東海大學資訊管理研究所

碩士學位論文

雲端儲存環境中數位健康紀錄之
機密性資料的保護機制

Confidentiality Protection of Digital Health Records in Cloud Computing

指導教授：陳澤雄 博士
劉嘉惠 博士

研 究 生：江岱倫 撰

中華民國 104 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　　　江岱倫　　　君所提之論文

雲端儲存環境中數位健康紀錄之機密性資料的保護機制

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：賴飛羆 （簽章）

委　員：陳澤龍

陳志賢

劉嘉惠

陳澤雄

中 華 民 國　104　年　06　月　12　日

誌謝

完成這篇碩士論文需感謝的人甚多，在求學生涯中遇到如此美好的良師益友感到慶幸及珍惜。

由衷的感謝陳澤雄老師、劉嘉惠老師，以及鐘玉芳老師。密集地開會中老師總是耐心地陪伴我們走過每個階段，在困頓的時候適時提醒；當我在生活中遇到難題的時候，老師是知無不言、言無不盡的把他們所知道的一切與我分享；劉嘉惠老師於忙碌的行政系務中抽空與我們反反覆覆討論演算法和安全性，內心充滿感謝；所以三位老師當然是我成長過程中的貴人！

互相討論的習慣讓我獲益良多，與陳志賢老師討論的過程中瞭解到從數學家的觀點檢視論文原來有某些疏漏，並且更加實事求是；陳老師從百忙之中抽空從論文第一個字看到最後一個字甚是感動！討論的過程中磨練英文寫作的表達力、該如此嚴謹的定義演算法。感謝口試委員賴飛羆老師、陳志賢老師，陳澤龍老師對於論文提出重要的建議，讓論文更完整。撰寫論文的過程中有互相協助的夥伴真是幸運！感謝孫先昱與我同時學習演算法，遇到瓶頸時總是有人可以討論；尹姿在課業上總是認真，在多次練習簡報時、上台前夕即時救援已經疲憊的我；感謝一起努力、即時幫助的夥伴們，包含耀民、建銘、勝凱、俊毅。

當然也非常感謝重要的家人，家人總是給予支持，追求理想的現階段無後顧之憂；感到脆弱的時候想到還有家人，心裡又是溫暖；沒有他們我也無法在東海求學與這些優秀的夥伴們學習。

江岱倫 謹致於

東海大學資訊管理研究所

中華民國104年07月01日

論文名稱：雲端儲存環境中數位健康紀錄之機密性資料的保護機制

校所名稱：東海大學資訊管理學系研究所

畢業時間：2015年06月

研 究 生：江岱倫　　　　　　　　　　指導教授：陳澤雄 博士
劉嘉惠 博士

論文摘要：

以往電子病歷是上傳生理資訊到雲端，讓醫護人員更容易存取和管理資料，或者有效整合病歷。這些資料往往只提供醫護人員檢視，並且著重於管理電子病歷和傳輸資料為主。

本論文提出於雲端環境執行且以病友為中心的個人健康紀錄 PHR(Personal Health Record)的架構。由病友主動管理自身健康資訊，如就診的資料、健康報告，生理資訊…等，明確了解自己的健康狀況，並且採取更積極的態度維持健康。從病友的角度思考，由病友決定資料的開放權限，以及其使用期限。

在雲端的環境中存放資料有助於降低成本、資訊分享，卻也伴隨潛在的資訊安全的威脅。因此本論文提出適用於多重使用者(如照護人員、病人本身，家屬…)的雲端環境安全傳送機制，使用者藉由本論文提出的傳送機制與伺服器端溝通，獲得欲取得的資料，並同時保障使用者以及伺服器端的隱私與安全性，同時也能提供多重使用者傳輸資料的過程中確保資訊的安全性。

關鍵詞：個人健康紀錄、安全傳輸、隱私保護、雲端計算、模糊傳送

Title of Thesis：Confidentiality Protection of Digital Health Records in Cloud Computing

Name of Institute: Tunghai University, Graduate Institute of Information Management

Graduation Time：(06/2015)

Student Name：Dai Lun, Chiang　　　　　Advisor Name：Dr. Tzer-Shyong Chen

Dr. Chia-Hui Liu

Abstract：

Electronic medical records containing vital information were uploaded to the cloud, allowing medical crews more easy access and management of data and integration of medical records. Such data system provides relevant information to medical personnel and facilitates and stress on electronic medical record management and data transmission.

A structure of cloud-based and patient-centered personal health record (PHR) is proposed in this study. Which enables patients to automatically manage their health information, such as appointment date with doctor, health reports, and a throughout understanding of their own health conditions, and a positive attitudes to maintain the health. The patients decides for themselves who has access to their records over a specific span of time specified by the patients.

Storing data in a cloud environment could reduce costs and enhance the share of information, but the potential threat of information security should be taken into consideration. A cloud-based secure transmission mechanism suitable for multiple users (like nurse aides, patients, and family members) is proposed in this study.

Key words: personal health record, secure transmission, privacy preservation, cloud computing, oblivious transfer

Contents

Chapter 1—Introduction 1

1.1 Research Background 1

1.2 Research Motivation 3

1.3 Research Purpose 5

Chapter 2—Related work 7

2.1 Introduction of PHR..7

2.3 Cloud Computing..10

2.3 Security Issues of the Cloud Environment..............................12

2.4 Oblivious Transfer 14

Chapter 3—The Proposed Scheme 16

3.1 Architecture of PHR System in Cloud 16

3.2 A New Oblivious Transfer Protocol..17

3.2.1 Initialization Phase...19

3.2.2 Oblivious Transfer Phase 19

3.3 Example 21

Chapter 4—Security Analysis...23

4.1 Security Analysis 23

4.1.1 Accuracy 23

4.1.2 Sender Privacy..23

4.1.3 Receiver Privacy 23

4.2 Performance Analysis 24

Chapter 5 — Conclusion..25

Reference 26

List of Figures

Figure 2.1 : PHR Construction..8

Figure 2.2 : NIST 11

Figure 2.3 : Oblivious Transfer Protocol 15

Figure 3.1 : PHR System in Cloud Environment...17

Figure 3.2 : The Process of The Encrypt Protocol...20

List of Tables

Table 1 : Notations Defined And Used in Our Scheme 18

Table 2 : Comparisons of Transmission Costs and Computation Costs 24

Chapter 1—Introduction

1.1 Research Background

With the development of information technology, traditional paper medical records have been replaced by EMR (Electronic Medical Records) gradually. The relevant medical applications contain HL7 (Health Level Seven), EMR (Electronic Medical Records), HIS (Health Information System). Through the internet connection, medical crews can access the system patients' rewards of a medical institute for editing, revising and exchanging data. However the main application still focuses on EMR management and data transformation. Although a lot of hospitals have implemented the EMR and also the plan of medical records exchanging construction has already been proposed, there is still not a general standard. Therefore, it is difficult for each institution to reach the goal of interoperability in a short time. Besides, instead of focusing on patient health management, EMR is mainly designed for the applications in clinical medicine by the professional medical crews. With the progress and popularity of technology and the raise of patients' awareness, a lot of information management scheme related to these kinds of topics can be upgraded to data involving health care services for long-term treatment [1-4], groups [5], health care centers and services [6]. WHO (World Health Organization) also suggests that when it comes to patients' caring, medical institutions should put more emphasis on prevention rather than curing. In that case, it also needs highly proactive participation of patients. the e-health tools which provide constant support can help patients have more opportunities to access their own records and enable them to have a proactive interest in their therapy. In those situations, American Health Information Management Association [7] define PHR (Personal Health Record) as an electronic, highly accessible, and lifelong personal health information. Since medical records may be scattered in different medical institutions [8], integrating the whole data from different sources can make PHR more complete, updated and user friendly.

