J Med Syst (2012) 36:3375–3384
DOI 10.1007/s10916-012-9830-6

ORIGINAL PAPER

A Secure EHR System Based on Hybrid Clouds

Yu-Yi Chen · Jun-Chao Lu · Jinn-Ke Jan

Received: 11 November 2011 / Accepted: 5 February 2012 / Published online: 21 February 2012

Abstract Consequently, application services rendering remote medical services and electronic health record (EHR) have become a hot topic and stimulating increased interest in studying this subject in recent years. Information and communication technologies have been applied to the medical services and healthcare area for a number of years to resolve problems in medical management. Sharing EHR information can provide professional medical programs with consultancy, evaluation, and tracing services can certainly improve accessibility to the public receiving medical services or medical information at remote sites. With the widespread use of EHR, building a secure EHR sharing environment has attracted a lot of attention in both healthcare industry and academic community. Cloud computing paradigm is one of the popular healthIT infrastructures for facilitating EHR sharing and EHR integration. In this paper, we propose an EHR sharing and integration system in healthcare clouds and analyze the arising security and privacy issues in access and management of EHRs.

Keywords Electronic health record · Privacy · Cloud computing · Healthcare

Y.-Y. Chen (✉)
Department of Management Information System,
National Chung Hsing University,
250 Kuo Kuang Road,
402 Taichung, Taiwan, Republic of China
e-mail: chenyuyi@nchu.edu.tw

J.-C. Lu · J.-K. Jan
Department of Computer Science and Engineering,
National Chung Hsing University,
250 Kuo Kuang Road,
402 Taichung, Taiwan, Republic of China
e-mail: phd941@cs.nchu.edu.tw
e-mail: jkjan@cs.nchu.edu.tw

Introduction

Electronic healthcare record systems promise to increase the efficiency and effectiveness of healthcare systems. The purpose of electronic healthcare record services is to provide continuous and uninterrupted healthcare reports and to facilitate the process of administering healthcare to the public through providers of home, community and institutional healthcare service modes.

According to Health Information Management Systems Society's (HIMSS) definition[1], "The Electronic Health Record (EHR) is a longitudinal electronic record of patient health information generated by one or more encounters in any care delivery setting." and it also told "The EHR has the ability to generate a complete record of a clinical patient encounter, as well as supporting other care-related activities directly or indirectly via interface-including evidence-based decision support, quality management, and outcomes reporting." Many different application scenarios are envisaged in electronic healthcare (e-health), such as electronic health records [2, 3], medical research, trading intellectual property [4], and some prototype system [5–7].

A common adopted some form of electronic medical record systems is to store medical records in centralized databases, which build the core concept of a centrally managed healthcare telematics infrastructure. However, cost and poor usability have been cited as the biggest obstacles to adoption of EHR systems [8]. The costs of EHR system depending on what's included, how robust the system is, and how many providers use it. Moreover, an EHR is generated and maintained only within an institution, such as a hospital, integrated delivery network, clinic, or physician office. An EHR is not a longitudinal record of all care provided to the patient in all venues over time. A patient may have many healthcare providers, including primary care physicians, specialists, therapists, and other medical practitioners. Currently, each provider or institution typically has its own database.

However, the aim of EHRs is to the sharing of patients' medical record separate among medical institutions through the Internet. Sharing information between healthcare practitioners across administrative boundaries is translated to sharing information between EHR systems. It can let every doctor making the proper diagnosis and treatment with comprehensive information for a patient in any medical institution.

All EHR system must have a proper security and privacy framework and mechanisms since the disclosure of health data may have severe consequences especially for patients [9, 10]. Modern information technology is increasingly used in healthcare with the goal to improve and enhance medical services and to reduce costs. With the rapid development of Internet and cloud computing technologies, integration of IT services with cloud computing has become an emerging researching topic. Cloud computing paradigm is one of the infrastructures for facilitating EHR sharing and EHR integration. The cloud computing infrastructures delivers information technology as services, by enabling the renting of software, computing power and storage. It provides an attractive IT platform to cut down the cost of EHR systems in terms of both ownership and IT maintenance burdens for many medical practices. The United States National Standards for Information Technology (NIST) defines cloud computing as a model for enabling convenient, on-demand network access to a shared pool of configurable resources that can be rapidly provisioned and released with minimal management effort or service provider interaction. Today, cloud computing is important cornerstones to streamline healthcare whether it is for maintaining health records, monitoring of patients, managing diseases and cares more efficiently and effectively, or collaboration with peers and analysis of data. For the site authentication between cloud, the authentication function can be deployed by one of the standard function such as OAuth, WS-Security and WS-Federation.

The requirements of cloud EHR system [9]

- Ownership of information

  Establishing the ownership of the information is necessary for protection against unauthorized access or misuse of patient's medical information.
- Authenticity and Authentication

  Authenticity in general refers to the truthfulness of origins, attributions, commitments, and intentions. Authentication is the act of establishing or confirming claims made by or about the subject are true and authentic.
- Non-repudiation

  Non-repudiation implies one's intention to fulfill its obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction.
- Patient consent and authorization

  Patient can allow or deny sharing their information with other healthcare practitioners or Care Delivery Organization (CDOs).
- Integrity and confidentiality of data

  Integrity means preserving the accuracy and consistency of data. In the health care system, it refers to the fact that data has not been tampered by unauthorized use.
- Availability and utility

  For any EHR system to serve its purpose, the information must be available when it is needed. This means that the computing systems used for storing and processing the EHR data, the security controls used for protecting it, and the communication channels used for accessing it must be functioning correctly.
- Audit and archiving

  Audit means recording user activities of the healthcare system in chronological order, such as maintaining a log of every access to and modification of data. Archiving means that moving healthcare information to off-line storage in a way that ensures the possibility of restoring them to on-line storage whenever it is needed without the loss of information. [10]

How to develop EHR cloud

In healthcare application scenarios, data confidentiality is not only a security/privacy issue, but also the juristic concerns. The use and disclosure of protected health information should meet the requirements of Health Insurance Portability and Accountability Act (HIPAA) [11], and keeping user's data confidential against the storage servers. Recently, researches on the healthcare focus on the resource sharing on the cloud for providing more convenient lifelong personal health care services. A medical center who stores millions of healthcare medical records in the cloud would like to take advantage of the abundant resources that the cloud provides for efficiency and economy. But, they must to keep the data contents confidentiality on the cloud to meet the policy admitted by HIPAA.

