J Med Syst
DOI 10.1007/s10916-011-9776-0

ORIGINAL PAPER

RBAC-Matrix-Based EMR Right Management System to Improve HIPAA Compliance

Hung-Chang Lee · Shih-Hsin Chang

Received: 30 June 2011 / Accepted: 22 August 2011

Abstract Security control of Electronic Medical Record (EMR) is a mechanism used to manage electronic medical records files and protect sensitive medical records document from information leakage. Researches proposed the Role-Based Access Control(RBAC). However, with the increasing scale of medical institutions, the access control behavior is difficult to have a detailed declaration among roles in RBAC. Furthermore, with the stringent specifications such as the U.S. HIPAA and Canada PIPEDA etc., patients are encouraged to have the right in regulating the access control of his EMR. In response to these problems, we propose an EMR digital rights management system, which is a RBAC-based extension to a matrix organization of medical institutions, known as RBAC-Matrix. With the aim of authorizing the EMR among roles in the organization, RBAC-Matrix also allow patients to be involved in defining access rights of his records. RBAC-Matrix authorizes access control declaration among matrix organizations of medical institutions by using XrML file in association with each EMR. It processes XrML rights declaration file-based authorization of behavior in the two-stage design, called master & servant stage, thus makes the associated EMR to be better protected. RBAC-Matrix will also make medical record file and its associated XrML declaration to two different EMRA(EMR Authorization)roles, namely, the medical records Document Creator (DC) and the medical records Document Right Setting (DRS). Access right setting, determined by the DRS, is cosigned by the patient, thus make the declaration of rights and the use of EMR to comply with HIPAA specifications.

Keywords Electronic medical records · Matrix organization · Smart card · Digital rights management system · XrML

Introduction

With the rapid development of information technology, EMR is likely to have medical records disclosure issues. Some international medical records leakage happens recently. In USA 2011, there is a leakage about hospitalized Hawkeye football players. In Philippines 2009, president Arroyo is leaked information on her breast medical checkup. In Taiwan, artist Selina, due to severe burns in 2010, came news that physicians of other subjects are free to browse the medical records used his position in the medical records privilege [1].

Such well-known facts reflect that EMR document divulgation is overflowing and can cause serious damages. Hence the management security of EMR documents catches highly attention in these few years and it induces the development of EMR right management system.

Electronic medical records management system is a management method to control the EMR documents with security [2]. Medical organizations already practice the methods recently to protect the medical information. But current EMR management systems are designed according to the traditional type of medical organization without consideration for the latest fad or the development of moderm medical organization.

H.-C. Lee (✉) · S.-H. Chang
Department of Information Management, TamKang University,
New Taipei City, Taiwan
e-mail: johnez.lee@gmail.com

Published online: 01 September 2011

Ferraiolo et al. proposed the concept of role-based access control (RBAC) [3]. But it was mostly realized only by dichotomizing the roles of the medical into physician or nurse, or by the formation of the linear type of organization, i.e., classifying staff roles into the vertical top, middle and lower levels. With the increases scale of medical staff organization structure, access control behavior is difficult to be declared among roles in RBAC. Furthermore, with the stringent specifications such as the U.S. HIPAA and Canada PIPEDA etc. [4, 5], patients are encouraged to have the right in regulating the access control of his EMR.

In this paper, we propose an EMR digital rights management system for matrix organization [6] known as RBAC-Matrix. With the aim of authorizing the EMR among roles in the matrix organization of medical institution, RBAC-Matrix also allow patients to be involved in defining access rights of his records. RBAC-Matrix authorizes access control declaration among matrix organizations of medical institutions by using XrML [7–9] file in association with each EMR. It processes XrML rights declaration file-based authorization of behavior from the two-stage design called master & servant stages. With this design, the system can dynamic reflect the role change within each employee and obtain a better efficiency at the same moment.

RBAC-Matrix is based on EMRA(EMR Authorization) role identification through a personnel server authenticated by smartcard. RBAC-Matrix will also make medical record file and its associated XrML declaration to two different EMRA roles, namely, the medical records Document Creator (DC) and the medical records Document Right Setting (DRS). Access right setting, determined by the DRS, is cosigned by the patient, thus make the declaration of rights and the use of EMR to comply with HIPAA specifications.

The rest of this paper is organized as follows. "Related Literature" introduces the related literature. We depicts the proposed scheme RBAC-Matrix and its operation in "The Proposed RBAC-matrix", then discuss and summarize the features of RBAC-Matrix in "Summary and Comparison". Finally, we provide conclusions in "Conclusion".

Related literature

Role-based access control(RBAC)

The concept of Role-based access control first proposed in 1992 by *Ferraiolo* et al. [3], be improved to a formal role-based access control model by *Sandhu* et al. in 1996 [10], and finally redefined into a standard (which is called the NIST RBAC) by the American National Standards Institute [11].

The RBAC four elements

RBAC model, shown in Fig. 1, includes the following four elements, User (U), Roles (R), Permissions (P), and Session (S). The relationship between the elements outlined in the following two points.

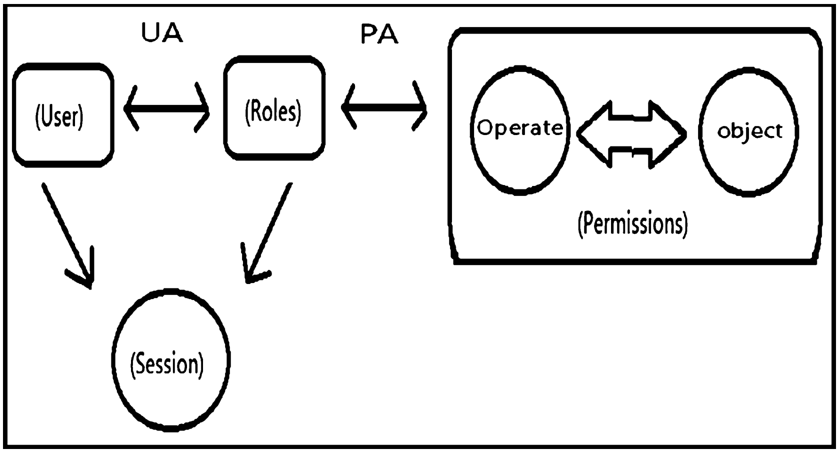
1. User-Role Assignment (UA)

User obtained the role of the mechanism *t* by assignment, each user may be multiple roles, and each role can be assigned to multiple users. The user implement a particular role through the session, and the work of a particular session is participated by multiple roles, but each user can only play a role in a particular session.