M.Li et. al [9] proposed a patient-focused health record exchange construction. The PHR was managed by patients themselves, including medical records and derived application services. PHR preserves complete personal medical information, and users can also communicate with health care supporters through proactive participation and self-maintaining [10-11]. The medical information and records can be transferred to PHR through the internet, allowing the users to have knowledge each of their medical history. According to the former research, providing the summary information at the end of treatment for patients could help them get much more understanding about their own medical condition as well as encourage them to dedicate themselves to the treating programs [12]. Meanwhile, PHR should satisfy the following essential requirements [13]. Users have the right to determine who has the authority to access the PHR, which includes the lifelong health information offered by health care providers. PHR can be accessed anytime and anywhere and is able to ensure the privacy and security. PHR can be used as a reference for a family physician or an attending physician when it is needed. In that way, it is more convenient for medical or crews to get more information about patients' health conditions. Besides, it can also be regarded as a sample of home caring and telemedicine for the purpose of conducting research and analysis. For the contents of PHR, there is still no consistent standard; it mainly depends on the type of medical cares the patients receive.

As technology progresses, it has become a trend to place information systems and other application services in the cloud. Also, most of medical information technology suppliers and health care providers have begun to transfer PHR application services and data to the cloud, instead of constructing new data centers, to reduce cost. The combination of PHR application services with cloud computing brings lots of benefits.

(1) Reducing Cost. Medical institutes or care centers use infrastructures, platforms, softwares, and storage space provided by cloud service providers, rather than having IT departments establish their own medical data centers, to reduce the costs of building, updating softwares, and equipping hardware, as well as maintenance and administration of the system.

(2) Medical information resource sharing and high ductility. Cloud technology reaches the goal of connecting documents from various sources, which in terms makes sharing data, and exchanging information instantly. In addition, it can also integrate information concerning services from various suppliers. Therefore, patients enjoy cross-platform medical services, such as remote care and family physicians.

(3) Resource dynamic extensibility. PHR is limited by the number of users, as it has to support the sudden increase of users. Cloud services are be flexible to scale up and down and meet the expectation of hospitals to expand the medical information systems.

(4) Enhancing the flexibility. In clouds, authorized users can always access the medical files, and when one of the users modifies a file, it will be updated automatically. For the integration of medical records, it offers a quick and complete access to information at any place with internet connection.

1.2 Research Motivation

Making patients be the center of a PHR management framework helps the users manage their own health records. Besides, putting PHR on a cloud management has the advantages of sharing relevant information efficiently, reducing the waste of health care resources, allowing patients to control their own medical records, lowering setup and administrative costs. Service providers provide various Infrastructures such as a Service

(IaaS), Platform as a service (PaaS), and Software as a Service (SaaS), allowing health care institutions or agencies to reduce the administrative burden and to focus on providing a higher quality of medical care.

The most common PHR services currently employed are the myPHR and other related service systems provided by the American Health Information Management Association. It is a combination of portable devices with Wi-Fi technology, allowing people to exchange information when storing personal health records in storage devices such as smart cards, mobile phones, flash drives, and computers. PHR combined with the function of the internet services helps people manage their own health information (AHIMA, e-HIM Personal Health Record Work Group, 2005). Two other cloud platform providers, Google and Microsoft, provide their PHR services on the cloud, namely Google Health [14] and Microsoft HealthVault [15]. Taking Google launched Google Health medical record service as an example, US users not only can record their personal medical information, but can also connect with the major pharmacies and clinics, making it more easily to get medical records through this service on the internet.

PHR services are established to improve illness management and to enhance personal health of the patients. However, the users also concern about security and privacy of PHR systems. Health Insurance Portability and Accountability Act [7, 10, 11] addressed the PHR privacy and security law protection in 1996, but did not involve in all issues. Especially, HIPAA was only applied to the covered entities, including health plans, healthcare clearinghouses, and healthcare providers. Emerging cloud-based PHR service providers like Dossia, Microsoft, and Google were not the covered entities.

Moreover, the security mechanism of information systems has to work in an effectively confident and appropriate way, when it comes to the security of cloud computing. In response to the possibility of a security research of a cloud-based PHR, it not only requires the PHR service providers to encrypt patients' medical data, but also let patients decide who can access their PHR medical records.

Data must be protected in cloud; therefore, the user information stored in the cloud has to be encrypted in order to strengthen the security of documents and prevent user's information from being revealed. Importing PHR in cloud services must be done carefully for the PHR privacy and the system safety. The PHR can provide more safety protection functions than traditional paper medical records do, such as password protection and record trace. The PHR is stored in the cloud service, instead of building a real system for saving medical records, which makes the users lose the direct control of PHR. Besides, there are many security threats to cloud environments, such as the inadequacy in the verification of user identity, the abuse of cloud computing to illegal act topics, malicious acts carried out by the internal staff of the cloud service providers cloud service providers' internal staff, and shared environments caused by the information or service being stolen. Above issues were not fully addressed by the HIPPA.

1.3 Research Purpose

Due to the development of the internet, more and more transactions and data transfers are taking place through public networks. Therefore, how to ensure the security of transmitted data has become an important issue. Constructing PHR in a cloud environment has the advantages of lowering management costs, effective sharing of information, dynamic expansion of resources, and improved system ductility, etc. However, without the ability to transfer information in a safe way, the system would not be able to work effectively. In order to solve above problems, it is necessary to have a safe and patient-based PHR encryption system under cloud environments. Traditional cryptographic systems offered a secure transmission method, but could not be fully replicated in above environments.

The oblivious transfer protocol is an important fundamental encryption system. Although many studies have been proposed to improve the oblivious transfer data encryption technology, [13-15], most of which focus on the structure involving a single owner. Yet, none of them have given a serious application consideration to implement PHR implement the technology in and modified in the cloud environment. Besides, cloud-based PHR can be accessed by multiple users such as, doctors, nurses, users and family members, and each users one has an access authority according to the hierarchy. Therefore, in order to solve the above problems, a PHR management system in the cloud environment is proposed in this study. This system can safely transmit PHR information among of multi-users as an oblivious transfer mechanism based on the bilinear pairing function to ensure the security when transmitting PHR information is also proposed. The main concept is to transfer secret message in PHR under the multi-user cloud environment and let the receiver choose which message to receive.

According to the modified oblivious transfer protocol proposed in this paper, the users can communicate with the server to acquire data and, on top of that, protect the privacy and safety of users and servers. Through the security analysis, it is proven that the proposed scheme can attain the goals of both efficiency and safety.

Chapter 2—Related work

2.1 Introduction of PHR

PHR is an electronic application of medical health information management [16], where lives are stored in accordance to a formal standard as specified by the HIPAA and HL7 that were adopted by health care providers. It provides user-related physiological conditions, medication information, medical diagnosis, test results and other health information [17]. According to the definition given by AHIMA, PHR mainly records health information relevant to the users. Such information can be a reference when there is a need for the users to receive medical treatment. Being portable and flexible, PHR can integrate medical certificates and a user's personal records of daily life. [7]. PHR integrates users' health-related data such as dietary habits, exercising records, physiological information, genetic disorders, and other information, making it more convenient to get a full understanding of the health status users as well as provide useful information for medical research [18]. In addition, PHR has the following features [19].

