Secure Electronic Medical Records Exchange System implementation based on Secure MIME and RESTful Service

Chien Hua Wu, Ruey Kei Chiu

***Abstract*—The exchange of Electronic Medical Records (EMR), improve the management of medical records on paper, by reducing the amount of paper used and storage spaces. This system has been effectively used in Taiwan; where enterprises are sharing EMR through the Exchange Center of EMR under the Virtual Private Network, however this system is slightly secure. The purpose of this study was to propose a security mechanism, and to achieve the information exchange security: (1) Authentication of EMR;(2) Confidentiality storage of EMR;(3) Integrity of EMR;(4) Non-repudiation of EMR exchange with each stakeholder. The combination of the security mechanism of S/MIME message level and RESTFul Service was adopted to build a secure mechanism for the sharing of EMR; Three scenarios were simulated and implemented to verify the feasibility of this mechanism. It can be concluded that the use of RESTful and S/MIME can enhance the security exchange of the EMR.**

***Index Terms*—Electronic Medical Record, Message Security, RESTFul, S/MIME**

I. Introduction

THE Ministry of Health and Welfare conducted an EMR exchange center (EEC) in 2009 to share EMR for hospitals in Taiwan.[1] There are already five categories of EMR that can be exchanged through the EEC between hospitals under Virtual Private Network.[2] The development of EMR now has a considerable effect in hospitals. After the government passed a legislation, hospitals now can use EMR and does not required to create and save papers of medical records.[3] Hwang et al. indicated that EMR information quality exchange was the key factor to attract more users.[4] EMR allows physicians rapid access to medical treatment in different hospitals, saving medical resources. This paper focused in the prevailing exchange EHR architecture. Figure 1 represents three scenarios were simulated and implemented to evaluate and verify the feasibility of such a mechanism. The purpose of this study was to propose a security mechanism, and to achieve the information exchange security:(1) Authentication of EMR;(2) Confidentiality storage of EMR; (3) Integrity of EMR;(4) Non-repudiation of EMR exchange with each stakeholder.

Manuscript received January8, 2016; revised January19, 2016.

Chien Hua Wu is with the Graduate Institute of Business Administration, Fu Jen Catholic University, Taiwan (phone: +886-2-25536336#162; fax: +886-2-25537973; e-mail: kevin930202@gmail.com).

Ruey Kei Chiu was with Department of Information Management, Fu Jen Catholic University, Taiwan (e-mail: 004271@mail.fju.edu.tw).