2. Role-Permission assignment (PA)

Mechanism grants the role related rights accordance with the needs of different roles, and the user use the related rights accordance with the role of identity. User can easily transfer, add or remove roles, and rights can also be

Fig. 1 RBAC elements diagram



transferred easily between roles, add or remove in the maintenance of the relationship between roles and rights, and between users and roles, making management more simple and flexible.

Five characteristics of RBAC

(1) Least Privilege

Assigning related rights accordance with the role of identity makes authorization simply, hence the authorization will not cause excessive administrative burden. That is users exercise rights accordance with the user's role in a particular session, to avoid abuse of rights.

(2) Separation of Duties

Against the power and responsibility conflict caused by exclusive roles, Separation of Duties avoid the disadvantages caused by two roles operate the same data. This are divided into Static Separation of Duty Relations and Dynamic Separation of Duty Relations. Static Separation of Duty Relations is used to avoid user gets exclusive roles, such as: a medical staff can't have both application and review. Dynamic Separation of Duty Relations is used to limit user can only perform the role of a certain exclusive rights at the same specific point in time, such as: a medical staff can't execute the duties of application and audit at the same time.

(3) Data Abstraction

RBAC allows enterprises to work by semantic manner, such the actual information will be hidden in the operation and users to classify their daily duties to replace the computer's low-level operation. This means use something like natural language to describe the rights declaration provided by users to avoid false authority arising from misunderstandings.

(4) Role Hierarchical

The relationship between roles and roles can be hierarchical, the more upper layer role has more rights, whereas the more layer lower role has basic rights than the general rights, so to simplify license management, and reduce the duplication of rights to assign work.

(5) Ease of Administration

RBAC assigns roles to the user and then digital rights to roles for execution. The user need only adjust the role to vary rights when change position, making the authority setup and management more simple.

Access control structures of RABC

Two proposed access control structures of RABS are called Roles-to-Resources access matrix(RBAC-RR for short) and Hierarchical RBAC (H RBAC-H for short) [12, 13].

In the RBAC-RR structure, an access matrix is built to depict the access rights between roles and resources. The relationship between them is many to many. Each role will have specific access rights to one or more resources. The set of resources and the specific access rights associated with a particular role are expected to be changed infrequently.

As for the RBAC-H structure, the access control is based on the concept of hierarchy and inheritance. In the proposition, assuming role r_1 is said to be a descendant of role r_2, role r_2 inherits all the permissions from role r_1. The rationale for H RBAC is that inheritance property greatly simplifies the task of defining permission relationships. In addition, it can be used in organization that there are many users that share a set of common permissions, cutting across many organizational levels.

States laws and regulations in personal data protection

Privacy personal information draws more and more attention around the world. In this section, we introduce the Health Insurance Portability and Accountability Act, Canada PIPEDA regulations and Australia HRIPA specifications.

America-health insurance portability and accountability act

Health Insurance Portability and Accountability Act (HIPAA) was enacted by the U.S. Congress in 1996, the law against the patient's privacy and the application of medical information, is America's most important medical information law.

Privacy and Security regulations are principal kernels in the HIPAA laws. The Privacy Regulation addresses that the patient has the complete rights to control and understand the use and disclosure of their medical records. However, the consent exceptions of patient's authorization are existed in health business. When the patient is incapacitated, in an emergency treatment, for the purpose of jurisdictions, or in other possible exception situations, the covered EMRs need to be disclosed in the practice of the medical personnel judgment, in the best of his interests, or in life saving of the individual. Patients also have the rights to be told the possible exception situations and how their EMR will be accessed when occurring.

HIPPA's specifications in the signature scheme are as follows [4, 14]:

(1) Patient's understanding

For ensuring that patients have more rights to understand how their EMR will be used and kept, digital signature mechanism is significant to provide the services. To sign the content of signature implies that the patient had known the whole access rule of health information.

(2) Patient's control

Obtaining the permitting consent before use or disclosure of PHI is one objective for patient's control and could be supported by digital signature system. Furthermore, encryption techniques are easier to defend patient's totally control. Only patient holds key and is able to control the authorization for decrypting EMR.

(3) Confidentiality

Encryption makes EMR unreadable for storing and transmitting. Hence, the encryption technique is a suitable way to keep electronic EMR secretly and prevent from revealing without appropriate authorization.

(4) Data integrity

Guarding integrity of health data is an important duty of health organizations, to modify or destroy health information without patient's authorization is prohibited. The encryption technique and the cryptographic checksum can be combined to provide a helpful resolution for ensuring integrity.

(5) Consent exception

Besides the face-to-face EMR authorization of patient, to consider the possible exceptions and solutions without patients' involving is also need. It can be accomplished by the content of digital signature and the key recovery operations.

Canada-personal information protection and electronic documents act

Personal Information Protection and Electronic Documents Act (PIPEDA) became law on 13 April 2000 in Canada [5].

PIPEDA is Canada's bill relating to data privacy, which specification organization in the course of commercial business to collect, use and disclose personal information. The Act contains various provisions to regulate the electronic documents.

Relevant specifications are as follows:

(1) Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

(2) Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

(3) Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

(4) Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

(5) Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of those purposes.