However, those healthcare application scenarios face a dilemma, while medical records needs to be protected, preferably using cryptographic techniques, but it must be instantaneously available in emergency situations. HIPAA regulations are widely adopted by healthcare practitioners in the United States, by default allowing healthcare providers to share clinical information without the individual's explicit permission for treatment, payment and healthcare operations. [12] The emergency situation in EHR system represents an exception to the normal operation [13, 14], the health care provider in an emergency situation should be able to decrypt any data for the patient, even if he has no ordinary access rights. Availability of data is more important than confidentiality and crucial data must be made available in an emergency situation to any clinicians, irrespective of the employed data protection model.

In tradition EHR system, the patients' data translation and exchanging is complex between different hospitals. It is not conducive to patients who need emergency medical service. The cloud computing is suitable for emergency situations. Cloud computing provides a number of advantages to facilitate information sharing. By sharing the same underlying infrastructure, finding and accessing to patients' data potentially can be simplified and performance optimized.

In our scheme, the healthcare cloud ecosystem will be constructed by hospitals and cloud providers as shown in Fig. 1. Some large hospital can construct its own private cloud environment. The patient's medical data such as prescriptions, testing data, pathology data, and nursing charts are stored both in hospital's private cloud and public healthcare cloud provider. Within this kind of cloud environment, the cross hospital access is an important issue between the request-hospital and the owner-hospital.

We also set up a mechanism to make sure the ownership of medical record is protected in the scheme in normal and emergency situation. The patient's data is encrypted is the system. In the normal situation, the hospital or clinic needs to notify the data owner before the accessing of patient's data. In emergency situation, the accessing can be audited by the third party auditor.

The data format

For the data confidentiality, each medical record *file* is encrypted by an individual content key *cK* using a symmetric encryption scheme. The encrypted medical record *Mfile* is also comprised the special emergency licenses. The medical record *Mfile's* corresponding license is *eACL*. The license *eACL* contents the patient *uID*, the file identifier *cID*, usage rights that are directly determined by the security and privacy policies *uRight* and the content key *cK* which are encrypted patient's public key e_i.

For the emergency situation, the encrypted medical record *Mfile* must be instantaneously available in emergency situations. In this design, each medical record is combined with emergency licenses, which travels alongside the medical record. This license contains an emergency key that can be used for accessing the encrypted data, even if a party does not have explicit access permissions. It is deployed in conjunction with a secure audit logging facility by the third party auditor. The data format as following in Fig. 2.

The system operations

In our scheme, we assume that the system is composed of the following parts: New Electronic Medical Record Creation, Electronic Medical Record Access, and Emergency Electronic Medical Record Access. In the New Electronic Medical Record Creation, the data owner created the new medical record for the patient. This file will be encrypted as *Mfile* and generated the corresponding license *eACL* and be stored in the Cloud environment. The Electronic Medical Record Access is divided into two types: In the A-type, the electronic medical record is accessed by the data owner. It can get the data directly from its private cloud or from public cloud. In the B-type of Electronic Medical Record Access, the electronic medical record is access by the other hospital. Only after it gets the permission from the data owner, it can access the data. The Emergency Electronic Medical Record Access, the other hospital can bypass the process for notifying the data owner to decrypt the patient's medical records data at emergency center.

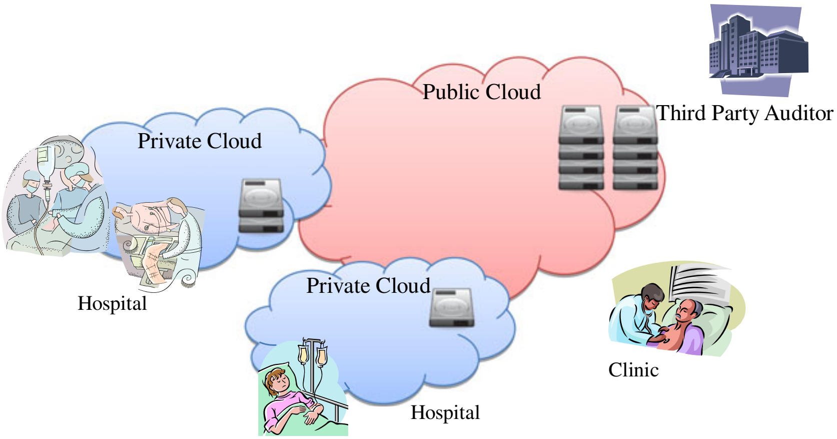


Fig. 1 The concept of EHR cloud

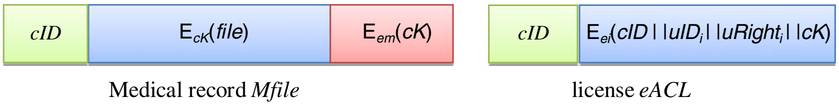


Fig. 2 The data format

Phase 1. Electronic medical record creation

As shown in Fig. 3, the patient's medical record is created by the doctor, it is encrypted by the individual content key *cK*. And the corresponding license *eACL* is created in this phase. For the consideration of the ownership, the license is not only encrypted by the patient’s public key, but also is encrypted with the owner’s key *x* to affirm the data confidentiality.

