Advances in Science, Technology and Engineering Systems Journal Vol. 2, No. 1, 172-176 (2017)

www.astesj.com

Special Issue on Computer Systems, Information Technology, Electrical and Electronics Engineering

ASTESJ

ISSN: 2415-6698

Implementation a Secure Electronic Medical Records Exchange System Based on S/MIME.

Chien Hua Wu[*,1], Ruey Kei Chiu[2]

[1]Graduate Institute of Business Administration, Fu Jen Catholic University, 242, Taiwan

[2]Department of Information Management, Fu Jen Catholic University, 242, Taiwan

ARTICLE INFO

Article history:
Received: 21 December, 2016
Accepted: 19 January, 2017
Online: 28 January, 2017

Keywords :
Electronic Medical Record
Message Security
RESTFul
S/MIME

ABSTRACT

The exchange of electronic medical records can reduce the preservation and the use of papers of medical records for management issues. The sharing of electronic medical records has been effective in Taiwan. Now days, enterprises are sharing their electronic medical records through the Exchange Center of EMR under the Virtual Private Network but slightly less secure. This study aims to propose a security mechanism for the sharing of electronic medical records. The combination of security mechanism of S/MIME message level and RESTFul Service were adopted to build a secure mechanism for the sharing of electronic medical records. Two scenarios were simulated and implemented to verify the feasibility of this mechanism. From the results of the simulation presented, it has been conclude that the use of RESTful and S/MIME can enhance the security exchange of the electronic medical records.

1. Introduction

The Ministry of Health and Welfare [1] planned to conduct an electronic medical record exchange center(EEC) from 2009 to share electronic medical records for hospitals in Taiwan. There are already five categories of electronic medical records that can be exchanged through the EEC between hospitals under Virtual Private Network [2]. The development of electronic medical records in the hospital now has a considerable effect. After having legislation [3] of electronic medical records, hospitals can use electronic medical records, do not need to create and save papers of medical records. Hwang et al. [4] indicated that information quality of EMR exchange was the key factor which influencing users. EMR allows physicians rapid access to medical treatment in different hospitals, save the use of medical resources. This paper references to the prevailing exchange EHR architecture. Aim to explore a core technology and the security approach among health care information systems. Two 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..

*Corresponding Author: Chien Hua Wu
Graduate Institute of Business Administration, Fu Jen Catholic University, 242, Taiwan
Email: kevin930202@gmail.com

2. Background

2.1. Medical Information share Standards

The Health Level Seven International [5] was founded in 1987. American National Standards Institute (ANSI) [6] and the International Organization for Standardization (ISO) [7] accredited international standards for the EMR exchange and sharing that support clinical practice. 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 also supports the secure authentication and identification of data exchange. HL7 standards can be quickly applied in hospital and can be easily integrated with several of the other systems. Clinical Document Architecture, Release Two (CDA R2), became an ANSI-approved [8] HL7 Standard in May 2005. CDA documents are encoded in Extensible Markup Language (XML) that 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]. This standard was announced by the committee (ACR-NEMA) which established by 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 ultrasound.

2.2. Representational State Transfer

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

2.3. Multipurpose Internet Mail Extensions

Multipurpose Internet Mail Extensions (MIME) is a network messaging applied to flexible message format standard [11]. It extends the standard of E-mail, MIME standard can support transmission such as images, audio, video, and other binary file. MIME message format consists of Header and Body. Header is a set of Header Fields, Body contains a single Party or more Parties. MIME Header provides the information structure and encoding. MIME 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. It provides digital signature and encryption; these two security mechanisms are based on RSA public key infrastructure (PKI).

2.4. Comparison to Web Services

Web Service is based on the Simple Object Access Protocol (SOAP) agreement, WS-Security [13] is the core of Web services security standards. Gabriel et al. [14], respectively, used the GET and POST methods to compare different security mechanisms among them. In the conditions of plain text, encryption or signature, the results show that RESTful services were processed more efficiently than Web Services. Cesare et al. [15] describes the differences between REST services and WS- * services. He used a variety of architectural decision models to determine which type of service were more appropriate. Their result shows 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.

3. Materials and Methods

3.1. System Architecture

A Secure Electronic Medical Record Services system (SEMRS) conducted in this paper references an existing electronic medical records exchange to enhance the message security. Figure 1 presents the whole architecture of SEMRS. Step 1 through Step3 presents the EMR upload and EMR index registry process of Hospital A, step 4 through Step 5presents the EMR index store query process of Hospital B, step 6 through step 7 presents EMR retrieve process of Hospital B.