(6) Accuracy

Personal information shall be as accurate, complete, and up-to-date as is necessary for the purposes for which it is to be used.

(7) Safeguards

Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.

(8) Openness

An organization shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

(9) Individual Access

Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

(10) Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

NSW-health records and information privacy act 2002

The Health Records and Information Privacy Act 2002 (or HRIP Act) protects the privacy of health information in NSW [15].

The HRIP Act contains 15 health privacy principles (HPPs) outlining how health information must be collected, stored, used and disclosed. The health privacy principles can be grouped into seven main headings—collection, storage, access & accuracy, use, disclosure, identifiers & anonymity, and transfers & linkage. Relevant specifications are as listed in Table 1

The proposed RBAC-matrix mechanism

RBAC-Matrix is an extension of RBAC to a matrix organization of medical institutions, with the aim of authorizing the EMR among roles in the organization. To improve HIPPA compliance, RBAC-Matrix also allows patients to be involved in defining access rights of his records.

Roles in RBAC-matrix

The user who obtains the role in RBAC-Matrix is authenticated by his smartcard through the personnel database server. To distinguish the meaning of role in different situations, we formally refer the role in RBAC-Matrix as EMRA(EMR Authorization) role, role for short if no ambiguity.

Table 1 HRIP act outlines

Headings	Principles	Specifications
Collection	1. Lawful	When an organization collects your health information, the information must be collected for a lawful purpose. It must also be directly related to the organization's activities and necessary for that purpose.
	2.Relevant	The organization must ensure that your health information is relevant, accurate, up to date and not excessive. The collection should not unreasonably intrude into your personal affairs.
	3.Direct	Your health information must be collected directly from you, unless it is unreasonable or impracticable for the organization to do so.
	4.Open	You must be told why your health information is being collected, what will be done with it, and who else might see it. You must also be told how you can see and correct your health information, and any consequences if you decide not to provide it.
Storage	5.Secure	Your health information must be stored securely, not kept any longer than necessary, and disposed of appropriately. It should be protected from unauthorized access, use or disclosure.
Access & Accuracy	6.Transparent	The organization must provide you with details about what health information they are storing about you, why they are storing it and what rights you have to access it.
	7.Accessible	The organization must allow you to access your health information without unreasonable delay or expense.
	8.Correct	The organization must allow you to update, correct or amend your health information where necessary
	9.Accurate	The organization must make sure that your health information is relevant and accurate before using it.
Use	10. Limited	The organization can only use your health information for the purpose for which it was collected, or a directly related purpose that you would expect. Otherwise they can only use it with your consent (unless one of the exemptions in HPP 10 applies).
Disclosure	11.Limited	The organization can only disclose your health information for the purpose for which it was collected, or a directly related purpose that you would expect. Otherwise they can only disclose it with your consent (unless one of the exemptions in HPP 11 applies).
Identifiers & Anonymity	12.Not identified	An organization can only give you an identification number if it is reasonably necessary to carry out their functions efficiently.
	13.Anonymous	You are entitled to receive health services anonymously, where this is lawful and practicable.
Transfers & Linkage	14.Controlled	Your health information can only be transferred outside New South Wales in accordance with HPP 14.
	15.Authorised	Your health information can only be included in a system to link health records across more than one organization if you expressly consent to this.

There are defined three abstract roles (i.e., DC, DRS, and DU roles) and two databases (i.e., PD and RD), and two server (i.e., RS and DS) in RBAC-Matrix. The functions and corresponding relationships among roles and characters of medical institution as shown below in Fig. 2:

(1) Document Creator (DC) is the one who creates EMR content, which is usually initiated by character of Registration Department (RD) and performed by the Attending Doctor and the specific treatment of the relevant Lab. test content. Document Right Setting (DRS) denotes the one who authorized the document rights, which is performed by Attending Doctor (AD) and approved by the patient. Document User(DU) is the person wants to use the EMR.

(2) The Right Server(RS) has two databases, personnel database(PD), and right database (RD). The personnel database keeps all patient's data and the department and level of all medical personnel. The RD keeps all the document right of the electric medical records.

(3) Document Server(DS) stores all encrypted EMRs.

Smartcard-based authentication

Smartcards are issued to the medical personnel, and patients, which is used as the personal certificate to identify the user's identity in the system. It must present the certificate at any operation stage. There are recorded medical personnel ID(D_{id}), a public key of the medical personnel (EK_{Did}), and a private key of the medical personnel (DK_{Did}) in the medical personnel card. There is recorded patient ID (P_{id}), a public key of the patient (EK_{Pid}), and a private key of the patient (DK_{Pid}) in the patient card.

The personnel database in the RS records all other data, such as the roles, the working departments and level for each medical personnel. With this kind of design can eliminate the action for updating whenever there is a change.

Matrix organization classification

In medical institutes, medical personnel are organized into different departments according their specialized fields, e.g., Cardiology, Internal Medical and Dermatology. Also, there are some special projects that perform task force treatment. Finally, exception handling team deals with the exception handling of EMR when emergency. These classifications define the basis for the access rights setting to be referred. For each organization, there is also a security clearance level which corresponds to characters in medical institution, e.g., Intern, Resident, Chief doctor, Doctor in Charge, and so forth, for the EMR to be accessed.

EMR access rights

Each EMR has a corresponding EMR access rights description which describes for which users what permissions. Permissions are formed by the patient and the Attending Doctor and both have the right to control all authorization. Usually, the authorization process is through the Attending Doctor. However, this authorization, which must go through the patients' understanding and agree, is cosigned by the patient, thus improve the patient's understanding and patient control features in HIPPA.

Each access rights description should include the exception handling team in case of the patient in unconscious, the legal factor, or other possible exceptions. The exception handling team comprise of senior staff, e.g. Chief Information Officer and the Superintendent.

