P_0)^{s_0 \times r})}{H_2(\hat{e}(Q_{U5}, P_0)^{s_0 \times r})} \times DK_3$$

$$= DK_3$$

When x = $H_2(\hat{e}(D_{U_5}, V))$, y = f_4, then

$$F_{U_5}(x, y) = \frac{x}{H_2(g_{U_5}^r)}\left[\sum_{j \in J_5} DK_j \times \prod_{\substack{k \in J_5 = \{1,3,4\} \\ k \neq j}} \left(\frac{y-f_k}{f_j-f_k}\right)\right]$$

$$= \frac{x}{H_2(g_{U_5}^r)}\left[DK_1 \times \frac{(f_4-f_3)(f_4-f_4)}{(f_1-f_3)(f_1-f_4)} + DK_3 \times \frac{(f_4-f_1)(f_4-f_4)}{(f_3-f_1)(f_3-f_4)} + DK_4 \times \frac{(f_4-f_1)(f_4-f_3)}{(f_4-f_1)(f_4-f_3)}\right]$$

$$= \frac{x}{H_2(g_{U_5}^r)}\left[DK_1 \times 0 + DK_3 \times 0 + DK_4 \times \frac{(f_4-f_1)(f_4-f_3)}{(f_4-f_1)(f_4-f_3)}\right]$$

$$= \frac{H_2(\hat{e}(s_0 \times Q_{U5}, P_0)^r)}{H_2(\hat{e}(Q_{U5}, s_0 \times P_0)^r)} \times DK_4$$

$$= \frac{H_2(\hat{e}(Q_{U5}, P_0)^{s_0 \times r})}{H_2(\hat{e}(Q_{U5}, P_0)^{s_0 \times r})} \times DK_4$$

$$= DK_4$$

Finally, U_5 will get the permissions to access the physiological information DK_1, the medication record DK_3, the health insurance DK_4.

4.2 Updating Access Control Matrix

During medical care, it might affect by the reasons of staff adjustment, plan changing or policy, and cause the fact that access permission need to update, so personal medical records must be amended with different situation, we take these methods below to update access control matrix:

Step1: Assuming the system user U_i which accesses the file permissions are subject to change, and the CA will update the corresponding column in the access

control matrix $A_{n\times m}$ updating to A[U_i, D_j], renewing J_i' set.

CA computes the new $F_{U_i'}$ as following.

$$F_{U_i'}(x,y) = \frac{x}{H_2(g_{U_i}^{r})}\left[\sum_{j\in J_i'} DK_j \times \prod_{\substack{k\in J_i' \\ k\neq j}} \left(\frac{y-f_k}{f_j-f_k}\right)\right]$$

Example 4.2

In Example 4.2, we will discuss two kinds of updating access control matrix cases. Case1 is to update general access, such as U_2could have access to J_2 = {1,3,4}, and now it need to update the permissions such as J_2 = {1,2,3}. Case2 is a special case of case1, which is to remove a user. For example, U_4 was originally able to access the set J_4= {1,2,3}, and now we want to remove the access of the user U_4 to every file, we can replace the row in the access control matrix with zeros which will remove U_4. The following we will describe more detail of these two Cases.

Case1: Assuming U_2 was healthcare professionals, who can access the $file_4$, health insurance, but because of the change of plan, U_2health care professionals can no longer access the $file_4$, health insurance, but have the new permission to access the $file_2$, surgery record. This situation is shown in Figure 4:

