MOBILE SYSTEMS

Confidentiality Protection of Digital Health Records in Cloud Computing

Shyh-Wei Chen[1] · Dai Lun Chiang[1] · Chia-Hui Liu[2] · Tzer-Shyong Chen[3] · Feipei Lai[1] · Huihui Wang[4] · Wei Wei[5]

Received: 22 June 2015 / Accepted: 28 March 2016 / Published online: 8 April 2016

Abstract Electronic medical records containing confidential information were uploaded to the cloud. The cloud allows medical crews to access and manage the data and integration of medical records easily. This data system provides relevant information to medical personnel and facilitates and improve electronic medical record management and data transmission. A structure of cloud-based and patient-centered personal health record (PHR) is proposed in this study. This technique helps patients to manage their health information, such as appointment date with doctor, health reports, and a completed understanding of their own health conditions. It will create patients a positive attitudes to maintain the health. The patients make decision on their own for thoese whom has access to their records over a specific span of time specified by the patients. Storing data in the cloud environment can reduce costs and enhance the share of information, but the potential threat of information security should be taken into consideration. This study is proposing the cloud-based secure transmission mechanism is suitable for multiple users (like nurse aides, patients, and family members).

Keywords Personal health record · Secure transmission · Privacy preservation · Cloud computing · Oblivious transfer

Introduction

Research background

With the development of information technology, medical records that write down on the paper have been replaced by EMR (Electronic Medical Records) gradually.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' records of a medical institute for editing, revising and exchanging. However the main application still focuses on EMR management and data transformation. Though a lot of hospitals have implemented the EMR and the plan of medical records exchanging construction has already been proposed as well, there is still lack of 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

This article is part of the Topical Collection on *Mobile Systems*

✉ Tzer-Shyong Chen
arden@thu.edu.tw

[1] Department of Biomedical Electronics and Bioinformatics, National Taiwan University, Taipei, Taiwan

[2] Department of Digital Literature and Arts, St. John's University, Taipei, Taiwan

[3] Department of Information Management, Tunghai University University, Taichung, Taiwan

[4] Department of Engineering, Jacksonville University, 2800 University Blvd N, Jacksonville, FL 32211, USA

[5] School of Computer and Engineering, Xi'an University of Technology, Xi'an, China

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 thorough understanding of the therapy that they are taking. 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 to help users can have an active participation with health care supporters and doing 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, the PHR should reach 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 at anytime and anywhere, it also can 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 crews to have a deeper understanding 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.

Because of the well developed of technology, it has become a trend to put 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. 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 of 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 can 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. An authorized user 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.

Research motivation

Making a patients-oriented 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. Regarding 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 focusing 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. The combination of PHR and 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 also connect with the major pharmacies and clinics, making it easier 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 the 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, health care 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 have 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 whom to access their PHR medical records.

To make the data more safety, 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's safety. The PHR can provide more safety protection functions than traditional paper medical records do, such as password protection and record tracing. Since the PHR is stored in the cloud service, instead of building a real system for saving medical records, it is difficult for the users to have 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.

Research purpose

Due to the development of the internet, more and more transactions and data transfers are taking place through public networks. Therefore, ensuring the security when transmitting 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 improving 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 overcome above problems, it is necessary to build 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 situation.

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 them focus on the structure that only involves a single owner. Yet, none of them have given a serious consideration to implement PHR to the technology 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 those problems, a PHR management system in the cloud environment is proposed in this study. This system can safely transmit PHR information among multi-users as an oblivious transfer mechanism based on the bilinear pairing function to ensure the security when transmitting PHR information is also proposed. In addition to the considerations to medical data safety, PHR architectures are based on fundamental assumptions that:

(1) The complete record is held in a central repository
(2) Patients retain authority over complete access to their own records

The main concept is to transfer secret messages 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 ask the server for data and protect the privacy of users and servers. Through the security analysis, it is proven that the proposed scheme can attain the goals of both efficiency and safety.

Related work

Introduction of PHR

PHR is an electronic application of medical health information management [16], where records 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 the health information relevant to users. Such information can be a reference when there is a need for the users to take medical treatment. Being portable and flexible, PHR can integrate medical certificates and a user's personal record of daily life, so that users' can get their own infarction easier [7]. Such as dietary habits, exercising records, physiological information, genetic disorders, and other information, making it more convenient to get a full understanding of users' health status, 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 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 the 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 the PHR, as shown in Fig. 1.