1. Users can manage their own PHR.
2. PHR contains records of lifelong health care information.
3. PHR is not limited by time and space.
4. PHR can be transferred in a private and secure way.
5. Owners of PHR can clearly know if the PHR has been accessed or modified.
6. Health records from medical institutions can also be collected and integrated into PHR, as shown in Fig. 2.1.

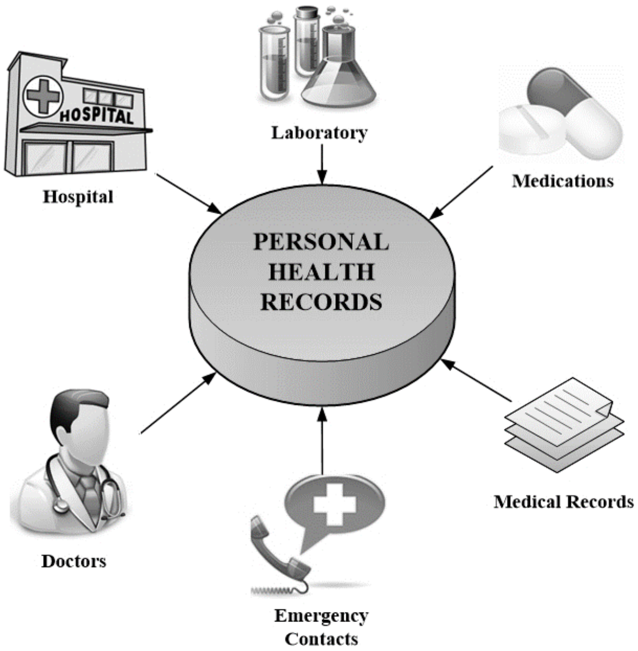

Figure 2.1 : PHR Construction

PHR has following advantages. (1) Users can learn more health information and knowledge from it to achieve self-health management and then improve personal health [21]. (2) PHR helps reduce communication barriers between the users and care takers. (3) Caretakers can get detailed information of the users' biological conditions to provide more comprehensive medical services immediately.

In 2009, HITECH (The Health Information Technology for Economic and Clinical Health Act) strengthened the security and privacy of medical information previously provided by the Health Insurance Portability and Accountability Act [20].

The system manages PHR, which combines with different sources of health information, including patients' measurements (blood pressure, diet, exercise habits, etc.), the physician's records (medical records, doctor, etc.), hospital and laboratory records (ECG, medical imaging, etc.), legal documents, power of attorney, and insurance documents. In addition, PHR also contains medical reference related to the treatment, drug uses, and other non-medical information, etc. Some of PHRs are acquired from the electronic medical record (EMR) database. Nevertheless, PHR is not as rigorous as EMR, because it is not non-repudiation and integrity. However, PHR should be stored in a safe and private environment for the implementation and needs permissions to read data. More importantly, PHR will not replace any medical records. PHR is adequate for personal health caring and treatment plans that a file user can communicate with doctors, nurses or other caretakers in a more efficient way.

PHR has become a connection to patients with medical crews to save time and cost of caring. PHR also integrates the people being cared, such as the health information between parents and children, and lets the users maintain and update the system by themselves. Thus, it is necessary to widely promote PHR. PHR also has the function to remind people, such as providing medication reminders, recognizing errors that may happen in programs and services for improving patients' safety, and allowing patients quickly obtaining important test results to improve communication and interaction between patients and clinicians. PHR also allows patients to get immediate update of care plans to improve the quality of caring. PHR provides continuous and extensive care and also becomes a useful tool when there is a need for patients to communicate with physicians and helps to reduce duplicate and unnecessary testing inspection services. Apart from strict security control which can strengthen personal health information privacy, the users can control their own PHR to make a selective sharing as well. Most important of all, PHR can save more costs, reduce the chances of misdiagnosis, and reduce duplicate testing and services.

In addition to above considerations of medical safety funding, PHR architectures are based on the fundamental assumptions. 1. The complete records are held in a central repository. 2. Each patient retains authority over access to any portion of his/her records. 3. Patients have the right to fully access to PHR and determine access permissions for users as well as remove an expired one. 4. Users can accurately set different access rights of PHR, and doctors can only have the health information of their own patients.

Once patients are referred to another hospital, the new access rights have to be properly transferred to the new physician. 5. The system provides security, privacy and sustained improvement of health management.

PHR can help home care and telemedicine services as well as be offered for medical research. Therefore, PHR needs to be authorized appropriately. PHR includes a lot of private information that the users should decide who can get the information and authorization time to protect the security of information. The PHR system needs to protect not only the information security, but also the security during transportation.

2.3 Cloud Computing

Cloud computing is a concept of the integration of virtualized resources, such as hardware, developing platforms, software services, to offer a flexible resource being used anytime and anywhere through the internet [21, 22]. Cloud computing is demand oriented. Instead of storing data on the user side, users can store data in the cloud server. End users access cloud-based applications through the internet while the software and users' data are stored on servers at a remote location.

These resources can cope with the requirement of being easily changed the load by repeatedly dynamic configuration to allow the optimized use of resources. For the users, the benefits of using this service include obtaining Apps, cost saving, lowering threshold, visual needs to scale to support a sudden increase in network traffic, and eliminating the need for storage of information. Cloud computing services contain three models [23, 24], Fig.2.2.

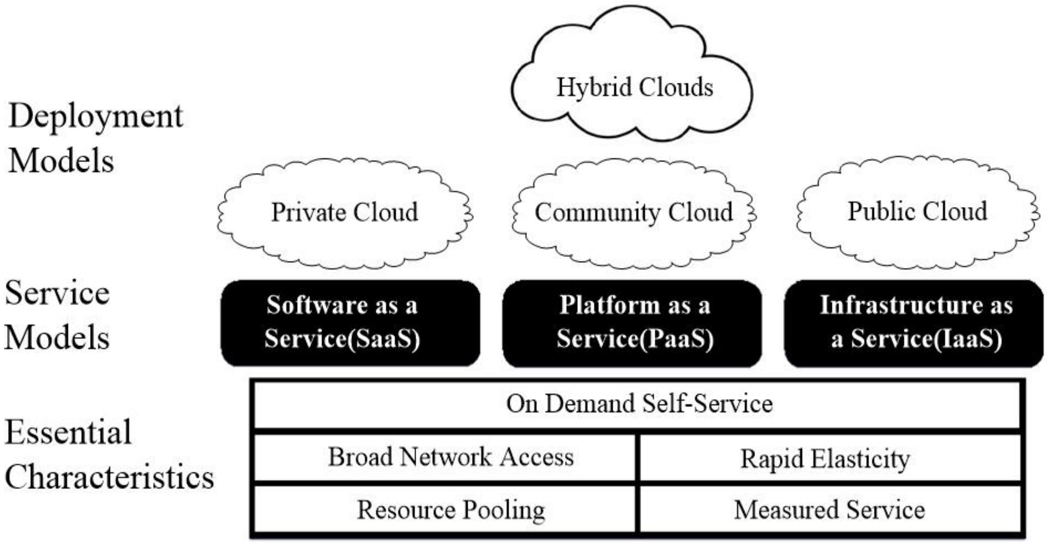

Figure 2.2 : NIST

1. Software as a Service, SaaS. It is a mode providing software through the internet, where manufacturers will deploy unified application software on the cloud server. It is also referred to as "on-demand software", which means customers can use the software according to their actual needs and by the numbers and length of times to pay the manufactures for getting the services on the internet. Offering customers on-line applications on the cloud architecture can be used in a variety of thin client devices.
2. Platform as a Service, PaaS. Manufacturers will open a cloud server platform to users so that the users can deploy their own applications using the programming language themselves, without the complexity of building and maintaining the infrastructure. End users can control and design the applications but are unable to reach the infrastructure.
3. Infrastructure as a Service, IaaS. Manufacturers provide infrastructure (IT systems, databases), which is technically the size of the virtual machine in accordance with the needs of a quick and easy distribution to customers, and then sublet to the users [25].