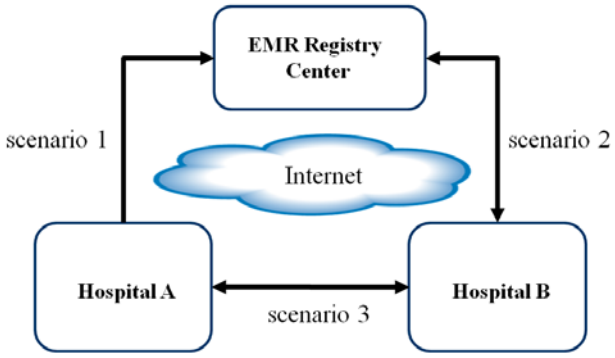

Fig. 1. Scenarios of EMR exchange System

II. Materials and Methods

A. Medical Information share Standards

Health Level Seven International (HL7) founded in 1987, the American National Standards Institute (ANSI) and the International Organization for Standardization (ISO) accredited international standards for the EMR exchange and sharing to support clinical practice.[5-7] Due to the wide range of medical services covered by the industry, such as medical care, medicines, medical equipment, medical information, health care, etc. The main objective of HL7 is to develop a commonality and interoperability system. The Level 7 layer supports the secure authentication and identification of data exchange; also protocols standards can be quickly applied in hospitals and is easily integrated with several of the other systems. Clinical Document Architecture, Release Two (CDA R2), became an ANSI-approved HL7 Standard in May 2005.[8] CDA documents are encoded in Extensible Markup Language (XML) which specifies the structure and semantics of a clinical document. A CDA document can include text, images, sounds, and other multimedia content. Digital Imaging and Communications in Medicine (DICOM) is currently the standard format widely used in hospitals for medical imaging message.[9] DICOM was announced by the committee (ACR-NEMA) which established by the American College of Radiology (ACR) and the National Electrical Manufacturers Association (NEMA), published in 1993, and officially named DICOM 3.0 to help the image storage, content distribution and viewing of medical images, such as Computerized Tomography (CT), Magnetic Resonance Imaging (MRI) and

ISBN: 978-988-19253-8-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

ultrasound.

B. Representational State Transfer

Representational State Transfer (REST) is a design concept. This concept comes from a published PhD thesis by Roy.[10] He proposed REST software architecture style as an abstract model of network applications, but it is not a standard format. REST systems interface with external systems like web resources and each resource will have a Uniform Resource Identifier (URI). REST relies on a stateless, client-server, and cacheable communications protocol. Web applications in HTML are only defined to the GET POST, because little use in given to other methods such as PUT and DELETE on Web-based applications as well as HEAD, STATUS and other methods. REST is a simple interface often used to describe any use of XML (or YAML, JSON, plain text), without having to rely on other mechanisms like SOAP. Compared to other commonly used Web Service standards, such as SOAP and XML-RPC,REST is more simple and easy to use, and it has the following characteristics:(1) All of the API is Resource form;(2) the service can accept and return MIME-TYPE, also can return XML / JPG / TXT and other formats; (3) Support operation of various HTTP methods (such as GET, POST, PUT, DELETE).

C. Multipurpose Internet Mail Extensions

Multipurpose Internet Mail Extensions (MIME) is a network messaging applied to flexible message format standard [11]. MIME format can support transmission such as images, audio, video, and other binary file extending the standard E-mail. MIME message format consists of Header and Body. Header is a set of Header Fields, Body contains a single Party or multiple Parties. MIME Header provides the information structure and encoding; the Body is the actual message content, supports a variety of data formats, sometimes also referred to as "Payload". Secure MIME (S/MIME) is a standard message format.[12] S/MIME provide MIME message format standard encryption and digital signatures to send and receive secure messages in MIME format on the web. MIME provides digital signature and encryption; these security mechanisms are based on RSA public key infrastructure (PKI).

D. Comparison to Web Services

Web Service is based on the Simple Object Access Protocol (SOAP) agreement, WS-Security is the core of Web services security standards.[13] Gabriel et al. used the GET and POST methods to compare different security mechanisms between them.[14] In the conditions of plain text, encryption or signature, the results show that RESTful services processed more efficiently than Web Services. Cesare et al. describes the differences between REST services and WS- * services.[15] They used a variety of architectural decision models to determine which type of service were more appropriate. Their result showed that REST was more suitable for basic and ad-hoc integration scenarios. When business requirements demand a higher quality of service WS- * was more flexible.

III. System Design

A. System Architecture

A Secure Electronic Medical Record Services system (SEMRS) conducted in this paper make reference to an existing electronic medical records exchange to enhance the message security. Figure 2 presents the whole architecture of SEMRS. Step 1-1 through Step 1-3 presents the scenario 1 of EMR upload and EMR index registry process of Hospital A, step 2-1 and Step 2-2 presents the scenario 2 of EMR index store query process of Hospital B, step 3-1 and step 3-2 presents the scenario 3 of EMR retrieve process of Hospital B.