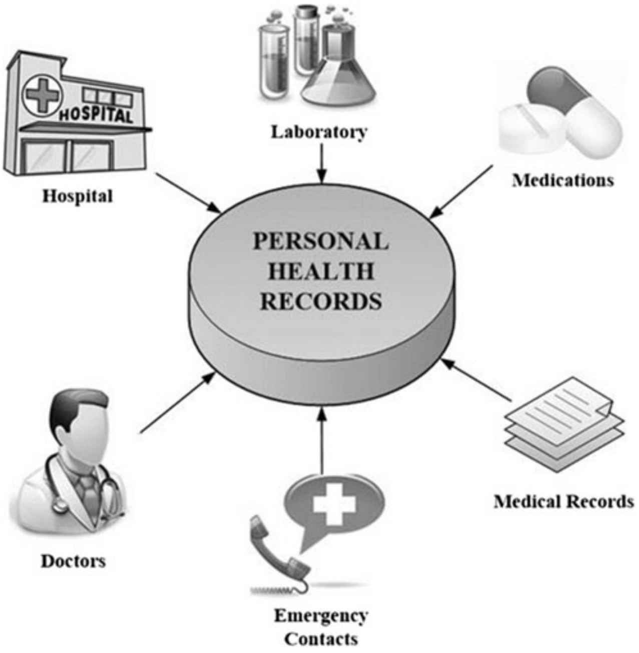


Fig. 1 PHR construction

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 reducing communication barriers between the users and care takers. (3) Caretakers can get detailed information about 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 can combine 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. On top of that, PHR also consists of medical reference related to the treatment, previous drug records, 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 enough 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 between patients and medical crews, which can save time and the 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. In addition, help to remind people is also one if its function, 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 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 the 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 has authority to access any portion of his/her records. 3. Patients have the right to fully access to PHR and determine access permissions of others 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 to have quality improvement, besides it can also 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 information from being stolen. The PHR system needs to protect not only the information security, but also the security during transportation.

There are seven special properties of PHR systems as following.

(1) Scope and Nature of Content: All PHR systems must have consumer health information, personal health journals, and information about benefits and/or providers. Some PHR systems may have clinical information, while some can be disease specific (such as laboratory reports).
(2) Source of Information: PHR data may come from the patient, caregiver, healthcare provider, payer, etc. Some PHR systems may be populated with data by EHRs.
(3) Features and Functions: PHR systems should offer a wide variety of features, including the ability to view personal health data, exchange secure messages with providers, schedule appointments, renew prescriptions, and enter personal health data; other services include

decision support, the ability to transfer data to or from an electronic health record (EHR), and the ability to track and manage health plan benefits and services.

(4) Custodian of the Record: The physical record may be operated by a number of parties, including the consumer or patient, an independent third party, a healthcare provider, an insurance company, or an employer.

(5) Data storage: Data may be stored in a variety of locations, including an Internet-accessible database, provider's EHR, consumer/patient's home computer, portable devices such as smart card or thumb drive, or privately maintained database.

(6) Technical approaches: Current PHR and PHR systems are generally not interoperable (with the exception of the PHRs that "views" into the EHR, and they vary in how they handle security, authentication, and other technical issues.

(7) Party Controlling Access to the Data: While consumers or patients always have access to their own data, they do not always determine who else may access it. For example, PHRs that "views" into a provider's EHR follow access rules set up by the provider. In some cases, consumers do have exclusive control.

Cloud computing

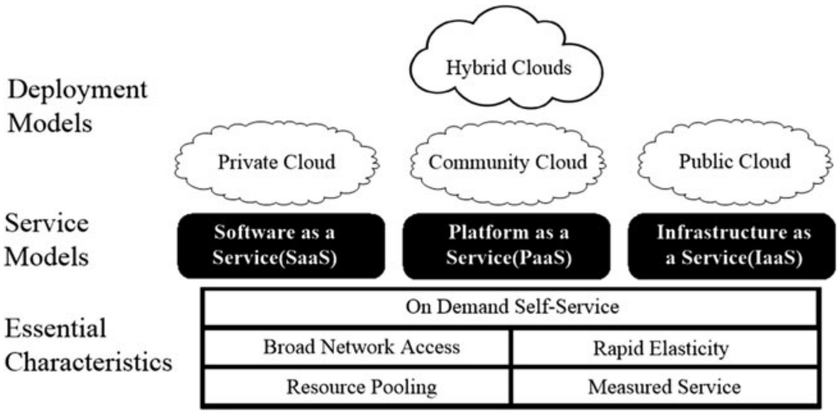
Cloud computing is a concept of integrating virtualized resources, such as hardware, developing platforms, software services, to offer a flexible resource that can be used at anytime and anywhere through the internet [21, 22]. Cloud computing is demand oriented. Instead of storing data on the user side, 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 meet the requirement of being easily changed the load by repeatedly dynamic configuration, so it allows 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.