Cloud computing includes several features, such as using virtualization technology to integrate resource pooling, providing dynamic services rapidly and elastically, on-demand self-service, paying according to usage, connecting to the internet using a variety of platforms, and doing extensive data processing. Resource pooling provides a multi-user application mode, allocating dynamic resources according to the user's needs automatically, and unlimited flexible and fast allocation functions. Measurement services can monitor the usage of resources in order to achieve the automatic control and optimization of cloud systems. Users can participate in cloud computing services anywhere and anytime, reducing the dependence on terminal equipment and information technology.

2.3 Security Issues of the Cloud Environment

The main concept of cloud computing is that users no longer need to actually set up local end storage devices and hardware devices; instead, user data are stored and computed in the cloud system. PHR allows authorized users to access anytime and anywhere [17]. Therefore, PHR is more suitable for the cloud system. Besides, there are also conducive to the implementation of the concept of telemedicine and home care. However, the PHR implemented in the cloud is subject to have the possibility to be exposed in an illegal way [17, 26]; the biggest concerns of PHR are security and stability. The common usage to protect information in cloud computing environments are as followings.

1. Encrypt information before storing the data.
2. Authenticate users’ identities before the users access files
3. Transmit user information through secure delivery methods.
4. User Information can be attached with digital signatures to achieve the purpose of verifying the authenticity of information.

5. Split the first user information processing, then store, and wait until one needs to use the information when conducting the recovery process.

Adopting encryption in the cloud environment has the benefits of strengthening the safety of the procedure of accessing information and ensuring that the encryption key needs to be used when trying to destruct a file. It makes the information not being easily restored or remained in the service provider. The most common way to protect information is to employ the encryption and decryption algorithm in the way that is used in the cloud environment. Information stored in the cloud system needs to be encrypted to avoid undue exposure of users' information. However, the problem is not only about encryption but also about the encryption and decryption keys being stored. In addition, the issues of data backup and recovery mechanism also needs to be taken into account [27]. When a user stores the data in the cloud environment, the cloud system will first encrypt the data first and restore again. When the user wants to read the stored information, cloud will first verify the identity. When the verification is validated, the system will decrypt the data and they offer the decrypted data to the user. Under that circumstance, the encryption key and encrypted data may be stored in the same cloud storage device. When an attack occurs, the data and key may be stolen at the same time, which might lead to data leakage. Besides, a privileged user of internal service providers, such as administrators, may also have the right to access information and decrypt the encrypted information which constitutes a potential risk of leaking the user information. The traditional encryption protocol is not mainly developed for cloud computing. The patient PHR is stored in an outsourcing service provider that the patient may lose control of the sensitive information and also may suffer from the risk of data leakage. Therefore, the purpose of this paper is to ensure the security of PHR and to make PHR flexible enough so that data can be updated steadily and interactively. A more flexible encryption mechanism is required.

2.4 Oblivious Transfer

With the advanced network and communications technology, E-commerce has played a major note in business. People can easily observe the use of the internet or wireless hand-held devices communication equipment to engage in commercial transactions in everyday life. However, it is exposed risk virus infection and hacker attack. Activities of e-commerce and personal privacy are usually the target of attacks. The e-commerce transactions are taking place in the cloud, the parties involved do not have physical contact with each other. Hence the parties involved must follow certain protocols to ensure that the transactions are carried out in a secure manner.

In the application to electronic stock markets, buyers should not reveal the items they bought to prevent the stock speculation. Therefore, apart from mutual identity recognition of the buyer and the server-side, some appropriate measures should be taken to ensure that the communication protocol through the entire transaction process. Oblivious transfer protocols play an important role in the whole process [28-30].

Two parties, the sender and the receiver, are considered in an oblivious transfer protocol. The sender holds a secret message and the receiver tries to get the message transmitted. Through oblivious transfer, the sender doesn’t know whether the receiver gets the secret message or not, and the receiver can only get the desired message, Fig 2.3. The earliest concept of oblivious transfer was first proposed by Rabin in 1981 [31], where which the sender transmitted secret messages to the receiver, and the the receiver receive the message with probability 0.5.

In 1985, Even, Goldreich and Lempel [32] proposed a general structure called 1 out of 2 OT. In the protocol, the sender had two secret messages, m1 and m2, and the receiver could choose to receive only one message at one time. The sender did not know which one was chosen by the receiver. Brassard and Cre’peau [33] expanded the 1 out of 2 OT to 1 out of n OT. In addition, a variety of different types of Oblivious Transfer agreements were proposed, such as Non-Interactive Oblivious Transfer Scheme [34, 35] and Verifiable oblivious transfer protocol [36]. In the t out of n OT, it only had to change the amount of secret message that the sender owned and the receiver obtained; then, it could satisfy both 1 out of n OT and 1 out of 2 OT. The t out of n OT was based on the Chinese remainder theorem. [39]

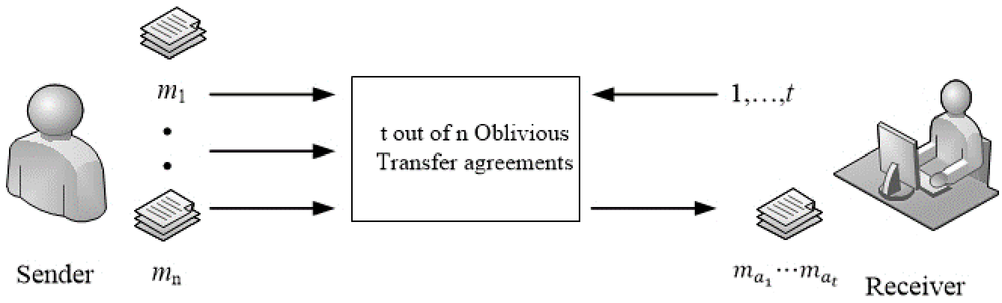

Figure 2.3 : Oblivious Transfer Protocol

An Oblivious Transfer agreement has to meet the following properties.

1. Accuracy. The receiver receives the demanded messages, when both the sander and the receiver follow the protocol.
2. Privacy of the receiver. The sender does not know out which message is chosen to receive by the receiver.
3. Privacy of the sender. The receiver knows only the content of messages that he chooses to receive.

Chapter 3—The Proposed Scheme

A patient-oriented PHR system constructed on clouds, presenting the advantages of reducing costs, sharing information effectively, being scalable, etc, is proposed is this paper. Furthermore, users can use an improved oblivious transfer protocol to communicate with the trust authority. Consequently, it can provide correct information and protect the data from being revealed. The main idea is that a receiver receives information from a sender, then the receiver selects the desired message under the conditions that the sender does not know which message is chosen to receive and the receiver cannot know other messages except the chosen one. Through the improved oblivious transfer protocol, the proposed scheme attains the goal of protecting both the user and server privacy and security as well as provides the access for multi-users.