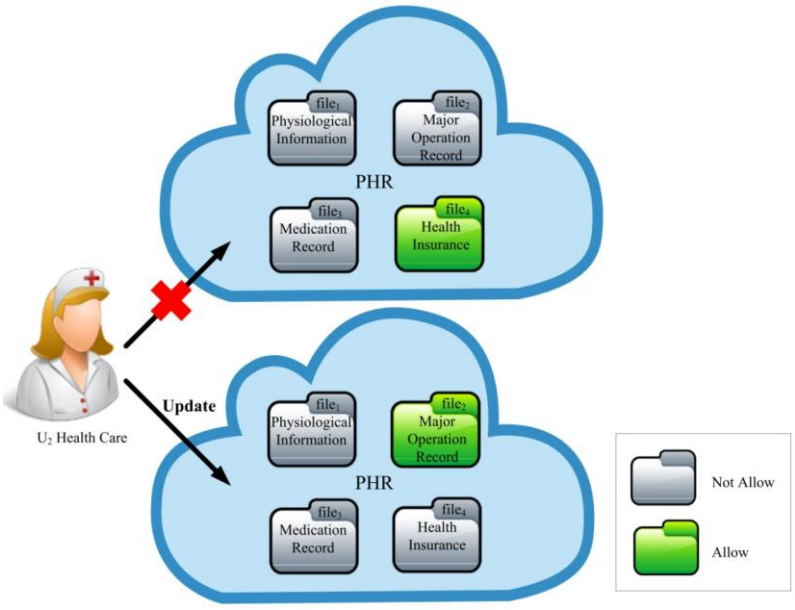


Figure 4 : Updating Access Control Matrix to Access Control Matrix

Its relation of access control matrix is shown below:

$$\begin{array}{c} \\ U_1 \\ U_2 \\ U_3 \\ U_4 \end{array} \begin{array}{c} \begin{array}{cccc} DK_1 & DK_2 & DK_3 & DK_4 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

U_1: patient, U_2: health care professionals, U_3: Medical Research Unit, U_4: physicians, U_5: pharmacists. DK_1: To decrypt $file_1$ the decryption key of physiological information. DK_2: To decrypt $file_2$ the decryption key of major surgery record. DK_3: To decrypt $file_3$ the decryption key of the medication record. DK_4: To decrypt $file_4$ the decryption key of health insurance.

First of all, CA will set access control matrix to A[U_2, $D_{j'}$] and recalculated for U_2.

$$F_{U_{2'}}(\mathrm{x},\mathrm{y}) = \frac{x}{H_2(g_{U_{2'}}^{r})}\left[\sum_{j\in J_{2'}} DK_j \times \prod_{\substack{k\in J_{\mathrm{i}'}=\{1,2,3\} \\ k\neq \mathrm{j}}} \left(\frac{y-f_k}{f_j-f_k}\right)\right]$$

When x = $H_2(\hat{e}(D_{U_{2'}}, V))$, y = f_1, then

$$= \frac{x}{H_2(g_{U_{2'}}^{r})}\left[DK_1 \times \frac{(f_1-f_2)(f_1-f_3)}{(f_1-f_2)(f_1-f_3)} + DK_2 \times \frac{(f_1-f_3)(f_1-f_1)}{(f_2-f_3)(f_2-f_1)} + DK_3 \times \frac{(f_1-f_1)(f_1-f_2)}{(f_3-f_1)(f_3-f_2)}\right]$$

$$= \frac{x}{H_2(g_{U_{2'}}^{r})}\left[DK_1 \times \frac{(f_1-f_2)(f_1-f_3)}{(f_1-f_2)(f_1-f_3)} + DK_2 \times 0 + DK_3 \times 0\right]$$

$$= \frac{H_2(\hat{e}(D_{U2'}, r \times P_o))}{H_2\left(\hat{e}(Q_{U2'}, P_{pub})^{r}\right)} \times DK_1$$

$$= \frac{H_2(\hat{e}(s_0 \times Q_{U2'}, P_0)^{r})}{H_2(\hat{e}(Q_{U2'}, s_0 \times P_0)^{r})} \times DK_1$$

$$= \frac{H_2(\hat{e}(Q_{U2'}, P_0)^{s_0 \times r})}{H_2(\hat{e}(Q_{U2'}, P_0)^{s_0 \times r})} \times DK_1$$

$$= DK_1$$

When x = $H_2(\hat{e}(D_{U_{2'}}, V))$, y = f_2, then

$$= \frac{x}{H_2(g_{U_{2'}}^{r})}\left[DK_1 \times \frac{(f_2-f_2)(f_2-f_3)}{(f_1-f_2)(f_1-f_3)} + DK_2 \times \frac{(f_2-f_3)(f_2-f_1)}{(f_2-f_3)(f_2-f_1)} + DK_3 \times \frac{(f_2-f_1)(f_2-f_2)}{(f_3-f_1)(f_3-f_2)}\right]$$