As the electronic medical record *Mfile* is created by the doctor, the corresponding license $eACL_{ci}$ also needs to be generated. The license $eACL_{ci}$ is encrypted with the patient’s public key e_i accordance with the content identity *cID*, the patient identity *uID*, the access right *uRights*, and the content key *cK*.

$$\begin{aligned} eACL_{ci} &= E_{e_i}(cID||uID_i||uRight_i||cK) \\ &= (cID||uID_i||uRight_i||cK)^{e_i} \bmod N \end{aligned}$$

The corresponding signature $sACL_{ci}$ is generated as follows.

$$SACL_{ci} = S_{sk_H}(H(eACL_{ci}))$$

Moreover, the license $eACL_{ci}$ is double encrypted by the hospital’s key *x*. This double encrypted function is used for affirming the data confidentiality since the reader must get the permission from the medical record owner to get the license. The double encrypted $hACL_{ci}$ is generated as follows.

$$hACL_{ci} = E_x(eACL_{ci})$$

The $hACL_{ci}$ and signature $sACL_{ci}$ are securely transmitted to the Cloud Server following the public cloud’s server-to-server authorization protocol.

Phase 2. Electronic medical record access

As the doctor access the patient’s electronic medical record, the patient provides his smart card to the doctor for decrypt his electronic medical record. The situation is divided into two types as shown in Fig. 4. As the A-type, the electronic medical record is accessed by the medical records Owner. It can directly decrypt the *hACL*. In the B-type, the electronic medical record is access by the doctor in different hospital. The doctor should notify the medical records Owner, and get the permission from medical records Owner before accessing the electronic medical record. The medical record Owner will decrypt *hACL* for the doctor in this session. At the end of this phase, the doctor can get the requiring medical record, moreover the patient and the medical record owner are both involved in the content access phase to avoid any unauthorized access.

(A-type). Private EMR access In this type as shown in Fig. 5, the doctor requests for the electronic health record created by the same hospital. The doctor requests for the patient’s medical files *Mfile* from the hospital’s private cloud, the *Mfile* is automatic gather from the hospital’s database or from the public cloud provider. The encrypted license $hACL_{ci}$ decrypted by the hospital’s key *x*. Then the doctor requests the patient’s smart card to be involved in the decryption process of the license $eACL_{ci}$ for providing further privacy protection.

Step 1. As the patient’s insert his smart card, the smart card automatically generate the split private key [15, 16] as follows :

$$d_i = d_{i1} + d_{i2} \bmod \phi(N)$$

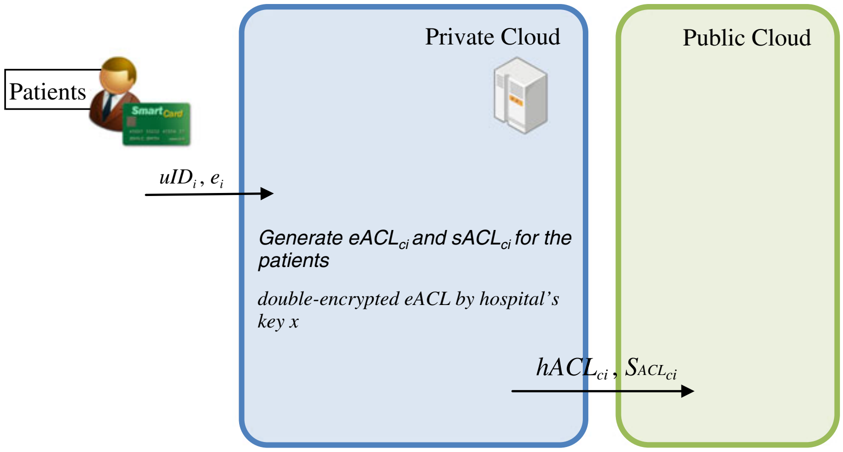

Patients
Smart Card
uID_i, e_i
Private Cloud
Public Cloud
Generate $eACL_{ci}$ and $sACL_{ci}$ for the patients
double-encrypted eACL by hospital’s key x
$hACL_{ci}, S_{ACL_{ci}}$

Fig. 3 Electronic medical record creation

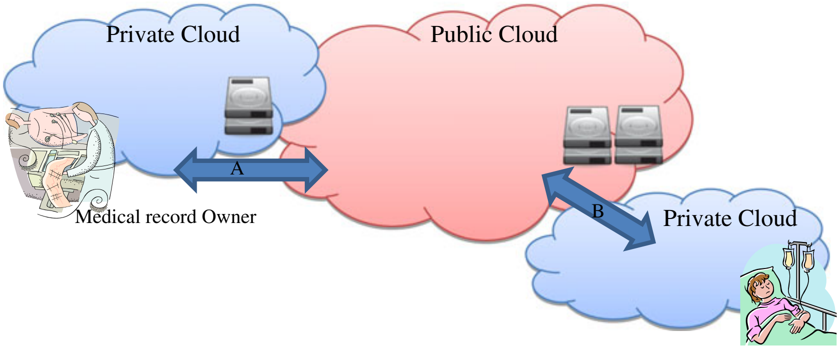


Fig. 4 Electronic medical record access

The patient's identity uID_i and the partial-key d_{i1} are escrowed to the hospital server. The other partial-key d_{i2} is held by the smart card.

Step 2. As the doctor tries to access the patient's electronic medical record by provides the content identity cID. The corresponding signature S_{cID} is generated as follows.

$$ScID = S_{sk_H}(cID, time)$$

Step 3. The public cloud provider stores the S_{cID} for preserving evidence for auditing. The encrypted license $hACL_{ci}$, and the corresponding signature S_{ACLci} are securely transmitted following the public cloud's server-to-server authorization protocol.