3.1 Architecture of PHR System in Cloud

Because the PHR system integrates various health information, including daily records, diagnoses from doctors, and statistical records of research centers, it presents the advantages of saving space, budget reduction, adjusting the storage depending on the needs and the capability for patients to record their physical information.

PHR contains useful information for doctors in the diagnosis of chronic illness and also makes telemonitoring more complete. For example, an urgency which can fasten the whole medical process. Constructing PHR in cloud does have many advantages, but the lack of transferring information in a secure way makes the system vulnerable. In order to solve the potential security problems that could faces, an encryption system which is safe, useful and can be adapted to the patient-oriented PHR is called for. In this article, an efficient t-out-of-n oblivious transfer scheme based on bilinear pairings over the elliptic curve is proposed for the PHR system under cloud environments, Figure 3.1.

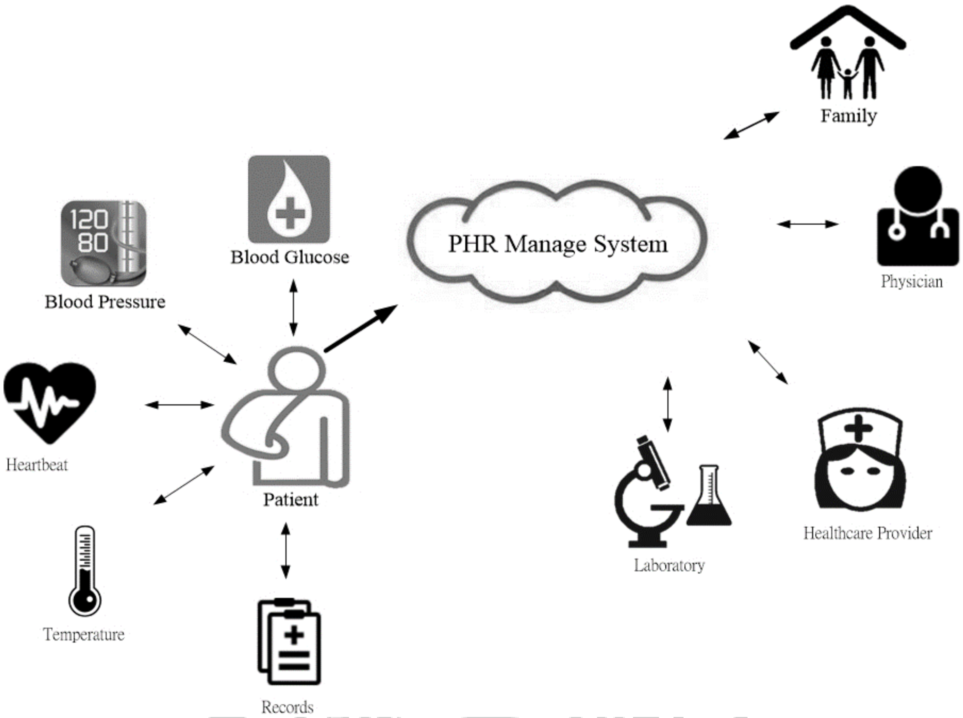

Figure 3.1 : PHR System in Cloud Environment

3.2 A New Oblivious Transfer Protocol

In this section, an ID-based t out of n oblivious transfer protocol based on the bilinear pairings over elliptic curves is proposed. PHR can be transferred in a safe way so that users with the right to access (doctors, nursing staffs, the PHR owner) can to select the desired data when the server-end responding to his request. However, except the user, no one will know what he has chosen through the whole process. Besides, there is also a limitation for the user that, except for the chosen message, no other information can be read. For example, no response will be given when a law clerk asks for the physiological information of a patient.

Table 1 : Notation Defined And Used in Our Scheme

TA	trusted authority of PHR management system
$h(\cdot)$	one-way hash function
$\hat{e}$	a bilinear map function
G_1	an additive group of order q
G_2	a multiplicative group of the same order q
$\oplus$	a bit-wise XOR operation
ID	the identity of an authorized user
m	The personal health record of a patient

A bilinear pairing establishes a correspondence relation between two cyclic groups. It can be applied to an elliptic curve because the dots on the elliptic curve form a group. Weil pairing and Tate pairing are the most common types of bilinear pairing.

Let G_1 and G_2 be two groups of order q for some large prime q, where G_1 is an additive group and G_2 is a multiplicative group. A pairing is a map $\hat{e}: G_1 \times G_1 \rightarrow G_2$ with the following properties.

(1) Bilinear:

Given $P, Q, R \in G_1$, $\hat{e}(P, Q+R)=\hat{e}(P, Q)\hat{e}(P, P+R)$ and $\hat{e}(P+Q, R)=\hat{e}(P, R)\hat{e}(Q, R)$ are acquired. Hence, for any $a, b \in Z_q^*$,

$\hat{e}(aP, bQ)=\hat{e}(abP, Q)=\hat{e}(P, abQ)= \hat{e}(\mathrm{a}P, Q)^b=\hat{e}(P, Q)^{ab}$

where $Z_q=\{0,1,\ldots,q-1\}$; $Z_q^*=\{u\in Z_q \mid \gcd(u, q)=1\}$

(2) Non-degenerate:

There exists a $P\in G_1$ such that $\hat{e}(P, P)\neq 1$

(3) Computable:

If $P, Q \in G_1$, $\hat{e}(P,Q)$ can be efficiently computed,

The identity of the message m_{i} in this protocol can be used by adopting the characteristics of ID-based in bilinear pairings.

3.2.1 Initialization Phase

Step 1. The cloud manager of PHR as a trusted authority (TA) selects a bilinear map ê: $G_1 \times G_1 \rightarrow G_2$ and $P_0 \in G_1$, where G_1 is an additive group of order q, G_2 is a multiplicative group of the same order, and P_0 is a random generator of G_1.

Step 2. TA generates three one-way hash functions H, H_1 and H_2.

H_1: $\{0, 1\}^* \rightarrow G_1$, H_2:$G_2 \rightarrow \{0, 1\}^*$

Step 3. TA selects a random $s_0 \in Z_q^*$ as the private key and computes the public key as $P_{pub} = s_0 P_0$.

Step 4. TA selects a random number R_u and computes the secret key $\acute{R}_u = s_0 * R_u$ for each legitimate user of the system and sends $\acute{R}_u$ and R_u to the user with a secure channel.

Step 5. TA computes $Di = s_0 * Q_i$ for each PHR records $\{m_1, m_2, \ldots, m_n\}$, where $Q_i = H_1(ID_i)$

Step 6. TA selects two large prime numbers a and b, computes N=ab and $\phi(N) = (a-1)(b-1)$, and selects e and d, satisfying $e * d = 1 \bmod \phi(N)$.

3.2.2 Oblivious Transfer Phase

In this phase, a user who has the right to access PHR can acquire the patient's relevant information by the following steps. The user has $\acute{R}_u$ and R_u, which are assigned by TA. The flow chart of the proposed protocol is shown in Figure 3.2.