$$= \frac{x}{H_2(g_{U_{2'}}^{r})}\left[DK_1 \times 0 + DK_2 \times \frac{(f_2-f_3)(f_2-f_1)}{(f_2-f_3)(f_2-f_1)} + DK_3 \times 0\right]$$

$$= \frac{H_2(\hat{e}(D_{U2'}, r \times P_o))}{H_2\left(\hat{e}(Q_{U2'}, P_{pub})^r\right)} \times DK_2$$

$$= \frac{H_2(\hat{e}(s_0 \times Q_{U2'}, P_0)^r)}{H_2(\hat{e}(Q_{U2'}, s_0 \times P_0)^r)} \times DK_2$$

$$= \frac{H_2(\hat{e}(Q_{U2'}, P_0)^{s_0 \times r})}{H_2(\hat{e}(Q_{U2'}, P_0)^{s_0 \times r})} \times DK_2$$

$$= DK_2$$

When x = $H_2(\hat{e}(D_{U_{2'}}, V))$, y = f_3, then

$$= \frac{x}{H_2(g_{U_{2'}}^r)}\left[DK_1 \times \frac{(f_3-f_2)(f_3-f_3)}{(f_1-f_2)(f_1-f_3)} + DK_2 \times \frac{(f_3-f_3)(f_3-f_1)}{(f_2-f_3)(f_2-f_1)} + DK_3 \times \frac{(f_3-f_1)(f_3-f_2)}{(f_3-f_1)(f_3-f_2)}\right]$$

$$= \frac{x}{H_2(g_{U_{2'}}^r)}\left[DK_1 \times 0 + DK_2 \times 0 + DK_3 \times \frac{(f_3-f_1)(f_3-f_2)}{(f_3-f_1)(f_3-f_2)}\right]$$

$$= \frac{H_2(\hat{e}(D_{U2'}, r \times P_o))}{H_2\left(\hat{e}(Q_{U2'}, P_{pub})^r\right)} \times DK_3$$

$$= \frac{H_2(\hat{e}(D_{U2'}, r \times P_o))}{H_2\left(\hat{e}(Q_{U2'}, P_{pub})^r\right)} \times DK_3$$

$$= \frac{H_2(\hat{e}(D_{U2'}, r \times P_o))}{H_2\left(\hat{e}(Q_{U2'}, P_{pub})^r\right)} \times DK_3$$

$$= DK_3$$

Finally U_2 will have new DK_1、DK_2、DK_3.

Case 2: Assuming the doctor U_4 has left, and does not have any access anymore. To do that, we can update the access control matrix. The situation is shown in Figure 5:

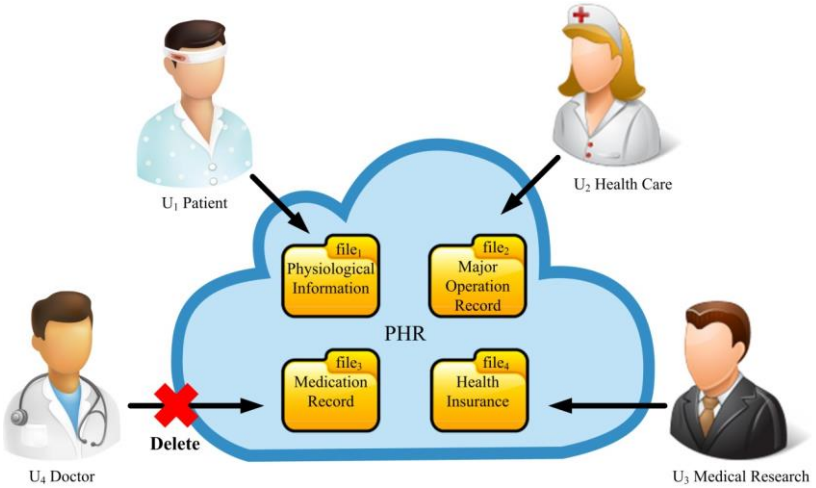


Figure 5 : Remove A User Authorization from Access Control Matrix

U_4 originally can access the set $J_4 = \{1,2,3\}$, and now we want to remove the access right of the user U_4 to every file. Then we can update the access control matrix of U_4, with zeros which means to make $J_4 = \{\emptyset\}$, therefore U_4 is removed. Its final relation of access control matrix is shown below:

$$\begin{array}{c} \\ U_1 \\ U_2 \\ U_3 \\ U_4 \end{array} \begin{array}{c} \begin{array}{cccc} DK_1 & DK_2 & DK_3 & DK_4 \end{array} \\ \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

U_1: patient, U_2: health care professionals, U_3: Medical Research Unit, U_4: physicians, U_5: pharmacists. DK_1: To decrypt $file_1$ the decryption key of physiological information. DK_2: To decrypt $file_2$ the decryption key of major surgery record. DK_3: To decrypt $file_3$ the decryption key of the medication record. DK_4: To decrypt $file_4$ the decryption key of health insurance.

Chapter 5 – Analysis of Security

In this section, a security analysis is performed to examine whether the proposed scheme is secure or not for practical applications. The analysis focuses upon four types of attack that may impact the system security.

5.1 Equation Attack

Definition: Equation Attack is when the attacker attempts to use public formula $F_{U_i}(\bullet)$ to crack the polynomial $F_{U_i}(\bullet)$ to get the decryption key.

Any attacker can take advantage of public information the $F_{U_i}(\bullet)$ in attempt to try to get the decryption key. However, in setting the system, the user must have the private key to decrypt the corresponding decryption key. The public formula is

$F_{U_i}(\mathrm{x},\mathrm{y}) = \frac{x}{H_2(g_{U_i}^r)}\left[\sum_{j\in J_i} DK_j \times \prod_{\substack{k\in J_i \\ k\neq j}}\left(\frac{y-f_k}{f_j-f_k}\right)\right]$,Where $g_{Ui} = \hat{e}(Q_{U_i}, P_{pub})$, $x = H_2(\hat{e}(D_{U_i}, V)$, f_k is file ID and y is user Ui for access to confidential files of File Identity. $x = H_2(\hat{e}(D_{U_i}, V)$ will be private D_{U_i} with an open V to compute Bilinear pairing. That is, when the attacker substitutes x with x', it must unravel the discrete logarithm problem, and the formula $F_{U_i}(\bullet)$ is based on the mathematics of the Bilinear Diffie-Hellman Assumption (BDH). Unless the attacker can break the basis of mathematical problems (eg, computational Diffie-Hellman problems (Computational Diffie-Hellman Problem CDHP), bilinear BDH problems (Bilinear Diffie-Hellman Problem, BDHP), the discrete logarithm problem (Discrete Logarithm Problem, DLP)), otherwise the formula to $F_{U_i}(\bullet)$ is safe.

5.2 External Attack

Definition: External Attack is non-legally authorized external personnel who attempts to unauthorized access through the open parameters, and trying to obtain the decryption key *DK* or to crack cipher text to obtain the private health record.

Since PHRs has huge users, PHR contains a high degree of privacy and sensitive information. In order to find some benefits in commercial, criminals try a non-legally authorized external personnel to derive the public parameters. After an external attacker obtained the public parameters or the public equation $F_{U_i}(x, y)$, because of not having the secret parameter s_0, therefore the attacker is unable to know the members D_{U_i}, involved in the secret communication because $x = H_2(\hat{e}(D_{U_i}, V))$, will be private D_{U_i} with open V to compute Bilinear pairing, if someone want to get the legal decryption key, must to solve the discrete logarithm problem firstly.

5.3 Collaborative Attack

Definition: Collaborative attack is two or more internal legally authorized user collaborate to collect each other's privacy parameters in attempt to derive the unauthorized decryption key *DK*.