1. Software as a Service, SaaS. It is a mode of providing software through the internet, where manufacturers will deploy unified application software on the cloud server. It is also be thought of as "on-demand software", which means customers can use the software in accordance with their actual needs and the way of charging is according to the volume of use and length of times. 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 for users so that the users can deploy their own applications by using the programming language, 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 need of quick and easy distribution to customers, and then sublet to the users [25].

Cloud computing contains several features, such as using virtualization technology to integrate resource pooling, providing dynamic services rapidly and elastically, on-demand self-service, paying according to the usage, connecting to the internet by 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 wherever they want, reducing the dependence on terminal equipment and information technology.

Fig. 2 NIST



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, users' data are stored and computed in the cloud system. PHR allows authorized users to access at all times and places [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 most common way to protect information in cloud computing environment are as followings.

1. Encrypting the information before storing the data.
2. Authenticate users' identities before the user access files.
3. Transmitting users' information through secure delivery methods.
4. User Information can be attached with digital signatures to reach the goal 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 when accessing information as well as ensuring 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. Encryption and decryption is widely used to protect information in the cloud environment, for the sake of avoiding undue exposure of users' information. However, the problem is not only about encryption but also the method to safekeeping encryption and decryption keys. In addition, the issues of data backup and recovery mechanism also need to be taken into account [27]. When a user stores the data in the cloud environment, the cloud system will encrypt the data first and restore again. When the user wants to read the stored information, cloud will first verify the identity. After the verification is validated, the system will decrypt the data and then 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, and yet the traditional encryption protocol is not mainly developed for cloud computing. Since 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.

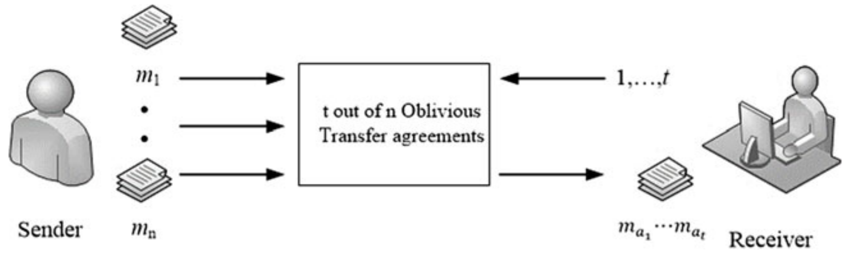
Oblivious transfer

With the advanced network and communications technology, E-commerce has played a major role in commercial activities. 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. E-commerce activities and personal profiles are usually the target for hackers to attack. The e-commerce transactions are taking place on the internet, 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 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 make certain that the communication protocol through the entire transaction process. Precisely because of it, oblivious transfer protocols play an important role in the whole process [28–30].

There are 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 have 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 3. The earliest concept of oblivious transfer was first proposed by Rabin in 1981 [31], which the sender transmitted secret messages to the receiver, and the receiver receive the message with only half the probability.

Fig. 3 Oblivious transfer protocol



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. [37]

An Oblivious Transfer agreement has to meet the following properties.

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

The proposed scheme

A patient-oriented PHR system is constructed on clouds, which presenting the advantages of reducing costs, sharing information effectively, being scalable, etc., is proposed in 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 the receiver selects the desired message under the conditions that the sender cannot know which message is chosen by the receiver, meanwhile the receiver also cannot know the content of other messages except the chosen one. Through the proposed scheme, it attains the goal of protecting both the user and server privacy and security as well as provides the access for multi-users.

Architecture of PHR system in cloud

Because the PHR system integrates a variety of 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 that depends on the need and the capability for patients to record their physical information.