Step 1. TA computes $V_i = m_i \oplus H_2(\hat{e}(Q_i, P_{pub})^{r_i})$, $X_i = (D_i)^e$, $U_i = r_i * P_0$ and publishes ID_i, V_i, X_i, and U_i for $i = 1 \sim n$

Step 2. The user with permission to access confidential PHR information needs to compute $Wu = h * \acute{R}_u$with everyone's secret key $\acute{R}_u$, in which h = H(K_b, ID_b) and $K_b \in Z_q^*$. The user randomly selects k numbers, $\lambda_1, \lambda_2, \ldots, \lambda_k$, representing k records that the user has selected, computes M_j, where $M_j = \lambda_j^e * X_j$, $j = 1, 2, \ldots, k$, and then sends $M_j = M_1, M_2, \ldots, M_k$, h and W_u to TA.

Step 3. TA can verify the user’s previous signature by checking $\hat{e}(P_{0,}\ W_{u})$ being equal to $\hat{e}(P_{pub},\ h\acute{R}_{u})$. If it is established, he has the permission to access. TA computes$\acute{M}_{j} = M_{j}^{d} \bmod N$ and sends $\acute{M}_{j}$ to the receiver.

Step 4. The user uses λ_{j}^{-1} and M_{j}' to compute D_j

$$M_{j}' * \lambda_{j}^{-1}$$

$$= M_{j}^{d} * \lambda_{j}^{-1} \bmod N$$

$$= (\lambda_{j}^{e} * X_{j})^{d} * \lambda_{j}^{-1} \bmod N$$

$$= \lambda_{j}^{ed} * (D_{j}^{e})^{d} * \lambda_{j}^{-1} \bmod N$$

$$= (\lambda_{j}^{ed} * \lambda_{j}^{-1}) * (D_{j}^{e})^{d} \bmod N$$

$$= \lambda_{j} * \lambda_{j}^{-1} * D_{j} \bmod N$$

$$= D_{j} \bmod N$$

Step 5. The user uses the derived D_j and the public parameters U_j, H_2 and V_j to have XOR. After that, the message of PHR, m_j, is available.

$$V_j \oplus H_2(\hat{e}(D_j, U_j))$$

$$= m_j \oplus H_2(\hat{e}(Q_j, P_{pub})^{rj}) \oplus H_2(\hat{e}(D_j, U_j))$$

$$= m_j \oplus H_2(\hat{e}(Q_j, P_{pub})^{rj}) \oplus H_2(\hat{e}(s_0*Q_j, r_j*P_0))$$

$$= m_j \oplus H_2(\hat{e}(Q_j, P_{pub})^{rj}) \oplus H_2(\hat{e}(Q_j, r_j*P_0)^{s0})$$

$$= m_j \oplus H_2(\hat{e}(Q_j, P_{pub})^{rj}) \oplus H_2(\hat{e}(Q_j, s_0*P_0)^{rj})$$

$$= m_j \oplus H_2(\hat{e}(Q_j, P_{pub})^{rj}) \oplus H_2(\hat{e}(Q_j, P_{pub})^{rj})$$

$$= m_j \oplus 0$$

$$= m_j$$

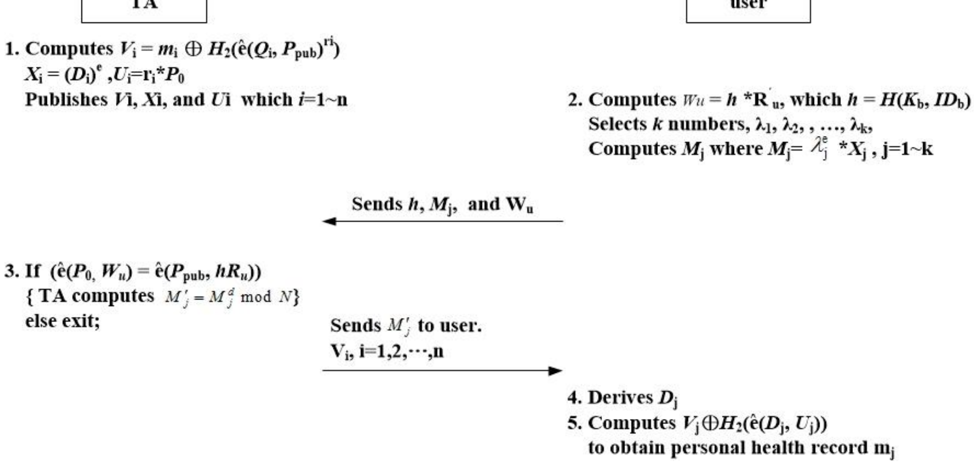
TA
user
1. Computes $V_i = m_i \oplus H_2(\hat{e}(Q_i, P_{pub})^{ri})$
$X_i = (D_i)^e$,$U_i = r_i*P_0$
Publishes Vi, Xi, and Ui which i=1~n
2. Computes $Wu = h * R'_u$, which $h = H(K_b, ID_b)$
Selects k numbers, $\lambda_1, \lambda_2, , \ldots, \lambda_k$,
Computes M_j where $M_j = \lambda_j^e * X_j$, j=1~k
Sends h, M_j, and W_u
3. If $(\hat{e}(P_{0,} W_u) = \hat{e}(P_{pub}, hR_u))$
{ TA computes $M'_j = M_j^d \bmod N$}
else exit;
Sends M'_j to user.
V_i, i=1,2,⋯,n
4. Derives D_j
5. Computes $V_j \oplus H_2(\hat{e}(D_j, U_j))$
to obtain personal health record m_j

Figure 3.2 : The Process of The Encrypt Protocol.

3.3 Example

In this section, a situation of using PHR in a medical environment is illustrated. A variety of data, such as blood pressure, electrocardiography, surgery records, medication administration records, drug allergy, insurance documents, bold sampling, x-ray inspection, blood glucose and body temperature, are from different medical institutions. Those records can be significant as $m_1, m_2, \ldots, m_{10}$ are stored in the cloud server after being encrypted. TA, laboratory research specialist, clinical scientist, care taker and family members all have individual identity ID_1, ID_2, ID_3, ID_4, and ID_5.

Each step has a different function.

Assuming that laboratory research specialist ID_2 is lawfully authorized,

1. TA will calculate the following equations according to ID_2 : $V_2 = m_2 \oplus H_2(\hat{e}(Q_2, P_{pub})^{r_2})$, $X_2 = (D_2)^e$, $U_2=r_2*P_0$.

   Under the circumstance of having the authority to access, the user uses his own key $\acute{R}_{u2}$ to compute W_u = h $*\acute{R}_{u2}$, in which $h = H(K_b, ID_b)$, $K_b \in Z_q^*$. The user selects data $\lambda_1, \lambda_{2,\ldots}, \lambda_5$ from $m_1, m_2, \ldots, m_{10}$ and uses $\lambda_1, \lambda_{2,\ldots}, \lambda_5$ to calculate M_1, $M_2, \ldots, M_5$.

   $M_1=\lambda_1^e*X_1$

   $M_2=\lambda_2^e*X_2$

   $M_3=\lambda_3^e*X_3$

   $M_4=\lambda_4^e*X_4$

   $\mathrm{M_5=\lambda_5^e*X_5}$

   At the end of this step, return M_1~M_5, h and W_u to TA.

2. TA checks to see whether $\hat{e}(P_0, W_u)$ is equal to $\hat{e}(P_0, W_u)$ to identify the authorization of the second user. If the authorization is validates, TA then computes the following entries.