Assuming in collaborative attack, two or more internal users want to attack another internal legitimate users. Collusion attacker will try to collect each other's privacy parameters to obtain another internal user who has permission to access the private key *DK*. The explanation is as the situation in example 4.1. Collusion attacker's permission is $J_4 = \{1, 2, 3\}$, and $J_5 = \{1, 3\}$, and the victim user rights is $J_1 = \{1, 2, 3, 4\}\}$, U_1 has more access permission of $file_4$ than U_4 and U_5. Therefore U_4 and U_5 want to do collision attack on U_1 to obtain the decryption key DK_4. Then substituting U_1 into

F_{U_i}(x, y), as shown below.

$$F_{U_1}(\mathrm{x},\mathrm{y}) = \frac{x}{H_2(g_{U_1}^r)}\left[DK_1 \times \frac{(y-f_2)(y-f_3)(y-f_4)}{(f_1-f_2)(f_1-f_3)(f_1-f_4)} + DK_2 \times \frac{(y-f_1)(y-f_3)(y-f_4)}{(f_2-f_1)(f_2-f_3)(f_2-f_4)} + DK_3 \times \frac{(y-f_1)(y-f_2)(y-f_4)}{(f_3-f_1)(f_3-f_2)(f_3-f_4)} + DK_4 \times \frac{(y-f_1)(y-f_2)(y-f_3)}{(f_4-f_1)(f_4-f_2)(f_4-f_3)}\right]$$

Substitutes U_4 into $F_{U_4}(\mathrm{x},\mathrm{y})$, as shown below:

$$F_{U_4}(\mathrm{x},\mathrm{y}) = \frac{x}{H_2(g_{U_4}^r)}\left[DK_1 \times \frac{(y-f_2)(y-f_3)}{(f_1-f_2)(f_1-f_3)} + DK_2 \times \frac{(y-f_1)(y-f_3)}{(f_2-f_1)(f_2-f_3)} + DK_3 \times \frac{(y-f_1)(y-f_2)}{(f_3-f_1)(f_3-f_2)}\right]$$

Substitutes U_5 into $F_{U_5}(\mathrm{x},\mathrm{y})$, as shown below:

$$F_{U_5}(\mathrm{x},\mathrm{y}) = \frac{x}{H_2(g_{U_5}^r)}\left[DK_1 \times \frac{x}{H_2(g_{U_5}^r)} \times \frac{(y-f_3)}{(f_1-f_3)} + DK_3 \times \frac{(y-f_1)}{(f_3-f_1)}\right]$$

Even if U_4 and U_5 exchange their information, the members involved in secret D_{U_i} cannot be revealed directly, and the Bilinear pairing calculation will still result a null value. Therefore the collusion attack is the same as a single attacker. The attacker cannot get the additional information. That is why regardless of the relationship between the internal collusion attacker and the victim or the number of attackers, the attackers are still unable to collect other's private parameters to derive a non-authorized *DK*.

5.4 Internal Attack

Definition: Internal Attack is a legitimate internal attacker who uses the known publicly formula F_{U_i}(x, y) and the privacy of their own parameters to try and get other user decryption key.

The explanation is as the situation in example 4.1. Legitimate users U_1 and U_2 can be deduced to $F_{U_i}(\mathrm{x},\mathrm{y})$ and decryption key DK_4, and U_2 can access the set J_2 = {1, 3, 4}, U_1 can access the set J_1 = {1, 2, 3, 4}. Assuming U_2 is an attacker, he hopes to own his secret parameters D_{U_2} and the public parameters $F_{U_i}(\mathrm{x},\mathrm{y})$ to derive the privacy parameter D_{U_2}, then obtaining access permission file$_2$ of U_1. In this method, our

formula is as shown below:

$$F_{U_i}(\mathrm{x},\mathrm{y}) = \frac{x}{H_2(g_{U_i}^r)}\left[\sum_{j\in J_i} DK_j \times \prod_{\substack{k\in J_i \\ k\neq j}}\left(\frac{y-f_k}{f_j-f_k}\right)\right]$$