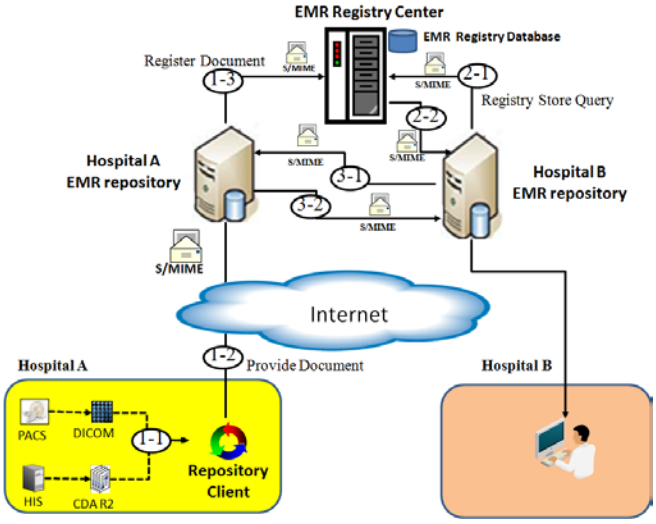

Fig. 2. System Architectureof SEMRS.

1) (1-1) Hospital A puts CDA R2 documents and DICOM documents which will be upload to repository to the Repository Client of Hospital. (1-2) Repository Client of Hospital A packaged the CDA R2 documents and DICOM documents into a S/MIME envelope then upload it to EMR repository of Hospital A through RESTFul service. (1-3) EMR repository of Hospital A used RESTFul service to register received EMR index to EMR Registry Center via RESTFul services using S/MIME.

TABLE I
MIME Header Tags

MIME Header Tag	Tag Description
X-EEC-Sender	Sender
X-EEC-Receiver	Receiver
X-EEC-SymmetricAlg	One-time password Algorithm
X-EEC-AsymmetricAlg	PKI Algorithm
X-EEC-DistAlg	Message Digest Algorithm
X-EEC-SignAlg	Digital Signature Algorithm
X-EEC-BodypartCnt	MIME Body Part count
X-EEC-HeaderCnt	MIME Header tag count
X-EEC-MessageType	EMR category

2) (2-1) EMR Repository of Hospital B sent EMR registry store query request to EMR Registry Center via RESTFul services using S/MIME. (2-2) EMR Registry

ISBN: 978-988-19253-8-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Center response it to the EMR repository of Hospital B through RESTFul service using S/MIME.

3) (3-1) EMR Repository of Hospital B sent a retrieve request to EMR Repository of Hospital A via RESTFul services using S/MIME. (3-2) EMR Repository of Hospital A packaged the documents into a S/MIME envelope then response it to the EMR repository of Hospital B through RESTFul service.

B. Message Structure

Figure 3 represents the message structure of SEMRS. Table 1 lists the usage of MIME header tags used in SEMRS. In the MIME body the encrypted CDA document is done in body part 1, encrypted message digest is done in body part 2, encrypted digital signature take place in body part 3, encrypted one-time password is in body part 4, encrypted DICOM documents are stored from body part 5 to the end part.