$\acute{M}_1 = M_1^{\mathrm{d}} \bmod N$

$\acute{M}_2 = M_2^{\mathrm{d}} \bmod N$

$\acute{M}_3 = M_3^{\mathrm{d}} \bmod N$

$\acute{M}_4 = M_4^{\mathrm{d}} \bmod N$

$\acute{M}_5 = M_5^{\mathrm{d}} \bmod N$

And Sends $\acute{M}_1 \sim \acute{M}_5$ to the laboratory research specialist ID_2.

3. The laboratory research specialist ID_2 uses $\acute{M}_1, \acute{M}_2, ..., \acute{M}_5$ and known numbers $\lambda_1^{-1}, \lambda_2^{-1}, \dots, \lambda_5^{-1}$ to compute D_1, $D_2, \dots, D_5$. Taking D_1 as the example, the others may be deduced analogically.

$M_1' * \lambda_1^{-1}$ mod N
$= M_1^{\mathrm{d}} \ * \lambda_1^{-1} \bmod N$
$= (\lambda_1^{\mathrm{e}} * X_1)^{\mathrm{d}} * \lambda_1^{-1}$
$= \lambda_1^{ed} * (D_1^{e})^{d} * \lambda_1^{-1}$
$= (\lambda_1^{\mathrm{ed}} * \lambda_1^{-1}) * (D_j^{e})^{d}$
$= \lambda_1 * \lambda_1^{-1} * D_1$
$= D_1$

4. Using D_1, U_1, H_2 and V_1, the file of a patient m_1 can be derive as follows:

$V_1 \oplus H_2(\hat{e}(D_1, U_1))$

$= m_1 \oplus H_2(\hat{e}(Q_1, P_{pub})^{r_1}) \oplus H_2(\hat{e}(D_1, U_1))$

$= m_1 \oplus H_2(\hat{e}(Q_1, P_{pub})^{r_1}) \oplus H_2(\hat{e}(s_0 {*} Q_1, r_1 {*} P_0))$

$= m_1 \oplus H_2(\hat{e}(Q_1, P_{pub})^{r_1}) \oplus H_2(\hat{e}(Q_1, r_1 {*} P_0)^{s_0})$

$= m_1 \oplus H_2(\hat{e}(Q_1, P_{pub})^{r_1}) \oplus H_2(\hat{e}(Q_1, s_0 {*} P_0)^{r_1})$

$= m_1 \oplus H_2(\hat{\mathrm{e}}(\mathrm{Q}_1, \mathrm{P}_{\mathrm{pub}})^{\mathrm{r}_1}) \oplus H_2(\hat{e}(Q_1, P_{pub})^{r_1})$

$= m_1 \oplus 0$

$= m_1$

Chapter 4—Security Analysis

4.1 Security Analysis

4.1.1 Accuracy

In the proposed protocol, TA is the sender and a user is the receiver. A user chooses to receive k files from the files sent by TA.

TA then computes$\acute{M_j} = M_{\mathrm{j}}^{\mathrm{d}} \bmod N$. Based on the difficulty of solving the discrete logarithm, the sender does not know which K files are selected by the user. After the user receives $\acute{M_j}$, j=1,2,…,k, the secret parameter D_j is applied to obtain $V_j \oplus H_2(\hat{e}(D_j, U_j)) = m_j$.

When the transmission is completed, the user (as receiver) correctly acquires k files from TA (as sender), but could not acquire other files. TA, on the other hand, does not know which files were selected by the user. This establishes the accuracy of the protocol.

4.1.2 Sender Privacy

The receiver (user) could acquire the selected t files after completing the protocol. When the user intends to acquire the other n-t files, D_i, i=t+1,…,n needs to be acquired to substitute for $V_i \oplus H_2(\hat{e}(D_i, U_i))$. Based on the difficulty of solving Bilinear Diffie-Hellman (BDH), the user cannot acquire the secret parameters s_0 for D_i. The sender's privacy is thus protected.

4.1.3 Receiver Privacy

The user (as a receiver) selects the desired k data files and transmits the parameters $\mathrm{M_j}$ to TA (as a sender), where $M_j = \lambda_j^e * X_j$, j=1,2,...,k. TA has to derive λ_j from M_j in order to know which k files were requested by the user.

Since λ_j is randomly selected by the user, the TA is not able to derive $\lambda_{j.}$ The receiver’s privacy is protected.

4.2Performance Analysis

We now conduct the performance analysis. The performance of the proposed PHR record management system is compared with that of the models proposed by Zhang et al[41] and chu et al [42]. Based on the fact that the time complexity for solving a 1024-bit discrete logarithm problem is roughly as the same as that of solving a 160-bit bilinear pairing encryption system. The following items are compared. (1) Number of times that messages are delivered. It’s better to have fewer rounds of message exchanges in order to reduce transmission delay. (2) Transmission cost. The PHR transmission is affected by the network qualify and bandwidth at the user end. In order to reduce transmission delay, the volume of data transmitted should be as small as possible.

Table 2 : Comparisons of Transmission Cost and Computation Cost

	Zhang [40]	Chu [41]	Our scheme
Number of runs of message exchanges between the TA and user	3	2	2
Data volume transmitted from the receiving end to the transfer end	(*k* +3)*1024 bits	*k* *1024 bits	(*k* +2)*160 bits
Data volume transmitted from the transfer end to the receiving end	2*n**1024 bits	(*n*+*k*+1)* 1024 bits	(*n*+*k*)* 160 bits

Our scheme requires fewer rounds of message exchanges than the offer two models. Using bilinear pairing encryption system, our scheme, compared with the other two models, demand, the least amount of data transmitted from the user to the TA and from the TA to the user.

Chapter 5 — Conclusion

The healthcare of patients and the elderly is improved by medicine and technologies. The ageing population is currently about 10% in Taiwan, and it is estimated that the elderly population would reach 14% by 2018 to become Ageing Society (Ministry of Health and Welfare). Personal health record (PHR) is therefore utilized for assisting patients or seniors actively concerning about their health conditions, including regular health checks, patient self-measurement, medication safety, and the integration of medical records among hospitals.

The cloud-based patient-centered PHR system proposed in this study presents the following functions of integrating the life-time health information of a patient, including the medical information from different hospitals, acquiring information anywhere and anytime, not being restricted to space and time, a patient being able to keep the complete personal health record (PHR), and a patient being able to decide the accessing users, while physicians could merely access to the served patients. For patient referral, a new access authority is transferred to the new physician. The bilinear pairing is applied to the elliptic curve for the information transmission security, which is protected because of the discrete logarithm and Bilinear Diffie-Hellman (BDH) being hard to destruct.

A user could communicate with the server through the proposed transmission mechanism to acquire the desired vital signs; meanwhile, the user and server privacy and security are guaranteed for the access of a patient and the protection of information security.

Reference

1. L. Kohn, J. Corrigan, M. Donaldson, “Committee on Quality of Health Care in America IoM. Crossing the Quality Chasm,” *Washington, DC: National Ac*ademy P*ress*, 2001.

2. Markle Foundation, “Connecting for health: A public private collaborative,” New York, *The personal health working group final report*; 2003.

3. C. Pagliari, D. Detmer, P. Singleton, “Potential of electronic personal health records,” *British Medical Journal*, Vol.335, No. 7615, pp. 330-333, 2007.

4. Computer Science and Telecommunications Board. National Research Council, “Networking Health: Prescriptions for the Internet,” Washington, DC, *United States: National Academy Press*, 2000.

5. The American Health Information Management Association and The American Medical Informatics Association, “The Value of Personal Health Records: A Joint Position Statement for Consumers of Health Care,” *Journal of AHIMA*, Vol. 78, No. 4, pp.22-24, 2007.