Substitutes U_1 into $F_{U_1}(\mathrm{x}, \mathrm{y})$, the result is as follows：

$$F_{U_1}(\mathrm{x},\mathrm{y}) = \frac{x}{H_2\left(g_{U_1}^r\right)}\left[DK_1 \times \frac{(y-f_2)(y-f_3)(y-f_4)}{(f_1-f_2)(f_1-f_3)(f_1-f_4)} + DK_2 \times \frac{(y-f_1)(y-f_3)(y-f_4)}{(f_2-f_1)(f_2-f_3)(f_2-f_4)} + DK_3 \times \frac{(y-f_1)(y-f_2)(y-f_4)}{(f_3-f_1)(f_3-f_2)(f_3-f_4)} + DK_4 \times \frac{(y-f_1)(y-f_2)(y-f_3)}{(f_4-f_1)(f_4-f_2)(f_4-f_3)}\right]$$

Substitutes U_2 into $F_{U_2}(\mathrm{x}, \mathrm{y})$, the result is as follows：

$$F_{U_2}(\mathrm{x},\mathrm{y}) = \frac{x}{H_2\left(g_{U_2}^r\right)}\left[DK_1 \times \frac{(y-f_3)(y-f_4)}{(f_1-f_3)(f_1-f_4)} + DK_3 \times \frac{(y-f_1)(y-f_4)}{(f_3-f_1)(f_3-f_4)} + DK_4 \times \frac{(y-f_1)(y-f_3)}{(f_4-f_1)(f_4-f_3)}\right]$$

Assuming the attacker U_2 uses his own privacy D_{U_2} to derive the DK_2 of U_1, then the attacker substitutes DK_2into $F_{U_1}(\mathrm{x}, \mathrm{y})$, as shown below:

$$= \frac{x}{H_2\left(g_{U_1}^r\right)}\left[DK_2 \times \frac{(y-f_1)(y-f_3)(y-f_4)}{(f_2-f_1)(f_2-f_3)(f_2-f_4)}\right]$$

$$= \frac{H_2(\hat{e}(D_{U2}, r\times P_o))}{H_2\left(\hat{e}(Q_{U1}, P_{pub})^r\right)} \times DK_2 \times \frac{(y-f_1)(y-f_3)(y-f_4)}{(f_2-f_1)(f_2-f_3)(f_2-f_4)}$$

The above equation shows that if U_2wants to get DK_2, it must first obtain U_1 secret parameters s_0, but each agreement are required to go through Bilinear pairing calculation unless you solve the discrete logarithm problem, otherwise it is impossible to obtain D_{U_2}. User access permissions to the file must also go through the CA authorized to pass the $F_{U_i}(\mathrm{x}, \mathrm{y})$ function verification, otherwise it will obtain null value. This attack cannot be reversed to the polynomial form, illegal messages, so they can effectively block the attack equation.

Chapter 6 – Conclusion

In this thesis, we propose a key management based on bilinear pairing which can work correctly on Cloud computing environment as the center of the Personal Health Records (PHR) exchange model to construct the relationship between access control matrix to manage each user. In order to ensure that each patient self-management and sharing their health records, we have designed a patient-centered access mechanism and multiuser access which reduces the complexity of key management solutions on the cloud environment.

In the method, in order to make the PHR suitable for development on Cloud computing environment, we must make sure that the integrity of the sources of information and content, and provide a flexible multi-user access control mechanism. We designed a public formula F_{U_i}(x, y), and filter user access to data through the access control matrix. Only users who pass the trusted authority or certification authority will obtain access to the encrypted information. This prevents from unexpected events, errors and unauthorized events that may bring risks to user. Access control scheme can be constructed through the Cloud computing environment effectively in order to resist the equation attack, external attack, collaborative attack, and internal attack.

References

[1] 吳老德. (2010)，高齡社會理論與策略：新文京開發出版有限公司。

[2] Li Ming Yu, Shucheng Ren Kui, & Lou Wenjing, 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*, pp. 89-106, 2010.