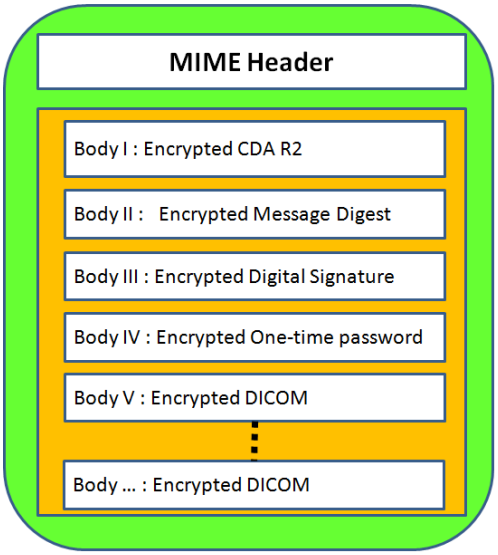

Fig. 3. Message Structure of SEMRS

C. Security Algorithm

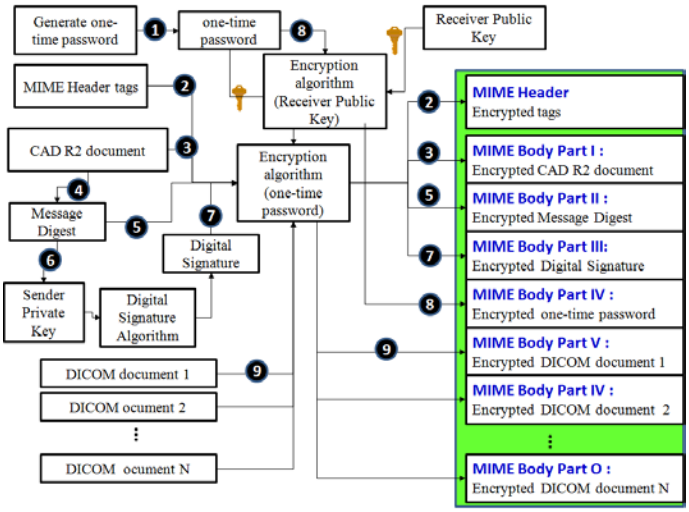

Fig. 4. The process of Hospital A.

Figure 4 represents the processes of Hospital A from step 1 through step 9, corresponding to the steps of algorithm in Table 2 respectively. The processes involved in this principle are:(1)Dynamically generated one-time password;(2)Use one-time password to encrypt all MIME Header tag values;(3)

TABLE II
ALGORITHM OF HOSPITAL A (PROVIDER)

STEP	ALGIRITHM
Step 1	OTPKey = KeyGenerator(KeyAlg)
Step 2	For all header.name Mhd[name].value=encryptData(header.value, OTPKey, OTPKeyAlg) End for

Step 3	EncEMR = encryptData (hisEMR, OTPKey, OTPKeyAlg)
	If EncEMR is not null then
	Mpart.AddBodyPart(EncEMR)
	End if

Step 4	mDist = digest(hisEMR, DistAlg)

Step 5	EncDist = encryptData (mDist , OTPKey, OTPKeyAlg)
	If EncDist is not null then
	Mpart .AddBodyPart(EncDist)
	End if

Step 6	SignEMR = sign(mDist, SenderPriKey, SignAlg) byteSign = concateToByte(mDist, FinPrt)

Step 7	EncSign = encryptData (SignEMR, OTPKey, OTPKeyAlg)
	If EncSign is not null then
	Mpart .AddBodyPart(EncSign)
	EndIf

Step 8	EncOTPKey = encryptData (OTPKey, ReceiverPubKey, PKIAlg)
	If EncOTPKey is not null then
	Mpart.AddBodyPart(EncOTPKey)
	End if

Step 9	EncDICOM = encryptData (hisDICOM, OTPKey, OTPKeyAlg)
	If EncEMR is not null then
	Mpart.AddBodyPart(EncDICOM)
	End if

TABLE III
ALGORITHM OF HOSPITAL B (CONSUMER)

STEP	ALGIRITHM
Step 1	EncOTPKey = Mpart .GetBodyPart(4)
Step 2	OTPKey = decryptData (EncOTPKey, ReceiverPriKey, PKIAlg)
Step 3	For all header.name Mhd[name].value=decryptData(heder.value,OTPKey,OTPKeyAlg) End for
Step 4	EncEMR =Mpart .GetBodyPart(1) hisEMR = decryptData (hisEMR, OTPKey, OTPKeyAlg)
Step 5	EncDist =Mpart .GetBodyPart(2) mDist = decryptData (EncDist , OTPKey, OTPKeyAlg)
Step 6	EncSign =Mpart .GetBodyPart(3) SignEMR = encryptData (EncSign, OTPKey, OTPKeyAlg)
Step 7	EncDICOM =Mpart .GetBodyPart(5) hisDICOM = decryptData (EncDICOM, OTPKey, OTPKeyAlg)

ISBN: 978-988-19253-8-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Use one-time password to encrypt CDA R2 document then puts it into MIME body part 1; (4) Use CDA R2 document to generate message digest; (5) Use one-time password to encrypt message digest then put it into MIME body part 2; (6) Use sender's private key and message digest to create digital signature; (7) Use one-time password to encrypt digital signature then put it into MIME body part 3; (8) Use receiver public key to encrypt one-time password then put it into MIME body part 4;(9) Use one-time password to encrypt DICOM document then put it into MIME body part 5 and so on.