PHR contains useful information for doctors to make a diagnosis for people who suffered from chronic illness and also makes telemonitoring more complete. 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, a safe and useful encryption system can be adapted to the patient-oriented PHR. In this article, an efficient t-out-of-n oblivious transfer scheme based on bilinear

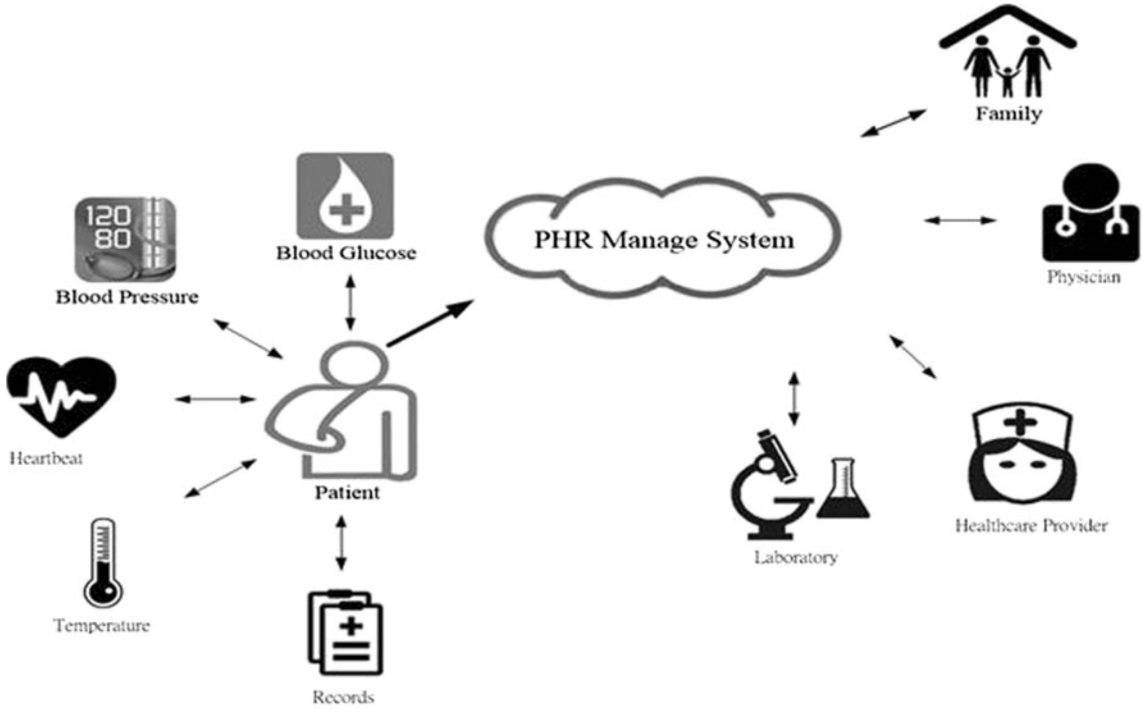


Fig. 4 PHR system in cloud environment

pairings over the elliptic curve is proposed for the PHR system under the cloud environments, Fig. 4.

Integration of PHR with cloud service provides the following benefits:

(1) Reduced cost: Since cloud providers provide the basic infrastructure, platform, software, and storage space, hospitals no longer need to create their own medical data center, cutting back on hardware setup costs, as well as software and hardware upgrade costs. As cloud providers also maintain different IT professionals for Platform as a Service (PaaS), and Software as a Service (SaaS), hospitals only need to select required value-added services, without having to maintain separate IT staff of its own, cutting back on administrative human resource expense.

(2) Medical resource sharing and exchange: Based on internet computation, cloud technology allows quick and spontaneous medical resource sharing and exchange from different sources upon users' connection to cloud servers via the web or the Internet.

(3) Dynamic scalability of resources: PHR is limited by user size but needs to be capable of supporting substantial increase in user numbers. Cloud services are very flexible in scaling and adjusting to demands and can support storage expansion demands for medical information systems when required.

(4) On-demand self-service: In cloud computing, computation resource is a shared pool (such as networks, servers, storage, applications, services, etc.) that can provide quick dynamic deployment to hospitals' demands upon purchase. When demands from multiple users are to be addressed, clouds provide optimal resource utilization that flexibly configures service and storage for users.

(5) Enhanced flexibility: Medical documents stored in cloud servers can be accessed by authorized users anytime. When a user modifies a document, the document is automatically updated on cloud. This represents not only quick and complete data access, but one unrestricted to place, facilitating better medical resource sharing.