Step 4. The encrypted license $hACL_{ci}$ decrypted by the hospital's key x. At the end of this step, the license $eACL_{ci}$, and the corresponding signature S_{ACLci} can be read in the hospital's private cloud.

According to license $eACL_{ci}$, the corresponding signature S_{ACLci} is verified by the server as follows.

$$V_{pk_H}(S_{ACL_{ci}}) \overset{?}{=} H(eACL_{ci})$$

The patient's escrowed partial-key d_{i1} is used for decrypting the license $eACL_{ci}$.

$$\begin{aligned} xACL_{ci} &= D_{d_{i1}}(eACL_{ci}) \\ &= (eACL_{ci})^{d_{i1}} \bmod N \end{aligned}$$

Step 5. The server sends the license $eACL_{ci}$ to the patient's smart card. The partial-key d_{i2} is used for decrypting the license $eACL_{ci}$.

$$\begin{aligned} yACL_{ci} &= D_{di2}(eACL_{ci}) \\ &= (eACL_{ci})^{d_{i2}} \bmod N \end{aligned}$$

Then $yACL$ is transmitted to the server.

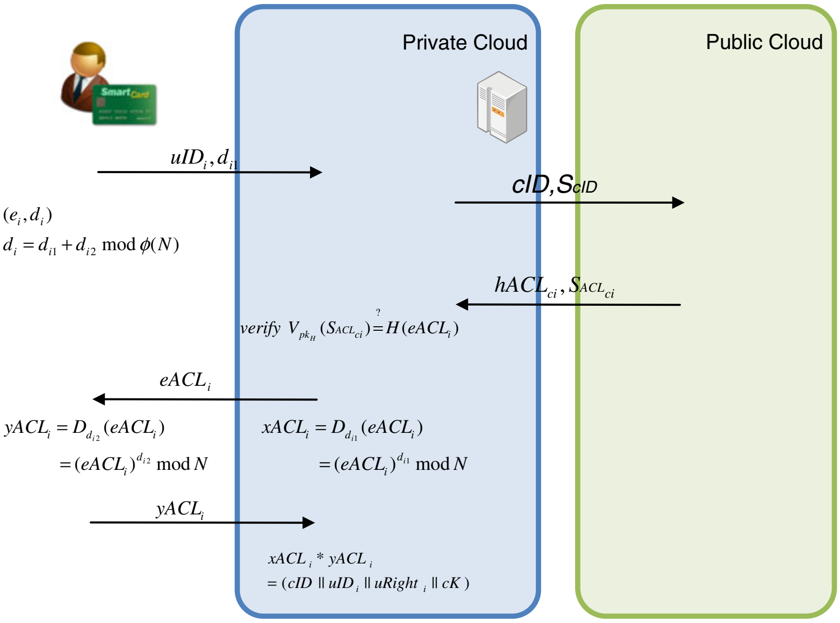

Private Cloud
Public Cloud
Smart Card
uID_i, d_{i1}
cID, S_{cID}
(e_i, d_i)
$d_i = d_{i1} + d_{i2} \bmod \phi(N)$
$hACL_{ci}, S_{ACL_{ci}}$
verify $V_{pk_H}(S_{ACL_{ci}}) \overset{?}{=} H(eACL_i)$
$eACL_i$
$yACL_i = D_{d_{i2}}(eACL_i)$
$= (eACL_i)^{d_{i2}} \bmod N$
$xACL_i = D_{d_{i1}}(eACL_i)$
$= (eACL_i)^{d_{i1}} \bmod N$
$yACL_i$
$xACL_i * yACL_i$
$= (cID \parallel uID_i \parallel uRight_i \parallel cK)$

Fig. 5 (A-type) private EMR access

Step 6. Then the ACL is completely decrypted by the server as follows.

$$
\begin{aligned}
&xACL_{ci} * yACL_{ci}\\
&= (eACL_{ci})^{d_{i1}} * (eACL_{ci})^{d_{i2}} \bmod N\\
&= (eACL_{ci})^{d_{i1}+d_{i2}} \bmod N\\
&= (eACL_{ci})^{d_i} \bmod N\\
&= \left((cID||uID_i||uRight_i||cK)^{ei}\right)^{di} \bmod N\\
&= (cID||uID_i||uRight_i||cK)
\end{aligned}
$$

Using the key cK, the medical record can be decrypted and read by the doctor who has the access right $uRight_i$.

(B-type). Cross hospital EMR access In this type as shown in Fig. 6, the doctor requests for the electronic health record that created by the different hospital. The encrypted content will need to be decrypted by the data owner. It is transmitted to the owner hospital to be decrypted by its secret key x. The patient's smart card is also requested to be involved in the decryption process for providing further privacy protection. Such design ensures that the patient and the medical record owner are both involved in the content access phase to avoid any unauthorized access.