Figure 5 represents the processes of Hospital B from step 1 through step 7 correspond to the steps of algorithm in Table 3 respectively. The processes involved in this principle are :(1)Extract encrypted one-time password from MIME body;(2) Decrypted password using receiver's private key then get one-time password;(3)Decrypted MIME header tags using one-time password;(4)Extract MIME body part 1 of encrypted CDA R2 document then decrypted it using one-time password;(5)Extract MIME body part 2 of message digest then decrypted it using one-time password;(6)Extract MIME body part 3 of digital signature then decrypted it using one-time password;(7)Extract MIME body part 4 of DICOM document then decrypted it using one-time password and so on. To verify the digital signature after successfully decrypted.

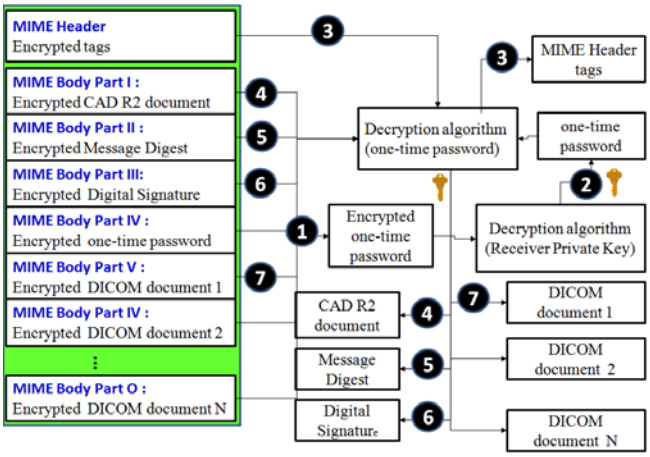

Fig. 5. The process of Hospital B.

IV. Expected Results

A. Provide and Register EMR of Hospital A

Fig. 6. Secure MIME Header

Hospital A packages CDA R2 and DICOM document into MIME envelope then uploads to Repository of Hospital A and registers to Registry EMR center. Figure 6 represents the encrypted MIME header and Figure 7 represents the encrypted MIME body. After successfully uploaded to the Registry EMR Center and signature verification success. It indicates that this transaction has non-repudiation.

Fig. 7. Secure MIME Body

B. Retrieve EMR from Hospital A to Hospital B

Hospital B inquires patient's EMR records from Registry EMR center then retrieves desired EMR records from Repository of Hospital A to Repository of Hospital B. Figure 8 represents the patient's EMR record which successfully retrieved from Hospital A to Hospital B using RESTful service.