(6) Elimination of device limitation: Irrespective of what computer or mobile services such as smart phones, notebooks, or tablets are used, users can enjoy services as long as they can connect to the Internet, making it easier for the use of health management service devices such as blood pressure detectors.

(7) High scalability and service integration: Through cloud computation, services from different providers such as health education, health management, drug safety, exercise and dietary intake analysis, etc., can all be integrated to create a single data center for management, analysis, and services like medical research. Patient transfer service and other patient-related information services like remote healthcare, family physician arrangement etc. can also be integrated and scaled up if required.

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 (doctors, nursing staffs, owner of PHR) can select the desired data when the server-end responds to his request. However, except the user, no one will know what he has chosen through the whole process. Besides, there is another limitation for the user, which is 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.

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 can form a group. Weil pairing and Tate pairing are the most common types of bilinear pairing (Table 1).

Let G1 and G2 be two groups of order q for some large prime q, where G1 is an additive group and G2 is a multiplicative group. A pairing is a map $\hat{e}$: G1 × G1 → G2 with the following properties.

(1) Bilinear:

Given P, Q, R∈G1, $\hat{e}$ (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∈ Z_q^*,

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

$$= \hat{\mathrm{e}}(\mathrm{P},\mathrm{Q})^{\mathrm{ab}}$$

where $Z_q = \{0, 1, \ldots, \text{q-1}\}$; $\mathrm{Z}_\mathrm{q}^* = \{u \in Z_q | \gcd\ (u, q) = 1\}$

(2) Non-degenerate:

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

Table 1 Notation defined and used in our scheme

TA	Trusted authority of PHR management system
h(.)	One-way hash function
ê	A bilinear map function
G1	An additive group of order q
G2	A multiplicative group of the same order q
⊕	A bit-wise XOR operation
ID	The identity of an authorized user
m	The personal health record of a patient

(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.

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 $P0 \in G_1$, where G_1 is an additive group of order q, G_2 is a multiplicative group of the same order, and P0 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 Ru 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 Ru to the user with a secure channel.

Step 5. TA computes Di = s0*Qi for each PHR records $\{m_1, m_2, \ldots, m_n\}$, where Qi = H1($ID_i$)

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

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 Fig. 5.

Step 1. TA computes $V_i = m_i \oplus H_2\ (\hat{e}(Q_i,\ P_{pub})^{ri})$, $X_i = (Di)^e$, $U_i = r_i * P_0$ 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 (Kb, IDb) and $Kb \in Z_q^*$. The user randomly selects k numbers, λ_1, λ_2, …, λ_k, representing k records that the user has selected, computes M_j, where $M_j = \lambda_j^e * X_j$ j = 1,2,…,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 whether $\hat{e}\ (P_{0,} W_u)$ being equal to $\hat{e}\ (P_{pub}, h\ \acute{R}_u)$ or not. 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 thus can use λ_j^{-1} and $\acute{M}_J$ to compute D_j

$$\begin{aligned}
&\acute{M}_J * \lambda_j^{-1} \\
&= M_j^d\ * \lambda_j^{-1} \bmod N \\
&= (\lambda_j^e * X_j)^d * \lambda_j^{-1} \bmod N \\
&= \lambda_j^{ed} * (D_j^e)^d * \lambda_j^{-1} \bmod N \\
&= (\lambda_j^{ed} * \lambda_j^{-1}) * (D_j^e)^d \bmod N \\
&= \lambda_j * \lambda_j^{-1} * D_j \bmod N \\
&= D_j \bmod N
\end{aligned}$$

Step 5. The user uses the derived Dj and the public parameters Uj, H2 and Vj to have XOR. After that, the message of PHR, mj, is available.

$$\begin{aligned}
&Vj \ \oplus\ H_2\left(\hat{e}\left(D_j, U_j\right)\right) \\
&= m_j \oplus H_2\left(\hat{e}\left(Q_j, P_{pub}\right)^{rj}\right) \oplus H_2\left(\hat{e}\left(D_j, U_j\right)\right) \\
&= m_j \oplus H_2\left(\hat{e}\left(Q_j, P_{pub}\right)^{rj}\right) \oplus H_2\left(\hat{e}\left(s_0 * Q_j, r_j * P_0\right)\right) \\
&= m_j \oplus H_2\left(\hat{e}\left(Q_j, P_{pub}\right)^{rj}\right) \oplus H_2\left(\hat{e}\left(Q_j, r_j * P_0\right)^{s0}\right) \\
&= m_j \oplus H_2\left(\hat{e}\left(Q_j, P_{pub}\right)^{rj}\right) \oplus H_2\left(\hat{e}\left(Q_j, s_0 * P_0\right)^{rj}\right) \\
&= m_j \oplus H_2\left(\hat{e}\left(Q_j, P_{pub}\right)^{rj}\right) \oplus H_2\left(\hat{e}\left(Q_j, P_{pub}\right)^{rj}\right) \\
&= m_j \oplus\ 0 \\
&= m_j
\end{aligned}$$

Example

In this section, a situation simulation of implementing PHR in a medical environment is proposed. 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 m1, m2,…, m10, being 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 different function.