Step 1. As the patient's insert his smart card, the smart card automatically generate the split private key as follows.

$$d_i = d_{i1} + d_{i2} \bmod \phi(N)$$

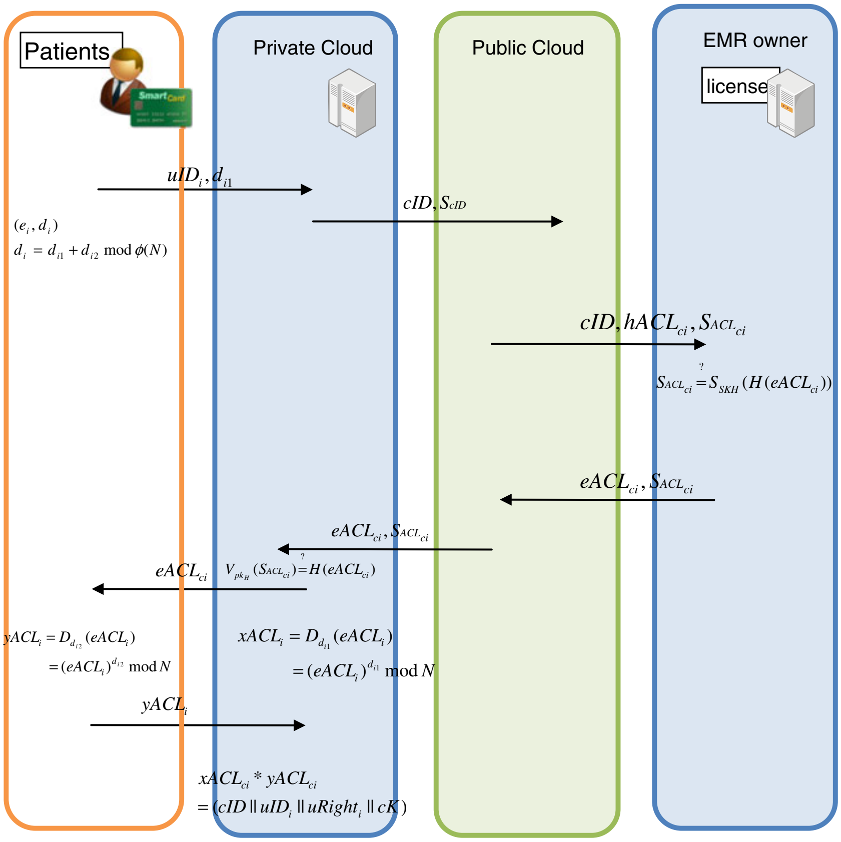
The patient's identity uID_i and the partial-key d_{i1} are escrowed to the hospital server. The other partial-key d_{i2} is held by the smart card.

Step 2. As the doctor requests for the patient's medical information. The content identity cID and the corresponding signature S_{cID} are provided to the public cloud. The corresponding signature S_{cID} is generated as follows.

$$ScID = S_{sk_H}(cID, time)$$

Step 3. The public cloud provider stores the S_{cID} for preserving evidence for auditing. The public cloud server finds the data owner. And the content's encrypted license $hACL_{ci}$ and the corresponding signature S_{ACLci} are securely transmitted to the medical record owner's private cloud following the public cloud's server-to-server authorization protocol. Or the medical record owner can get the license $eACL_{ci}$, and the corresponding signature S_{ACLci} in its hospital's private cloud.

Fig. 6 (B-type) Cross Hospital EMR Access


Patients
Private Cloud
Public Cloud
EMR owner
license
Smart Card
uID_i, d_{i1}
(e_i, d_i)
$d_i = d_{i1} + d_{i2} \bmod \phi(N)$
cID, S_{cID}
$cID, hACL_{ci}, S_{ACL_{ci}}$
$S_{ACL_{ci}} \overset{?}{=} S_{SKH}(H(eACL_{ci}))$
$eACL_{ci}, S_{ACL_{ci}}$
$eACL_{ci}, S_{ACL_{ci}}$
$eACL_{ci}$
$V_{pk_H}(S_{ACL_{ci}}) \overset{?}{=} H(eACL_{ci})$
$yACL_i = D_{d_{i2}}(eACL_i) = (eACL_i)^{d_{i2}} \bmod N$
$xACL_i = D_{d_{i1}}(eACL_i) = (eACL_i)^{d_{i1}} \bmod N$
$yACL_i$
$xACL_{ci} * yACL_{ci} = (cID \| uID_i \| uRight_i \| cK)$

Step 4. The owner-hospital server decrypts the *hACL* by its key *x*, and verifies the license $eACL_{ci}$ with the corresponding signature S_{ACLci} as follows.

$$SACL_{ci} \overset{?}{=} S_{SKH}(H(eACL_{ci}))$$

After, the owner-hospital server sends the license $eACL_{ci}$ and the corresponding signature S_{ACLci} to the public cloud.

Step 5. The license $eACL_{ci}$ and its corresponding signature S_{ACLci} are securely transmitted to the request-hospital server following the public cloud's server-to-server authorization mechanism, and are verified as follows.

$$V_{pk_H}(S_{ACL_{ci}}) \overset{?}{=} H(eACL_{ci})$$

Step 6. In the hospital server, the patient's escrowed partial-key d_{i1} is used for decrypting the license $eACL_{ci}$.

$$\begin{aligned} xACL_{ci} &= D_{d_{i1}}(eACL_{ci}) \\ &= (eACL_{ci})^{d_{i1}} \bmod N \end{aligned}$$

The server sends the license $eACL_{ci}$ to the patient's smart card. The partial-key d_{i2} is used for decrypting the license $eACL_{ci}$.

$$\begin{aligned} yACL_{ci} &= D_{di2}(eACL_{ci}) \\ &= (eACL_{ci})^{d_{i2}} \bmod N \end{aligned}$$

And it transmits *yACL* to the request-hospital server.

Step 7. Then the ACL is completely decrypted on the hospital server as follows.

$$\begin{aligned} & xACL_{ci} * yACL_{ci} \\ &= (eACL_{ci})^{d_{i1}} * (eACL_{ci})^{d_{i2}} \bmod N \\ &= (eACL_{ci})^{d_{i1}+d_{i2}} \bmod N \\ &= (eACL_{ci})^{d_i} \bmod N \\ &= ((cID||uIDi||uRighti||cK)^{ei})^{di} \bmod N \\ &= (cID||uID_i||uRight_i||cK) \end{aligned}$$

Using the key *cK*, the medical record can be decrypted and be read by the doctor on this session who has the access right $uRight_i$. Such design ensures that the patient and the medical record owner are both involved in the content access phase to avoid any unauthorized access.