6. P.C. Tang, J.S. Ash, D.W. Bates, J.M. Overhage, D.Z. Sands, “Personal health records: Definitions, benefits, and strategies for overcoming barriers to adoption, ” *Journal of the American Medical Informatics Association*, Vol. 13, Issue 2, pp. 121–126,2006.

7. AHIMA e-HIM Personal Health Record Work Group, “Defining the Personal Health Record,” *Journal of American Health Information Management Association*, 76, No. 6, pp. 24-25, 2005.

8. W. Pratt, K. Unruh, A. Civan, M. M. Skeels, “Personal health information management,” *Communications of the ACM*, Vol. 49, Issue 1, pp.51-55, 2006.

9. M. Li, S. Yu, K. Ren, W. Lou, “Securing Personal Health Records in Cloud

Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-owner Settings", *6th Iternational ICST Conference*, Vol. 50, pp. 89-106, 2010.

10. D. F. Sittig, "Personal health records on the internet: a snapshot of the pioneers at the end of the 20th Century," *International Journal of Medical Informatics*, Vol. 65, Issue 1, pp. 1–6, 2002.

11. W. C. Peter , "Closer to reality：Personal health records represent a step in the right direction for interoperability of healthcare IT systems and accessibility of patient data," *Health Manag Technol.*, Vol. 26, No. 5, pp. 16-18., 2005.

12. P. C. Tang and C. Newcomb, "Informing Patients: A Guide for Providing Patient Health Information," *Journal of American Medical Informatics Association*, Vol. 5, No.6, pp. 563-570, 1998.

13. Markle Foundation, "The Personal Health Working Group Final Report. Connecting for Health: A Public-Private Collaborative," *Markle Foundation*, 2003.

14. Google Health，https://www. ROORle. com/health

15. Microsoft Health Vault，http://www. healthvault. com

16. D.C. Kaelber, A.K. Jha, D. Johnston, B. Middleton, and D.W. Bates, "A research agenda for personal health records," *Journal of the American Medical Informatics Association*, Vol. 15, Issue 6,pp. 729-736, 2008.

17. A. Sunyaev, D. Chornyi, C. Mauro, H. Krcmar "Evaluation Framework for Personal Health Records: Microsoft HealthVault v.s. Google Health," *IEEE Conference on System Sciences, System Sciences (HICSS)*, pp.1-10, 2010.

18. M.I. Kim and K.B. Johnson, "Personal Health Records: Evaluation of Functionality and Utility", *Journal of American Medical Informatics Association*, Vol. 9, pp.171-180, 2002.

19. Working Group on Policies for Electronic Information Sharing between Doctors and Patients, "Connecting Americans to Their Healthcare: Final Report," *Markle*

Foundation, 2004.

20. J.T. Cohen, “HIPAA, The HITECH Act, and How Google May Still Be Able to Distribute, and Profit From, Your Personal Health Info”, *Health Reform Watch,* 2009.
21. L.M. Vaquero, L. Rodero-Merino, J. Caceres, M. Lindner, “A Break in the Clouds: Towards a Cloud Definition,” *ACM SIGCOMM Computer Communication Review*, Vol. 39, No. 1, pp.50-55, 2009.
22. P. Mell and T. Grance, “The NIST Definition of Cloud Computing,” *National Institute of Standards and Technology*, 2011.
23. D. Zissis and D. Lekkas, “Securing e-Government and e-Voting with an open cloud computing architecture,” *Government Information Quarterly*, Vol. 28, Issue 2, pp. 239–251, 2011.
24. C.S. Yoo, “Cloud Computing: Architectural and Policy Implications,” *Review of Industrial Organization*, Vol. 38, Issue 4, pp. 405-421, 2011.
25. L. M. Vaquero, L. Rodero-Merino, D. Morán, “Locking the sky: a survey on IaaS cloud Security,” *Computing*, Vol. 91, Issue 1, pp. 93-118, 2011.
26. B. R. Kandukuri, V. R. Paturi, A. Rakshit, “Cloud Security Issues,” *2009 IEEE International Conference on Services Computing*, pp. 517-520, 2009.
27. A. Parakh and S. Kak, “Online data storage using implicit security,” *Information Sciences*, Vol. 179, No. 19, pp. 3323-3331, 2009.
28. G. D. Crescenzo, T. Malkin, R. Ostrovsky, “Single Database Private Information Retrieval Implies Oblivious Transfer,” *Advances in Cryptology – EUROCRYPT 2000*, Bruges, Belgium, Vol. 1807, pp. 122-138, 2000.
29. J. A. Gara and P. D. MacKenzie, “Concurrent oblivious transfer,” *Proceedings of 41st Symposium on Foundations of Computer Science*, Redondo Beach, California, USA, pp. 314-324, 2000.

30. J. Kilian, “Founding cryptography on oblivious transfer,” *Proceedings of 20th ACM Symposium on Theory of Computing*, Chicago, USA, pp. 20-31, 1988.

31. M.O. Rabin, “How to Exchange Secrets by Oblivious Transfer,” *Technical Report TR-81*, Aiken Computation Lab, Harvard University, 1981.

32. S. Even, O. Goldreich, A. Lempel, “A Randomized Protocol for Signing Contracts,” *Communications of the ACM*, Vol. 28, Issue 6, Pages 637-647, 1985.

33. G. Brassard and C. Cre'peau, “Oblivious Transfer and Privacy Amplification,” *EUROCRYPT'97 Proceedings of the 16th annual international conference on Theory and application of cryptographic techniques*, pp. 334-347, 1997.

34. H. F. Huang, C. C. Chang, and J. S. Yeh, “Enhancement of Non-Interactive Oblivious Transfer Scheme,” *Proceedings of Fourth International Conference on Information and Management Sciences*, pp. 196-199, 2005.

35. Y. Mu, J. Zhang, V. Varadharajan, Y. X. Lin , “Robust Non-Interactive Oblivious Transfer,” *Communications Letters, IEEE*, Vol. 7, No. 4, pp. 153-155, 2003.

36. N.Y. Lee and C.C. Wang, “Verifiable oblivious transfer protocol,” *IEICE Trans. Information and Systems*, Vol. E88-D, No. 12, pp. 2890-2892, 2005.

37. C.K. Chu and W.G. Tzeng, “Efficient k-Out-of-n Oblivious Transfer Schemes with Adaptive and Non-adaptive Queries,” *Proceedings of the Public Key Cryptography（PKC '05)*, Vol. 3386 of LNCS, pp. 172-183**,** 2005.

38. H. Huang and C. Chang, “A New Design for Efficient t-out-n Oblivious Transfer Scheme,” *The 19th International Conference on Advanced Information Networking and Applications*, Vol. 2, pp. 499-502, 2005.

39. C.C. Chang and J.S. Lee, “Robust t-out-of-n Oblivious Transfer Mechanism Based on CRT,” *Journal of Network and Computer Applications*, Vol. 32, Issue 1, pp. 226-235, 2008.

40. J. Zhang and Y. Wang, “Two Provably Secure k-out-of-n Oblivious Transfer

Schemes," *Applied Mathematics and Computation*, Vol. 169, 2005.

41. C.K. Chu and W.G. Tzeng, "Efficient k-out-of-n Oblivious Transfer Schemes with Adaptive and Non-adaptive queries," *PKC 2005 LNCS*, pp. 172-183, 2005.