Assuming that laboratory research specialist ID_2 is lawfully authorized,

1. TA will calculate the following equations according to ID_2 : $V_2 = m_2 \oplus H_2\ (\hat{e}(Q_2,\ P_{pub})^{r2})$, $X_2 = (D_2)^e$, $U_2 = r_2 * P_0$.

   Under the circumstance of having the authority to access, the user can use his own key $\acute{R}_{u2}$ to compute

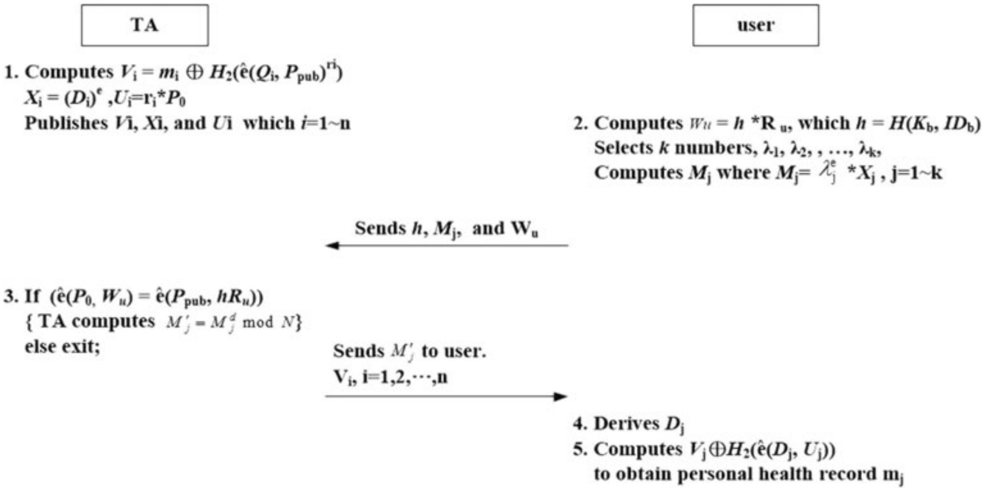

TA
user
1. Computes $V_i = m_i \oplus H_2(\hat{e}(Q_i, P_{pub})^{ri})$
$X_i = (D_i)^e$,U_i=r_i*P_0
Publishes Vi, Xi, and Ui which i=1~n
2. Computes $Wu = h$ *R_u, which $h = H(K_b, ID_b)$
Selects k numbers, $\lambda_1, \lambda_2, , \ldots, \lambda_k$,
Computes M_j where $M_j = \lambda_j^e * X_j$, j=1~k
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

Fig. 5 The process of the encrypt protocol

$W_u = h * \acute{R}_{u2}$, 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, $M_1 = \lambda_1^e * X_1$

$$M_2 = \lambda_2^e * X_2$$
$$M_3 = \lambda_3^e * X_3$$
$$M_4 = \lambda_4^e * X_4$$
$$M_5 = \lambda_5^e * X_5$$

At the end of this step, send back $M_1 \sim M_5$, h and W_u to TA.

2. TA will see whether ê ($P_{0,}$ Wu) is equal to ê ($P_{0,}$ Wu) to identify the authorization of user 2. If the authorization is validates, TA then computes the following entries.

$$\acute{M}_1 = M_1^d \bmod N$$
$$\acute{M}_2 = M_2^d \bmod N$$
$$\acute{M}_3 = M_3^d \bmod N$$
$$\acute{M}_4 = M_4^d \bmod N$$
$$\acute{M}_5 = M_5^d \bmod N$$

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

3. The laboratory research specialist ID_2 uses $\acute{M}_1, \acute{M}_2, \ldots, \acute{M}_5$, and known numbers $\lambda_1^{-1}, \lambda_2^{-1}, \ldots, \lambda_5^{-1}$ to compute $D_1, D_2 \ldots D_{5.}$ Taking D_1 as the example, the others may be deduced analogically.