Phase 3. Emergency access

The use of electronic medical record in the healthcare domain faces a dilemma: while medical data needs to be protected, preferably using cryptographic techniques, it must be instantaneously available in emergency situations. Availability of data is more important than confidentiality and crucial data must be made available in an emergency situation to any clinicians, irrespective of the employed data protection model. Modern protection systems for health data must therefore offer special interfaces for emergency access. We implement emergency access shown in Fig. 7 by providing a special emergency license. This license contains an emergency key that can be used for accessing the encrypted data, even if a party does not have explicit access permissions. The scheme is deployed in conjunction with a secure audit logging facility.

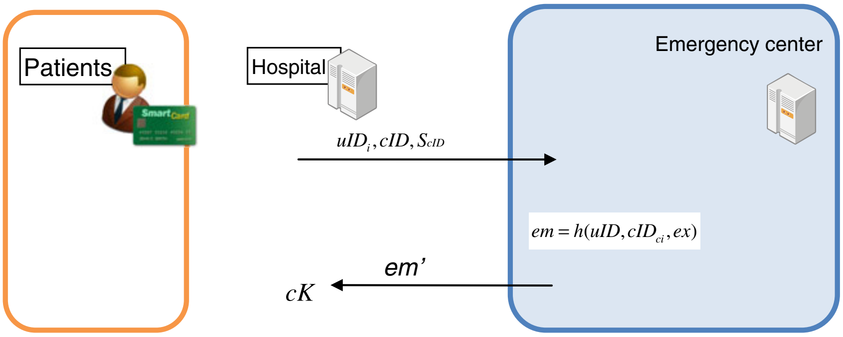
Step 1. As the doctor tries to access the patient's electronic medical record in emergency situations. The doctor needs to provide the patient's identity *uID*, the content identity *cID,* and the access hospital's identity *hID* to the emergency center. The corresponding signature S_{cID} are provided to the public cloud.

Step 2. The Emergency center generates the emergency access key *em* by the patient's identity *uID*, the content identity *cID* and the emergency center's key *ex* as follow.

$$em = h(uID, cID_{ci}, ex)$$

Step 3. The medical record's individual key *cK* can be generated from the emergency licenses, which travels alongside the data. Using the key *cK* and the emergency licenses, the medical record can be read by the doctor even if a party does not have

Fig. 7 Emergency Access



explicit access permissions. At the end of this emergency session.

Analysis

Ownership of information

In our system, the medical information "Manager" is the patient self, not the clinician or laboratory staff. The clinician or laboratory staff is the "Creator" of medical data. "Author" is the person or entity responsible for the content of the information in our system. Therefore, the clinician or physician needs to notify the data owner, the patient and the hospital, before accessing the patient's data. Base on such concept, the patient and the hospital private cloud are both involved in each electronic medical record access in our design. The encrypted medical record can be only decrypted by the content key *ck* embedded in the license $eACL_{ci}$. The license is cooperative decrypted by the patient and the hospital private cloud from step 4 to step 6 of EMR phase. Even in the cross EMR situation, the similar access process is design in the step 4 to step 7 in the cross EMR phase to avoid any unauthorized access or misuse of patient's medical information.

Authenticity and authentication

As EHR is implemented on the cloud, it takes more risk since the data is more accessible to anyone. Base on the modular design of the cloud EHR system, the authentication is an independent issue for EHR cloud. In fact, any appropriate authentication function such as OAuth, WS-Security and WS-Federation can be integrated in our design to solve the private and public cloud authentication. As well as site authentication, any well-designed smart card authentication can be integrated in our scheme for patient authentication. Based on the various smart card authentication schemes [17–23], the authenticity and authentication of user can be confirmed.

Non-repudiation

On the internet, a digital signature is used not only to ensure that a message or document has been electronically signed by the person that purported to sign the document, but also, since a digital signature can only be created by one person, to ensure that a person cannot later deny that they furnished the signature. In our design, each request of patient's medical information is the content identity *cID* combined with its signature $ScID = S_{sk_H}(cID, time)$. The signature S_{cID} can be provided as an auditing evidence in the public cloud. The participating parties cannot falsely deny that a particular event or action has taken place, and evidence is generated, collected, and maintained to enable the settlement of disputes.

Patient consent and authorization

To implement patient consent in a healthcare system, patient may grant rights to users. The digital rights management (DRM) technology is deployed in our design. The access of medical information is limited by the access right *uRight* recorded in the license *ACL*. The restrictive licensing agreement is used for controlling the access of digital materials and its copyright under the client tamper-resistance DRM-application device. The patient can freely set the access right to allow or deny sharing their information with other healthcare parties. It is an easy and efficient design for patient consent and authorization.

Integrity and confidentiality of data

Confidentiality is one of the design goals for many crypto systems and made possible in practice by the techniques of modern cryptography. Confidentiality can be achieved by access control and encryption techniques in EHR systems. It is defined by the International Organization for Standardization (ISO) in ISO-17799 as "ensuring that information is accessible only to those authorized to have access".

In our design, all the medical record is encrypted. The content key *cK* is recorded in the license *ACL*. It can only be decrypted by the patient's private key. The patient's private key will not be delivered to hospital directly. It is randomly split into two parts at each medical record access phase. The partial-key d_{i1} is escrowed to the hospital server. The other partial-key d_{i2} is securely stored in the patient's smart card. The hospital server cannot obtain the complete private key during the decryption process. The first partial-key d_{i1} cannot be extracted from the partially-decrypted-ACL $xACL_{ci}$, which is based on DLP (discrete logarithm problem). DRM-enabled application deposits license *ACL* on the Hospital's private cloud. Only under the client tamper-resistance DRM-application device, the content key *cK* can be used for decrypting the medical record. It assure that only legally DRM-enabled application know the content key *cK*. The content key *cK* expires at the end of the current session. This provides a tamper-resistance feature to the DRM-application. So it will not be compromised further. Based on the process described above, only authorized user can access electronic health record content.