The proposed EMR access rights is done by using XrML [7, 8] file description, which depicts the EMR's permissions for which characters can record what permissions (*read*, *print*, *filling*). The EMR can only be added comment, can't be edited or deleted to prevent the past medical records to be modified, so that the authorized rights are *read, print*, or *comment.*

It will be packaged as Document Usage License with other information and stored in the right database(RD) after DRS

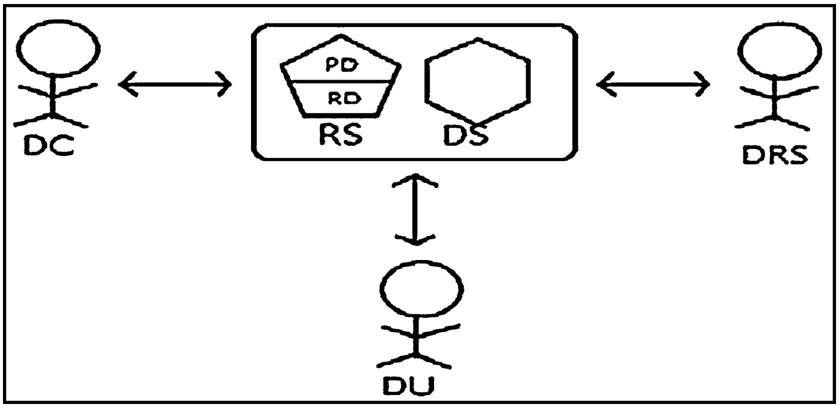
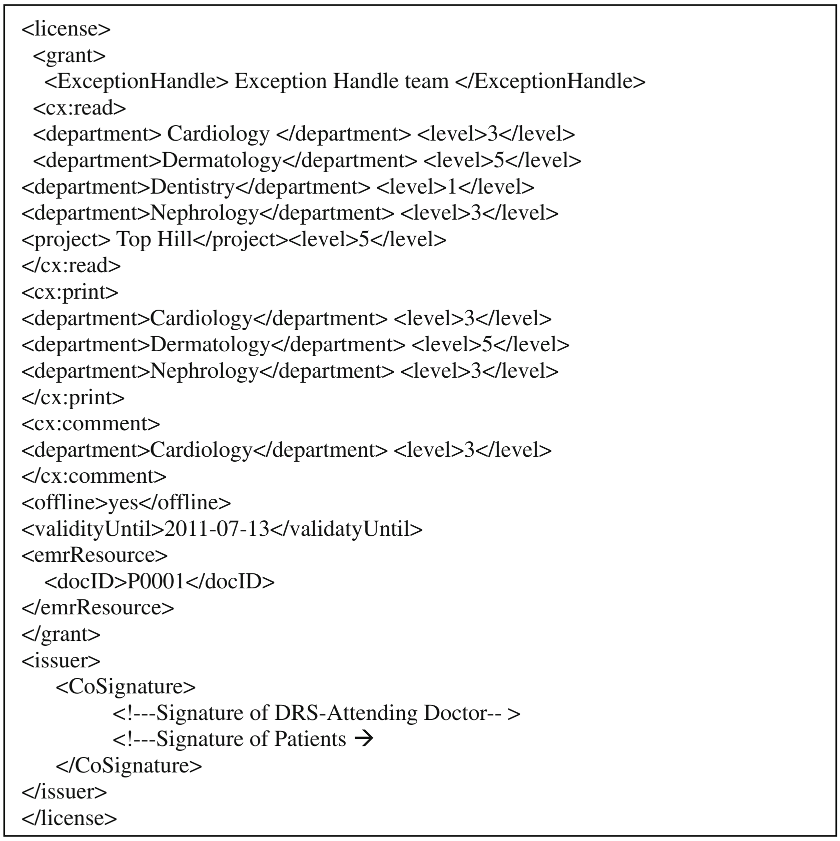


Fig. 2 RBAC-Matrix in the three operating roles and the two servers



```
<license>
  <grant>
    <ExceptionHandle> Exception Handle team </ExceptionHandle>
  <cx:read>
  <department> Cardiology </department> <level>3</level>
  <department>Dermatology</department> <level>5</level>
<department>Dentistry</department> <level>1</level>
<department>Nephrology</department> <level>3</level>
<project> Top Hill</project><level>5</level>
</cx:read>
<cx:print>
<department>Cardiology</department> <level>3</level>
<department>Dermatology</department> <level>5</level>
<department>Nephrology</department> <level>3</level>
</cx:print>
<cx:comment>
<department>Cardiology</department> <level>3</level>
</cx:comment>
<offline>yes</offline>
<validityUntil>2011-07-13</validatyUntil>
<emrResource>
   <docID>P0001</docID>
</emrResource>
</grant>
<issuer>
     <CoSignature>
            <!---Signature of DRS-Attending Doctor-- >
            <!---Signature of Patients →
     </CoSignature>
</issuer>
</license>
```

Fig. 3 Example of XrML Document Right

upload the XrML document right. If requested, the document server (DS) will produce shorter XrML document right attached only to medical personnel ID for each document user(DU), according to the XrML right description.