[3] Tang P. C., Ash J. S., Bates D. W., Overhage J. M., & Sands D. Z., Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption. *Journal of the American Medical Informatics Association*, Vol. 13, No.2, pp. 121-126, 2006.

[4] Cloud Computing in Health Care to Reach $5.4 Billion by 2017: Report Retrieved 2012/10/23, from http://www.eweek.com/c/a/Health-Care-IT/Cloud-Computing-in-Health-Care-to-Reach-54-Billion-by-2017-Report-512295/

[5] Kahn J. S., Aulakh V., & Bosworth A., What It Takes: Characteristics of The Ideal Personal Health Record, *Health Affairs*, Vol. 28, No.2, pp.369-376, 2009.

[6] Burrington-Brown J., Fishel J., Fox L., Friedman B., Giannangelo K., Jacobs E., Morgan, J., Defining The Personal Health Record. *Journal Of AHIMA/American Health Information Management Association*, Vol. 76, No.6, pp. 24. 2005.

[7] 台灣家庭醫學醫學會醫學資訊委員會(2010)，個人健康記錄指導原則。檢自：http://www.tafm.org.tw/data/012/meeting/209.pdf

[8] Alawneh, Ruba, Development of Embedded Personal Health Care Record System. *iBusiness*, Vol.3, pp.178-183. 2011.

[9] Detmer Don, Bloomrosen, Meryl, Raymond, Brian, & Tang, Paul, Integrated Personal Health Records: Transformative Tools for Consumer-Centric Care. *BMC Medical Informatics and Decision Making*, Vol.8, No.1, pp. 45. 2008.

[10] Mell, Peter, & Grance, Timothy. The NIST Definition of Cloud Computing. *NIST Special Publication*, Vol. 800, pp.145, 2011.

[11] Rolim, Carlos Oberdan, Koch, Fernando Luiz, Westphall, Carlos Becker, Werner, Jorge, Fracalossi, Armando, & Salvador, Giovanni Schmitt. A Cloud Computing Solution for Patient's Data Collection in Health Care Institutions. *Second International Conference on eHealth, Telemedicine, and Social Medicine*, Vol. pp. 95-99, 2010

[12] Mahoney, Diane Feeney, Tarlow, Barbara J, & Jones, Richard N., Effects of An Automated Telephone Support System on Caregiver Burden and Anxiety: Findings from The REACH for TLC Intervention Study. *The Gerontologist*, Vol. 43, No.4, pp.556-567, 2003.

[13] Hoang Doan B., & Chen Lingfeng., Mobile cloud for assistive healthcare (MoCAsH). *Services Computing Conference*, Vol., pp. 325 – 332, 2010.

[14] Brennan, Patricia Flatley, & Yasnoff, William A., Medical Informatics and Preparedness. *Journal of the American Medical Informatics Association*, Vol.9, No.2, pp. 202-203, 2002.

[15] Narayanan, Hema Andal Jayaprakash, & Gunes, Mehmet Hadi, Ensuring Access Control in Cloud Provisioned Healthcare Systems, *Consumer Communications and Networking Conference*, pp.247 – 251, 2011.

[16] Subashini S., & Kavitha V., A Survey on Security Issues in Service Delivery Models of Cloud Computing. *Journal of Network and Computer Applications*, Vol.34, No.1, pp.1-11,2011.

[17] Shamir, Adi., Identity-Based Cryptosystems and Signature Schemes. *Advances in Cryptology*, pp. 47-53,1985.

[18] Koblitz Neal., Elliptic Curve Cryptosystems. *Mathematics of Computation*, Vol.48, No.177, pp.203-209, 1987.

[19] Menezes, Alfred J., Okamoto, Tatsuaki, & Vanstone, Scott A., Reducing Elliptic Curve Logarithms to Logarithms in A Finite Field, *IEEE Transactions on Information Theory*, Vol. 39, No.5, pp. 1639-1646, 1993.

[20] Boneh Dan, & Franklin, Matt. Identity-Based Encryption from The Weil Pairing. *Advances in Cryptology*, pp. 213-229, 2001.