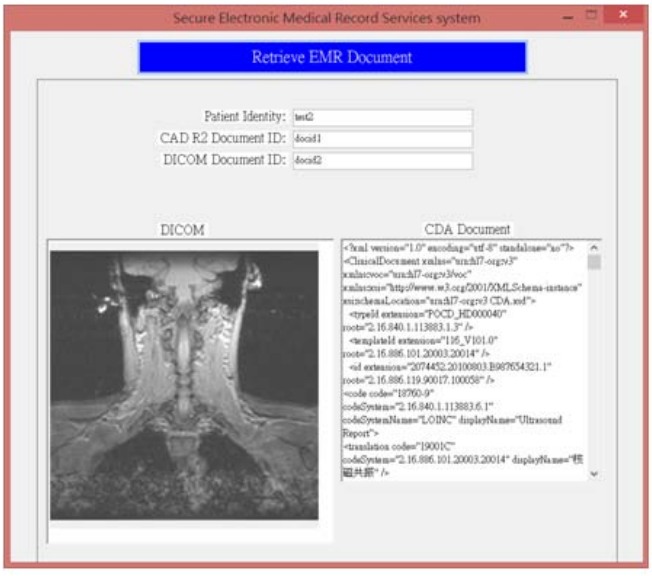

Fig. 8. Retrieved EMR document from Hostital A

V. Discussion and Conclusion

This paper, was focused on how to use S/MIME and RESTful Web service to develop a secure mechanism of EMR documents exchange. With the flexibility of REST and MIME envelope, the RESTful Web service have become more acceptable. It has been a more secure solution compare to VPN. The proposed approach respects the REST

ISBN: 978-988-19253-8-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

philosophy by implementing the message security with MIME envelope. This approach enforces the message to be encrypted and protected during transmission. It was also applied, message digest and digital signature for verification. Thus, the proposed approach can achieve the exchange of confidentiality, integrity, authentication and non-repudiation.

When needed patient's electronic medical records can be easily accessed by any hospital. It can be integrated in-house system of hospitals and provide a way to exchange EMR documents securely between different enterprises. Enterprises can exchange patient's information when it is convenient to access the patient's treatment. This avoids repetitive inspections to save medical resources. In order to know if the mechanism can improve or not the security, it must be tested by EEC.

REFERENCES

[1] Ministry of Health and Welfare(2009, May 10). "Health Care Platinum program". Available: http://www.mohw.gov.tw/news/448238669.

[2] National Health Insurance Administration(2012, May 24), "Healthcare Information Network Service System (VPN) User Manual".

[3] Ministry of Justice (2014, January 29), "Law & Regulations Database of The Republic of China"., Available: http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=L0020021。

[4] H. G., Hwang, C. H. Lu, J. L. Hsiaoand R. F. Chen (2009), "Factors Influencing Benefits of Electronic Medical Records Exchange : Physician Perspectives"., Journal of e-business., 11(1), pp. 95-118.

[5] Health Level Seven International (1987),"About HL7"., Available: http://www.hl7.org/about/index.cfm?ref=nav.

[6] American National Standards Institute (2011),"HL7 V3 Normative "., Available: http://webstore.ansi.org/RecordDetail.aspx?sku=HL7+V3+Normative-2011.

[7] ISO (2009),"Data Exchange Standards -- HL7 Clinical Document Architecture, Release 2".,Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44429.

[8] American National Standards Institute (2005),"HL7 Version 3 Standard: Clinical Document Architecture (CDA), Release 2"., Available: http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI%2FHL7+CDA+R2-2005+(R2010).

[9] NEMA (2013),."DICOM PS3.1 2014c - Introduction and Overview"., Available: http://medical.nema.org/medical/dicom/current/output/pdf/part01.pdf.

[10] T.F. Roy (2000). "Architectural Styles and the Design of Network-based Software Architectures"., Ph.D. dissertation, University of California, Irvine, USA, 2000.

[11] SoftwareAG (2011), "MIME-S/MIME Developer's Guide Version 8.2 "., April 2011.

[12] Internet Engineering Task Force (2010), "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message specification" , RFC 5751, January 2010.

[13] OASIS (2006), "Web Services Security: SOAP Message Security 1.1 (WS-Security 2004)"., OASIS Standard Specification,Available:http://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

[14] S. Gabriel, S. D. O. Anderson, M. Julienand R. Yves (2012),"Enabling Message Security for RESTful Services"., IEEE 19th International Conference on Web Services (ICWS 2012) , Hawaii, USA.

[15] P. Cesare, Z. Olaf andL. Frank (2008),"RESTful Web Services vs. "Big" Web Services:Making the Right Architectural Decision"., 17th International World Wide Web Conference (WWW 2008) , Beijing, China.

ISBN: 978-988-19253-8-1
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)