Example of XrML document right, shown in Fig. 3, as follows: first, exception handling by characters in exception handle team, then (1) The medical personnel of the Cardiology Department at level 3 or above, Dermatology

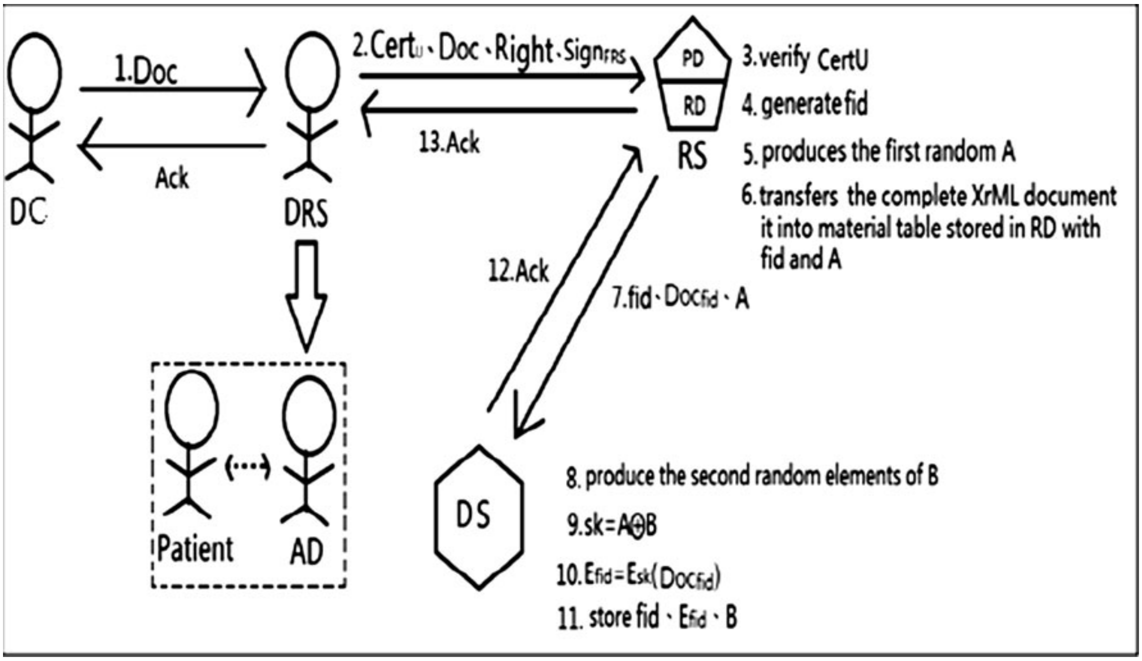
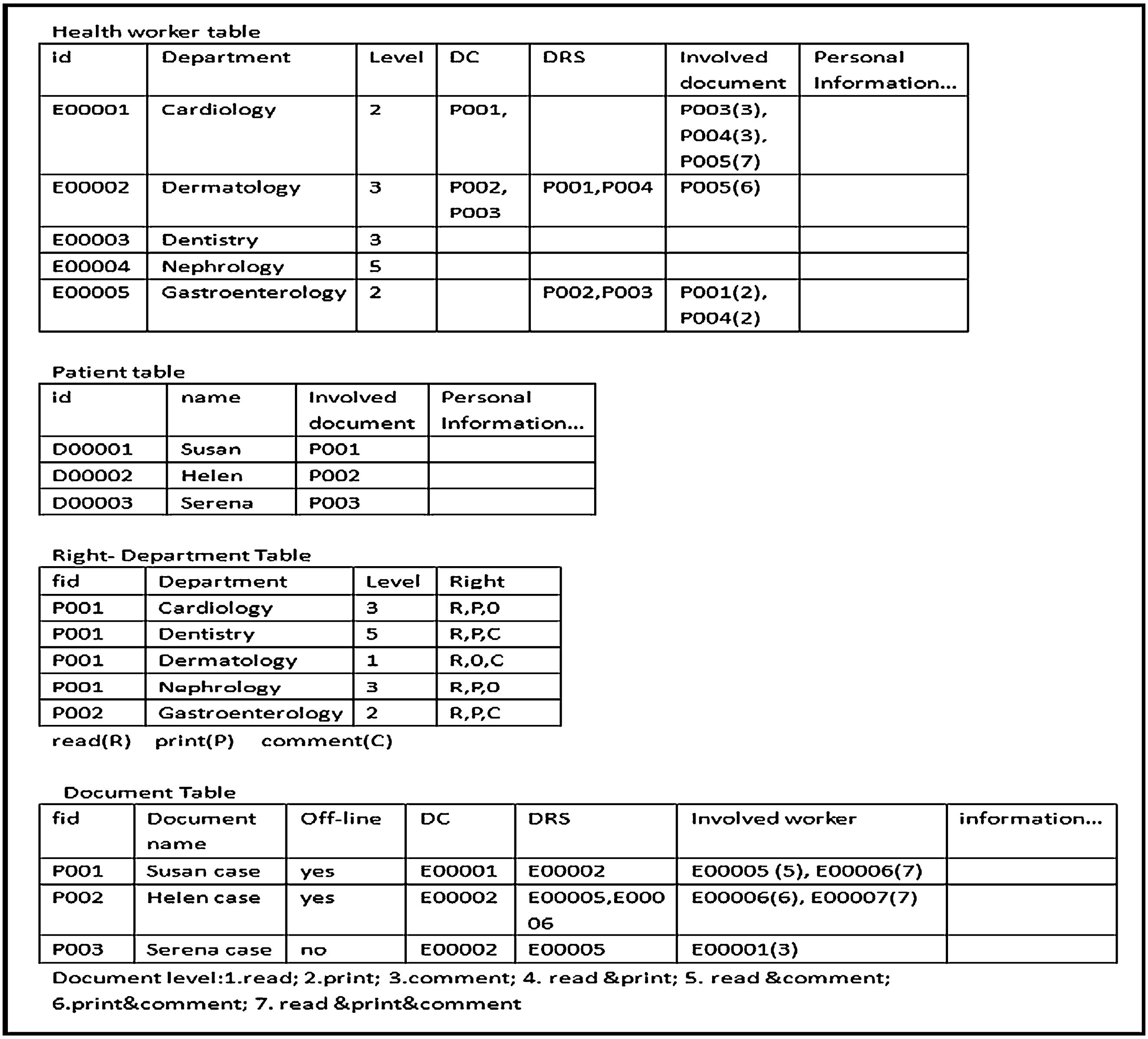