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

4. Using D1, U1, H2 and V1, the file of a patient m1 can be derive as follows:

$$\begin{aligned} & \mathrm{V1} \oplus \mathrm{H2}\left(\hat{e}(\mathrm{D1}, \mathrm{U1})\right) \\ & = m_1 \oplus H_2\left(\hat{e}(Q_1, P_{pub})^{r1}\right) \oplus H_2\left(\hat{e}(D_1, U_1)\right) \\ & = m_1 \oplus H_2\left(\hat{e}(Q_1, P_{pub})^{r1}\right) \oplus H_2\left(\hat{e}(s_0 * Q_1, r_1 * P_0)\right) \\ & = m_1 \oplus H_2\left(\hat{e}(Q_1, P_{pub})^{r1}\right) \oplus H_2\left(\hat{e}(Q_1, r_1 * P_0)^{s}{}_0\right) \\ & = m_1 \oplus H_2\left(\hat{e}(Q_1, P_{pub})^{r1}\right) \oplus H_2\left(\hat{e}(Q_1, s_0 * P_0)^{r1}\right) \\ & = m_1 \oplus H_2\left(\hat{e}(Q_1, P_{pub})^{r1}\right) \oplus H_2\left(\hat{e}(Q_1, P_{pub}) r_1\right) \\ & = m_1 \oplus \ 0 \\ & = m_1 \end{aligned}$$

Security analysis

Accuracy

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

TA then computes $\acute{M}_j = M_j^d \bmod N$. Based on the difficulty of solving the discrete logarithm, the sender does not know those K files that are selected by the user. After the user receives $\acute{M}$, j = 1,2,…,k, the secret parameter Dj is applied to obtain Vj ⊕ H_2 (ê(D_j,U_j)) = m_j.

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

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, Di, i = t + 1,…,n needs to be acquired to substitute for Vi ⊕ H2 (ê(Di, Ui). Based on the difficulty of solving the problem of Bilinear Diffie-Hellman (BDH), so that the user cannot acquire the secret parameters s_0 for Di. The sender's privacy is thus protected.

Receiver privacy

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

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

Performance 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. [39]. Based on the fact that the time complexity for solving a 1024-bit discrete logarithm problem is roughly as 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).

Our scheme requires fewer rounds of message exchanges than the other 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.

Conclusion

The healthcare of patients and the elders is improved by medicine and technologies. The ageing population is currently about 10 % in Taiwan. Also, 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.

Table 2 Comparisons of transmission cost and computation cost

	Zhang [38]	Chu [39]	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	2n*1024 bits	(n + k + 1)* 1024 bits	(n + k)* 160 bits

The PHR system proposed in this study presents the functions of integrating the life-time health information, including the medical information from different hospitals, acquiring information anywhere and anytime and unrestricted space and time. Furthermore, patients are able to keep the complete personal health record (PHR) and decide the accessing users, while doctor can 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 can 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.

References

1. Kohn, L., Corrigan, J., and Donaldson, M., *Committee on Quality of Health Care in America IoM. Crossing the quality chasm*. National Academy Press, Washington, DC, 2001.
2. Markle Foundation, *Connecting for health: a public private collaborative*. New York, The personal health working group final report, 2003.
3. Pagliari, C., Detmer, D., and Singleton, P., Potential of electronic personal health records. *Br. Med. J.* 335(7615):330–333, 2007.
4. Computer Science and Telecommunications Board, National Research Council, *Networking health: prescriptions for the internet*. National Academy Press, Washington, DC, 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. *J. AHIMA* 78(4):22–24, 2007.
6. Tang, P. C., Ash, J. S., Bates, D. W., Overhage, J. M., and Sands, D. Z., Personal health records: definitions, benefits, and strategies for overcoming barriers to adoption. *J. Am. Med. Inform. Assoc.* 13(2): 121–126, 2006.
7. AHIMA e-HIM Personal Health Record Work Group, Defining the personal health record. *J. Am. Health Inf. Manag. Assoc.* 76(6):24–25, 2005.
8. Pratt, W., Unruh, K., Civan, A., and Skeels, M. M., Personal health information management. *Commun. ACM* 49(1):51–55, 2006.
9. Li, M., Yu, S, Ren, K., Lou, W., Securing personal health records in cloud computing: patient-centric and fine-grained data access control in multi-owner settings, *6th International ICST Conference*, Vol. 50, pp. 89–106, 2010.