Availability and utility

High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades. Ensuring availability also involves preventing denial-of-service attacks, and preserving utility of EHR data. The cloud environment can provide high availability and utility by the technology of virtualization, resiliency, redundancy, data restoration and disaster recovery. In the emergency situation, an emergency key contains in the emergency license can be used for accessing the encrypted data, even if a party does not have explicit access permissions. The scheme is deployed in conjunction with a secure audit logging facility.

Audit and archiving

Audit means recording user activities of the healthcare system in chronological order, such as maintaining a log of every access to and modification of data.

In our design, cID and the signature S_{cID} are provided to the public cloud for each access request. Those information will be stored by the public cloud for the purpose of auditing. We also implement emergency access by providing a special emergency license. This license contains an emergency key that can be used for accessing the encrypted data, even if a party does not have explicit access permissions. In emergency situation, the hospital's request is also provided to the public cloud and the emergency center for auditing

Archiving means moving healthcare information to offline storage for possibility of restoring whenever it need. With the capability of data restoration and disaster recovery in the cloud environment, the archiving of the encrypted medical license and data can back up by the public and private cloud separated. Moreover, the medical record and the corresponding license are encrypted. The privacy information will be not be leak not even when the data is backed up in an unsecure off-line storage.

Compare with relative paper

Table 1 shows an initial comparison of some relative paper with the Security requirements HER [24]: Confidentiality, Integrity, Availability, Non-repudiation, Protection of patient's privacy, and Patient consent and authorization.

Moreover, in the above relative paper, only our scheme proposes a solution on emergency situation to meet emergency situation. In the normal situation, the data request hospital or clinic needs to notify the data owner before the accessing of patient's data. In emergency situation, the accessing can audit by the third party auditor. A special emergency license can be used for accessing the encrypted data, even if a party does not have explicit access permissions. It used the DRM to against data leaking both on data within an organization, or out on the internet.

Conclusion

The paper actually proposed a method to make authorized doctor can get the patient's medical record on the cloud. This design effectively improves the drawback of current EHR system. In our design, the patient's medical data such as prescriptions, testing data, pathology data, and nursing charts are stored both in hospital's private cloud and public healthcare cloud provider. Within this kind of cloud environment, the cross hospital access is an important issue between the request-hospital and the owner-hospital. We also set up a mechanism to make sure the ownership of the medical record is been protected in the scheme in normal and emergency situation. The patient's data are all encrypted. In the normal situation, the data request hospital or clinic needs to notify the data owner before the accessing

Table 1 Comparison with relative paper

paper	Security Objective					
	Confidentiality	Integrity	Availability	Non-repudiation	Protection of patient's privacy	Patient consent and authorization
Lekkas [25]	O	O	O	O	X	X
Pharow [26]	O	O	O	O	X	X
Kuge [27]	X	X	X	X	X	X
Ahmad [28]	O	O	O	X	X	X
Takeda [29]	O	O	O	X	X	X
Hu [30]	O	O	O	O	X	X
Kalra [31]	O	O	O	O	X	X
Sucurovic [32]	O	X	O	X	X	X
Bonacina [33]	O	O	O	O	X	X
Gobi [34]	O	O	O	O	O	X
Our Scheme	O	O	O	O	O	O

of patient's data. In emergency situation, the accessing can audit by the third party auditor.

Conflict of Interest The authors declare that they have no conflict of interest.