1.Doc
Ack
DC
DRS
2.Cert_U · Doc · Right · Sign_FRS
13.Ack
PD
RD
RS
3.verify CertU
4. generate fid
5. produces the first random A
6. transfers the complete XrML document it into material table stored in RD with fid and A
12.Ack
7.fid · Doc_fid · A
Patient
(…)
AD
DS
8. produce the second random elements of B
9.sk=A⊖B
10. E_fid=E_sk(Doc_fid)
11. store fid · E_fid · B

Fig. 4 Document upload and Right declaration



Health worker table

id	Department	Level	DC	DRS	Involved document	Personal Information...
E00001	Cardiology	2	P001,		P003(3), P004(3), P005(7)	
E00002	Dermatology	3	P002, P003	P001,P004	P005(6)	
E00003	Dentistry	3				
E00004	Nephrology	5				
E00005	Gastroenterology	2		P002,P003	P001(2), P004(2)	

Patient table

id	name	Involved document	Personal Information...
D00001	Susan	P001	
D00002	Helen	P002	
D00003	Serena	P003	

Right- Department Table

fid	Department	Level	Right
P001	Cardiology	3	R,P,O
P001	Dentistry	5	R,P,C
P001	Dermatology	1	R,O,C
P001	Nephrology	3	R,P,O
P002	Gastroenterology	2	R,P,C

read(R) print(P) comment(C)

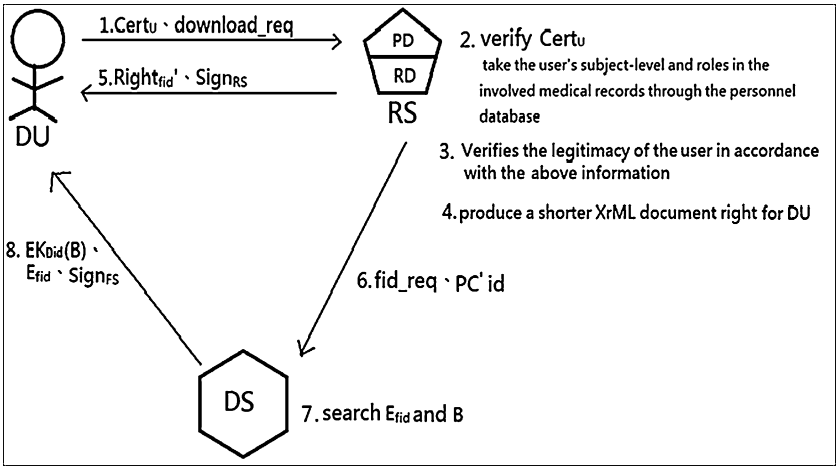
Document Table

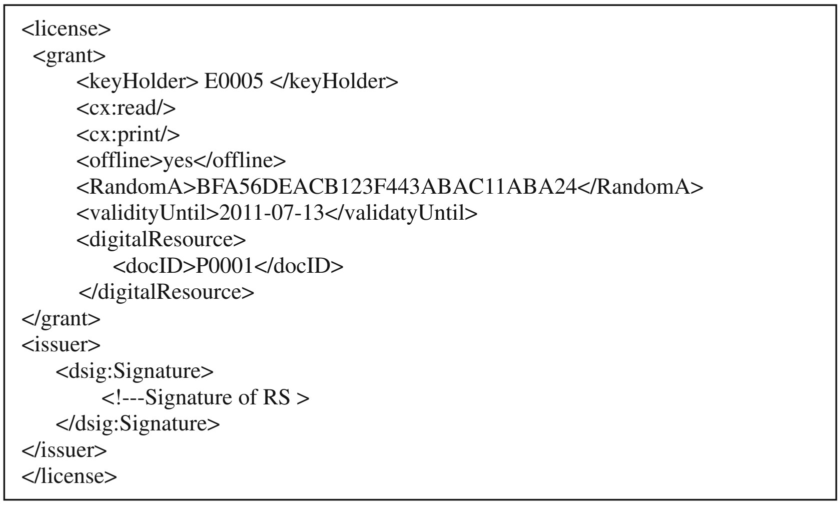
fid	Document name	Off-line	DC	DRS	Involved worker	information...
P001	Susan case	yes	E00001	E00002	E00005 (5), E00006(7)	
P002	Helen case	yes	E00002	E00005,E00006	E00006(6), E00007(7)	
P003	Serena case	no	E00002	E00005	E00001(3)	

Document level:1.read; 2.print; 3.comment; 4. read &print; 5. read &comment; 6.print&comment; 7. read &print&comment

Fig. 5 Working tables for Document Right

Fig. 6 Document download and Usage


1.Cert$_U$ 、download_req
PD
RD
RS
2. verify Cert$_U$
take the user's subject-level and roles in the involved medical records through the personnel database
5.Right$_{fid}$' 、Sign$_{RS}$
DU
3. Verifies the legitimacy of the user in accordance with the above information
4.produce a shorter XrML document right for DU
8. EK$_{Did}$(B) 、 E$_{fid}$ 、Sign$_{FS}$
6.fid_req 、PC' id
DS
7.search E$_{fid}$ and B



```
<license>
  <grant>
        <keyHolder> E0005 </keyHolder>
        <cx:read/>
        <cx:print/>
        <offline>yes</offline>
        <RandomA>BFA56DEACB123F443ABAC11ABA24</RandomA>
        <validityUntil>2011-07-13</validatyUntil>
        <digitalResource>
            <docID>P0001</docID>
         </digitalResource>
</grant>
<issuer>
     <dsig:Signature>
          <!---Signature of RS >
     </dsig:Signature>
</issuer>
</license>
```

Fig. 7 The shorter XrML document right for DU

Department at level 5 or above, the first layer of the Dentistry department, the Nephrology department at level 3 or above, and Special project Top Hill can do *read* to the document. (2) The medical personnel of the Cardiology Department at level 3 or above, Dermatology Department at level 5 or above, and the Nephrology department at level 3 or above, can do *print* to the document. (3) The medical personnel of the Cardiology Department at level 3 or above can do *comment* to the document.