10. Sittig, D. F., Personal health records on the internet: a snapshot of the pioneers at the end of the 20th Century. *Int. J. Med. Inform.* 65(1):1–6, 2002.
11. Waegemann, C. P., 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.* 26(5):16–18, 2005.
12. Tang, P. C., and Newcomb, C., Informing patients: a guide for providing patient health information. *J. Am. Med. Inform. Assoc.* 5(6):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. Kaelber, D. C., Jha, A. K., Johnston, D., Middleton, B., and Bates, D. W., A research agenda for personal health records. *J. Am. Med. Inform. Assoc.* 15(6):729–736, 2008.
17. Sunyaev, A., Chornyi, D., Mauro, C., and Kremar, H., *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. Kim, M. I., and Johnson, K. B., Personal health records: evaluation of functionality and utility. *J. Am. Med. Inform. Assoc.* 9:171–180, 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. Cohen, J. T., 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. Vaquero, L. M., Rodero-Merino, L., Caceres, J., and Lindner, M., A break in the clouds: towards a cloud definition. *ACM SIGCOMM Comput. Commun. Rev.* 39(1):50–55, 2009.
22. Mell, P., and Grance, T., *The NIST definition of cloud computing*. National Institute of Standards and Technology, 2011.
23. Zissis, D., and Lekkas, D., Securing e-Government and e-Voting with an open cloud computing architecture. *Gov. Inf. Q.* 28(2):239–251, 2011.
24. Yoo, C. S., Cloud computing: architectural and policy implications. *Rev. Ind. Organ.* 38(4):405–421, 2011.
25. Vaquero, L. M., Rodero-Merino, L., and Morán, D., Locking the sky: a survey on IaaS cloud Security. *Computing* 91(1):93–118, 2011.
26. Kandukuri, B. R., Paturi V. R., Rakshit A., “Cloud Security Issues,” *2009 I.E. International Conference on Services Computing*, pp. 517–520, 2009.
27. Parakh, A., and Kak, S., Online data storage using implicit security. *Inf. Sci.* 179(19):3323–3331, 2009.
28. Crescenzo, G. D., Malkin, T., Ostrovsky, R., Single database private information retrieval implies oblivious transfer. *Advances in Cryptology – EUROCRYPT 2000*, Bruges, Belgium. Vol. 1807, pp. 122–138, 2000.
29. Gara, J. A., and MacKenzie, P. D., Concurrent oblivious transfer. *Proceedings of 41st Symposium on Foundations of Computer Science*, Redondo Beach, California, USA, pp. 314–324, 2000.
30. Kilian, J., Founding cryptography on oblivious transfer. *Proceedings of 20th ACM Symposium on Theory of Computing*, Chicago, USA, pp. 20–31, 1988.
31. Rabin, M. O., How to exchange secrets by oblivious transfer. *Technical Report TR-81*, Aiken Computation Lab, Harvard University, 1981.
32. Even, S., Goldreich, O., and Lempel, A., A randomized protocol for signing contracts. *Commun. ACM* 28(6):637–647, 1985.
33. Brassard, G., and Cre’peau, C., 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. Huang, H. F., Chang, C. C., and Yeh, J. S., Enhancement of non-interactive oblivious transfer scheme. *Proceedings of Fourth International Conference on Information and Management Sciences*, pp. 196–199, 2005.
35. Mu, Y., Zhang, J., Varadharajan, V., and Lin, Y. X., Robust non-interactive oblivious transfer. *IEEE Commun. Lett.* 7(4):153–155, 2003.
36. Lee, N. Y., and Wang, C. C., Verifiable oblivious transfer protocol. *IEICE Trans. Inf. Syst.* E88-D(12):2890–2892, 2005.
37. Chang, C. C., and Lee, J. S., Robust t-out-of-n oblivious transfer mechanism based on CRT. *J. Netw. Comput. Appl.* 32(1):226–235, 2008.
38. Zhang, J., and Wang, Y, Two provably secure k-out-of-n oblivious transfer schemes. Appl. Math. Comput. 169, 2005.
39. Chu, C.-K., and Tzeng, W.-G., Efficient k-out-of-n oblivious transfer schemes with adaptive and non-adaptive queries, *PKC 2005 LNCS*, pp. 172–183, 2005.