References

1. HIMSS, definition of an electronic health record, http://www.himss.org/ASP/topics_ehr.asp.
2. Rau, H. H, Hsu, C. Y, Lee, Y. L., Chen, W., and Jian, W. S., Developing electronic health records in Taiwan, *IT Professional*, pp. 17–25, March/April, 2010
3. Schabetsberger, T., Ammenwerth, E., Andreatta, S., Gratl, G., Haux, R., Lechleitner, G., Schindelwig, K., Stark, C., Vogl, R., Wilhelmy, I., and Wozak, F., From a paper-based transmission of discharge summaries to electronic communication in health care regions. *Int. J. Med. Inform.* 75(3):209–215, 2006.
4. Hsu, C. Y., Chen, Y. C., Luo, R. C., Rau, H. H., Fan, C. T., Hsiao, B. S., and Chiu, H. W., A resource-sharing platform for trading biomedical intellectual property. *IT Prof.* 12(2):42–49, 2010. doi:10.1109/MITP.2010.48.
5. Li, S. H., Wang, C. Y., Lu, W. H., Lin, Y. Y., and Yen, D., Design and implementation of a Telecare information platform. *J. Med. Syst.*, 2010. doi:10.1007/s10916-010-9625-6.
6. Takemura, T., Araki, K., Arita, K., Suzuki, T., Okamoto, K., Kume, N., Kuroda, T., Takada, A., and Yoshihara, H., Development of fundamental infrastructure for nationwide EHR in Japan. *J. Med. Syst.*, 2011. doi:10.1007/s10916-011-9688-z.
7. Heslop, L., Weeding, S., Dawson, L., Fisher, J., and Howard, A., Implementation issues for mobile-wireless infrastructure and mobile health care computing devices for a hospital ward setting. *J. Med. Syst.* 34(4):509–518, 2010. doi:10.1007/s10916-009-9264-y.
8. Moore, P., Navigating the Tech Maze, Physicians practice. http://www.physicianspractice.com/display/article/1462168/1590647, 2009
9. Zhang, R., and Liu, L., Security models and requirements for healthcare application clouds, *Cloud Computing (CLOUD), 2010 IEEE 3 rd International Conference on*, vol., no., pp. 268-275, 5–10 July 2010, Doi: 10.1109/CLOUD.2010.62
10. Linden, H., Kalra, D., Hasman, A., and Talmon, J., Inter-organization future proof EHR systems-A review of the security and privacy related issues. *Int. J. Med. Inform.* 78:141–160, 2009.
11. 104th United States Congress, Health Insurance Portability and Accountability Act of 1996 (HIPPA), Online at http://aspe.hhs.gov/admnsimp/pl104191.htm, 1996.
12. Pritts, J., and Connr, K., The implementation of e-Consent mechanisms in three countries: Canada, England, and The Netherlands. *SAMHSA report*, http://ihcrp.georgetown.edu/pdfs/prittse-consent.pdf; 2007.
13. Künzi, J., Koster, P., and Petković, M., Emergency access to protected health records. *Stud. Health Technol. Inform.* 150:705–9, 2009.
14. Coskun, N., and Erol, R., An optimization model for locating and sizing emergency medical service stations. *J. Med. Syst.* 34(1):43–49, 2010. doi:10.1007/s10916-008-9214-0.
15. MacKenzie, P., and Reiter, M. K., Networked cryptographic devices resilient to capture. *In Proceedings of the 2001 IEEE Symposium on Security and Privacy*, May 2001, 12–25.
16. MacKenzie, P., and Reiter, M. K., Delegation of cryptographic servers for capture-resilient devices. *In Proceedings of the 2001 ACM Conference on Computer and Communication Security*, November 2001, 10–19
17. Takeda, H., Matsumura, Y., and Kuwata, S., Architecture for networked electronic patient record systems. *Int. J. Med. Inform.* 60(2):161–167, 2000.
18. Chan, A. T. S., Cao, J., Chan, H., and Young, G., A web-enabled framework for smart card application in health services. *Comm. ACM* 44(9):77–82, 2001.
19. Wang, D. W., Liu, D. R., and Chen, Y. C., A mechanism to verify the integrity of computer-based patient records. *J. Chin. Med. Assoc.* 10:71–84, 1999.
20. Yang, Y., Han, X., Bao, F., and Deng, R. H., A smart-card-enabled privacy preserving E-Prescription system. *IEEE Trans. Inf. Technol. Biomed.* 8(1):47–58, 2004.
21. Wu, Z. Y., Chung, Y. F., Lai, F. P., and Chen, T. S., A password-based user authentication scheme for the integrated EPR information system. *J. Med. Syst.*, 2010. doi:10.1007/s10916-010-9527-7.
22. He, D.B., Chen, J.H. and Rui, Z., A more secure authentication scheme for telecare medicine information systems, *J. Med. Syst.*, 10.1007/s10916-011-9658-5, http://dx.doi.org/10.1007/s10916-011-9658-5, 2011
23. Pu, Q., Wang, J., and Zhao, R. Y., Strong authentication scheme for Telecare medicine information systems. *J. Med. Syst.*, 2011. doi:10.1007/s10916-011-9735-9.
24. Farzandipour, M., Sadoughi, F., Ahmadi, M., and Karimi, I., Security requirements and solutions in electronic health records: lessons learned from a comparative study. *J. Med. Syst.* 34:629–642, 2010.
25. Lekkas, D., and Gritzalis, D., Long-term verifiability of the electronic healthcare records' authenticity. *Int. J. Med. Inform.* 76 (5):442–448, 2007. doi:10.1016/j.ijmedinf.2006.09.010.
26. Pharow, P., and Blobel, B., Electronic signatures for long-lasting storage purposes in electronic archives. *Int. J. Med. Inform.* 74 (2):279–287, 2005. doi:10.1016/j.ijmedinf.2004.04.018.
27. Kluge, W. E. H., Secure e-Health: managing risks to patient health data. *Int. J. Med. Inform.* 76(5):402–406, 2007. doi:10.1016/j.ijmedinf.2006.09.003.
28. Ahmad, N., Restrictions on cryptography in India – A case studyof encryption and privacy, *Comput. Law Secur. Rev.*, Volume 25, Issue 2, 2009, Pages 173–180, ISSN 0267–3649, 10.1016/j.clsr.2009.02.001.
29. Takeda, H., Matsumura, Y., Kuwata, S., Nakano, H., Shanmai, J., Qiyan, Z., Yufen, C., Kusuoka, H., and Matsuoka, M., "An assessment of PKI and networked electronic patient record system: lessons learned from real patient data exchange at the platform of OCHIS (Osaka Community Healthcare Information System). *Int. J. Med. Inform.* 73(3):311–316, 2004.
30. Hu, J., Chen, H.H., A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. *Compu. Stand. Interfaces.*, 2009
31. van der Linden, H., Kalra, D., Hasman, A., and Talmon, J., Inter-organizational future proof EHR systems: a review of the security and privacy related issues. *Int. J. Med. Inform.* 78:3, 2009.
32. Sucurovic, S., Implementing security in a distributed web-based EHCR. *Int. J. Med. Inform.* 76(5):491–496, 2007. doi:10.1016/j.ijmedinf.2006.09.017.
33. Bonacina, S., Marceglia, S., Bertoldi, M., and Pinciroli, F., Modelling, designing, and implementing a family-based health record prototype. *Comput. Biol. Med.* 40(6):580–590, 2010. doi:10.1016/j.compbiomed.2010.04.002.
34. Gobi, M., and Vivekanandan, K., A new digital envelope approach for secure electronic medical records., *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, VOL. 9 No.1, January 2009