Three operation phases

RBAC-Matrix mechanism can be divided into three operation phases, namely "Document upload and Right declaration", "Document download and Usage" and "Document Execution".

Document upload and right declaration

Within this phase, EMR content and associated XrML access rights are created and upload to DS and RS, shown in Fig. 4. Steps as follows:

(1) EMR record(called, Doc) is initiated by staff in the Registration department of medical institution, filled with Medical Examination and Diagnosis, performed by Document Creator(DC). The Doc is then sent to Document Right Setting(DRS) for authorization.

(2) DRS(the Attending Doctor) authorizes his underlying medical personnel rights according to the situation in the patient, and the contents of this authorization have to go through the patient's understand and agree by means of a cosign by the patient. The DRS sets the corresponding access right and produces a complete XrML rights description file. And then send his certificate(in his smartcard), Doc, XrML right file, and signatures of DRS and the patient to Right Server(RS).

(3) RS verifies the certificate of DRS through the personnel database(PD).

(4) RS generates the corresponding document file number (*fid*) for the Doc.

(5) RS produces the first random key element of *A*, for the encryption taken in the DS.

(6) RS also transfers the complete XrML document right into working tables to speed up the services of the RS query, shown in Fig. 5, and stores the fid and the first key element A into the Right Database (RD).

(7) RS transfers documents, *fid*, and random element of *A* to document server (DS).

(8) DS generating the second random elements of *B* after receives the above information.

(9) DS calculate the document encryption key($sk=A\oplus B$).

(10) DS encrypts the document ($\mathrm{Doc}_{\mathrm{fid}}$) into encrypted document ($\mathrm{E}_{\mathrm{fid}}$) through this key.

(11) DS store random element *B*, encrypted document ($\mathrm{E}_{\mathrm{fid}}$), and the *fid* in the DS.

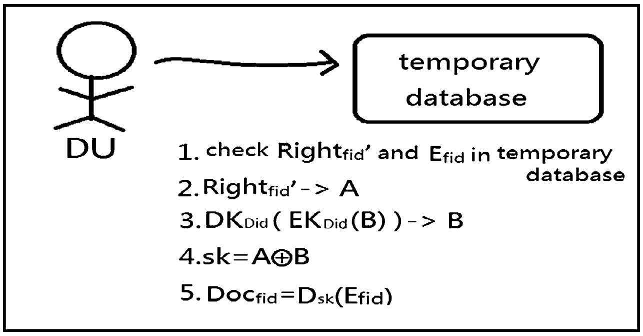

DU
temporary database
1. check Right_fid' and E_fid in temporary database
2. Right_fid' -> A
3. DK_Did (EK_Did (B)) -> B
4. sk=A⊕B
5. Doc_fid=D_sk(E_fid)

Fig. 8 Document execution phase

Table 2 RBAC-matrix key elements summary

Fields	RBAC-Matrix
Authentication	SmartCard-based
Document right setting	XrML setting by DRS(i.e.,Patient and Attending Doctor)
Mechanism roles	Three roles, two servers, and two databases.
Organization type	Matrix organization
Key combination	Two random elements *A* and *B*
Document right	XrML with two stages
Off-line operation	Can be set

Document download and usage

When a Document User(DU) wants to download the EMR, i.e., Doc, RS checks the DU's character and issues appropriate actions when the DU's character pass the document right setting, shown in Fig. 6. Details as follows:

(1) Document User(DU) sends the certificate from his smartcard and download request which contains a medical record number(*fid*) to the RS.
(2) RS verifies the certificate and obtains the user's character of medical institution through the personnel database (PD).
(3) RS Verifies the legitimacy of the user in accordance with the XrML description associated with the *fid*.
(4) RS produces a shorter XrML document right, signed by the RS, accordance with the user's authorization in this document, shown in Fig. 7. The shorter XrML document right records only the user's authorization in the corresponding document. This document right contains file number, the medical personnel ID, the medical personnel's authorization to use the document file (such as *read*, *comment*, and *print*),valid date, whether off-line work, and the first random element *A*.
(5) RS sends this shorter XrML document right and its signature value to DU.
(6) RS sends a download request and the address of the user's computer to DS.
(7) DS searches the corresponding encrypted document and the second random key element *B* in accordance with *fid*.
(8) DS sends the second random key element of *B*, encrypted by user's public key, the encrypted document, and its signature value to DU.

Document execution

This phase describes how to access downloaded EMR, i.e., Doc, after the previous phase. Details as follows, shown in Fig. 8:

(1) User's application checks whether the encrypted document and the corresponding Right'$_{\text{fid}}$ exist in temporary database. If not, back to the download phase.
(2) The application gets the first key element *A* from Right'$_{\text{fid}}$.
(3) The application gets the second key element *B* by its own private key.
(4) The application calculates the file encryption key ($sk = A \oplus B$).
(5) The application decrypts the encrypted documents by the encryption key and access the EMR in accordance with the document right.

This phase can provide offline function, if Right'$_{\text{fid}}$ permitted. All online files will be deleted and offline files will backup in the user's computer when the DU leave.

Security discussion

These three operating phases mentioned above is executed with assumption of a control environment, naming inside the medical institution, where server site and communication channel is well recognized and protected. As for a complex environment, some mechanisms [16] to do mutual authentication must be established before to make a secure communication channel. Following we will discuss others security issues within these operating phases:

Table 3 Comparison characters among RBAC access control structures

Fields/structures	RBAC-RR	RBAC-H	RBAC-Matrix
Role access structures	Individual	Hierarchy	Matrix
Access rights inherence	None	Vertical upwards	Vertical upwards and horizontal spreadable
Access rights setting	Statics	Statics	Dynamic

In the Document upload and Right declaration phase, all the operating roles are authenticated by the smartcard. The complete EMR record (Doc) is recognized and signed by the Attending Doctor(in fact private key in the AD's smartcard), and the associated XrML file is cosigned by the patient. The file is encrypted by a strong encryption algorithm like AES [17] to be well protected.

In the Document download and Usage phase, the DC is authenticated by the smartcard. After that, the DS encrypts the random key element *B* with DC's public key.

In the Document Execution phase, the application gets the key element *A* from $\text{Right}_{\text{fid}}$ and decrypts the key element *B* by using user's private key. Then perform the access right according to the file $\text{Right}_{\text{fid}}$.

All these operating can be secured if the authentication through smartcard and operating like encryption/decryption algorithm are secured.

Summary and comparison

RABC-Matrix provides a way to realize both the security issues: authentication, confidentiality, and availability, and the EMR's access control and digital right setting. In our scheme, users are authenticated through smartcard authentication to check for users' characters in the Medial Institution and do indirect mutual authentication. For the EMR's access control, we implement the access control structure in a matrix from and specify the rights in an associated XrML file. The XrML document rights is performed at two stages, i.e., the master stage(complete XrML rights file created in phase2) and the servant stage(shorter XrML rights file served for phase 3). Since the shorter XrML document right which contents only the medical personnel ID for each user, the user's application can easily authenticate the EMR usage through the user's smartcard. Besides, we generate the key with two random key elements *A* and *B*, stored in different databases, and encrypt all EMR records. Thus, we can obtain availability and reduce the potential risk of leakage.

For modern Medical Institution organizations, either the dichotomized (hierarchical) roles or roles of linear type are not sufficient to overcome the access control issues [18]. In RBAC-Matrix, we propose three views of the organizations, i.e., the departments, the projects, and the emergency handles. Within each views of the structure, we also assign a security clearance level to each character. Detailed operations within RBAC-Matrix are carried through the three roles(DC, DRS, and DU), the two servers(RS and DS), and the two database(PD, RD). Table 2 summarizes the key elements of RBAC-Matrix. The comparison characters of the previous proposed access control structures: RBAC-RR, RBAC-H, and proposed RBAC-Matrix are depicted in Table 3.

Conclusion

We propose the RBAC-Matrix digital rights management system, which is a RBAC-based extension to a matrix organization of Medical Institutions. RBAC-Matrix authorizes access control declaration among matrix organizations of medical institutions by using XrML file in association with each EMR. It transfers and processes XrML document rights files within the master & servant stages, thus makes better protection on the associated EMR file.

RBAC-Matrix will also make medical record file and its associated XrML declaration to two different EMRA(EMR Authorization)roles, namely, the medical records Document Creator (DC) and the medical records Document Right Setting (DRS). In associated with each EMR, the DRS set the access rights by constructing XrML rights file and sign it. That XrML rights file is cosigned by patients, thus maks the declaration of rights and the use of EMR to comply with HIPAA specifications

Acknowledgement This work was partially supported by NSC Taiwan under the project number: NSC 100-2219-E-002-032.

References

1. Apple Daily, Selina's bedside birthday, Chang Gung medical records of any translation, http://tw.nextmedia.com/applenews/article/art_id/32926156/IssueID/20101031, accessed 2010/11/02.
2. Win, K. T., Susilo, W., and Mu, Y., Personal health record systems and their security protection. *J. Med. Syst.* 30(4):309–315, 2006.
3. Ferraiolo, D. F., and Kuhn, R. Role-Based Access Control, Proceedings of the 15th National Computer Security Conference, 1992.
4. National Institutes of Health, Health Services Research and the HIPAA Privacy Rule, http://privacyruleandresearch.nih.gov, accessed Aug. 2010.
5. Office of the Privacy Commissioner of Canada, The Personal Information Protection and Electronic Documents Act (PIPEDA), http://www.priv,gc.ca, accessed Aug. 2010.
6. Condric, L., Dech, D., and Galic, D. The importance of project office in matrix organization. 8th International Conference on Telecommunications - ConTEL 2005, Zagreb, 2005.
7. ContentGuard, XrML: eXtensible rights Markup Language. http://www.xrml.org/index.asp, accessed Dec. 2010.
8. Yang, J. -T., *The research of XrML-based multimedia digital rights management system*. Master's thesis, National Chung Cheng University, 2005.
9. Fan, J. -S., *The XrML-based enterprise digital rights management system for access control*. Master's thesis, Tatung University, 2010.
10. Sandhu, R., et al., Role-based access control models. *IEEE Comput.* 29(2):38–47, 1996.
11. Ferraiolo, D. F., et al., Proposed NIST standard for role-based access control. *ACM Trans. On Information and System Security.* 4 (3), 2001.
12. National Institute of Standards and Technology (NIST), security requirements for cryptographic modules, FIPS PUB 140–2, 2001.

13. Sauders, G., Hitchens, M., and Varadharajan, V., Role-based access control and the access control matrix. *ACM Operating Systems Review*, Oct. 2001.
14. Lee, W. -B., Lee, C. -D., *A cryptographic key management solution for HIPAA privacy/security regulations*. Master's thesis, Feng Chia University, 2008.
15. Office of the NSW Privacy Commissioner, "Health Records and Information Privacy Act 2002," http://www.ipc.nsw.gov.au, accessed Sep. 2010.
16. Wu, Z. Y., Lee, Y. C., Lai, F., Lee, H. C., and Chung, Y. F., A secure authentication scheme for telecare medicine information systems. *J. Med. Syst.*, 2010. doi:10.1007/s10916-010-9614-9.
17. National Institute of Standards and Technology (NIST), Advanced Encryption Standard (AES), FIPS PUB 197, 2001.
18. Chen, J.-L., A enterprise digital rights management system based on group-oriented authorization. *Electron. Commer. Res.* 7 (2):133–150, 2009.