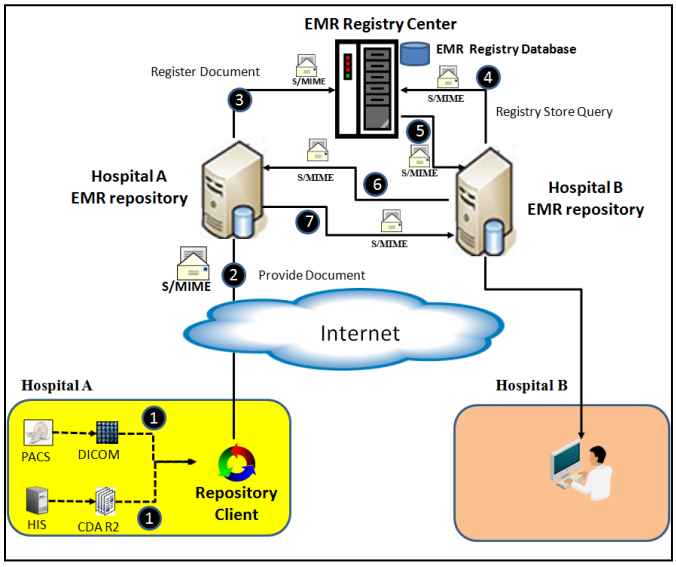

Figure 1. System Architecture of SEMRS.

- Step 1 through Step 3 are described as follows: (1)Hospital A puts CDA R2 documents and DICOM documents which will be upload to repository to the Repository Client of Hospital.(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.(3)EMR repository of Hospital A used RESTFul service to register received EMR index to EMR Registry Center via RESTFul services using S/MIME.
- Step 4 through Step 5 are described as follows:(4)EMR Repository of Hospital B sent EMR registry store query request to EMR Registry Center via RESTFul services using S/MIME.(5)EMR Registry Center response it to the EMR repository of Hospital B through RESTFul service using S/MIME.
- Step 6 through Step 7 are described as follows:(6)EMR Repository of Hospital B sent a retrieve request to EMR Repository of Hospital A via RESTFul services using S/MIME.(7)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.

3.2. Message Structure

Figure 2 presents the message structure of SEMRS. Table 1 lists the usage of MIME header tags which were used in SEMRS.MIME body presents in figure 2 which encrypted CDA document is in body part 1, encrypted message digest is in body part 2, encrypted digital signature is 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.

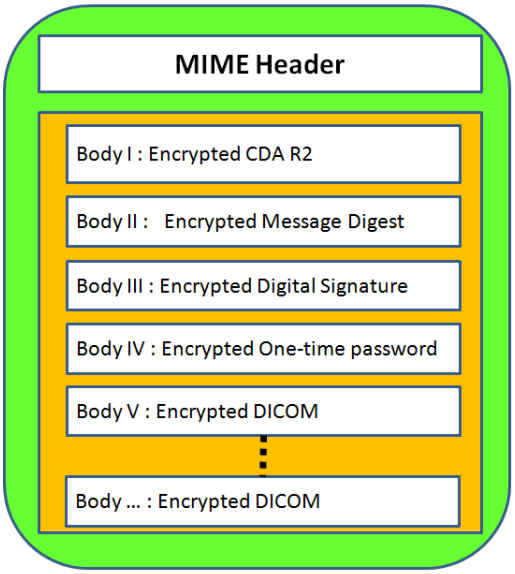

Figure 2 Message Structure of SEMRS

3.3. Algorith of SEMRS

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

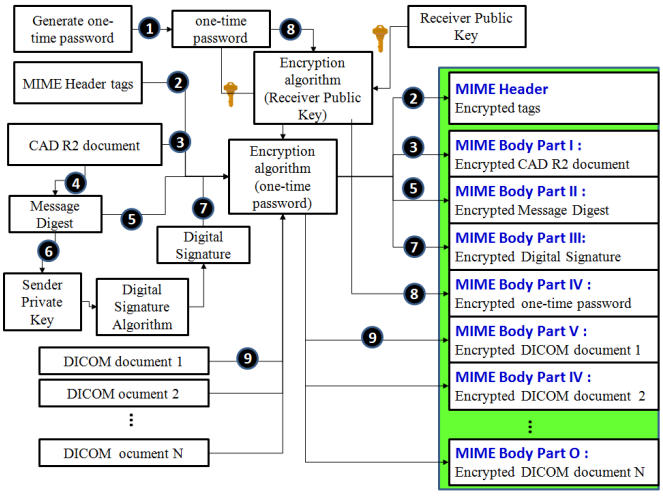

Figure 3 The scenario of Hospital A

Figure 4 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 it 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.

Table 1 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

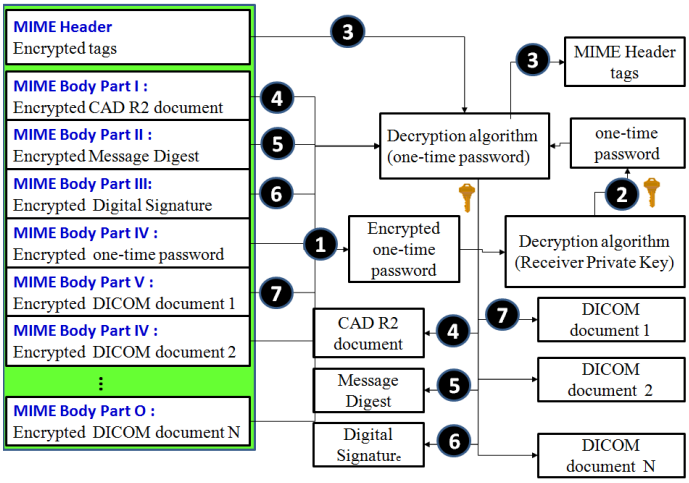

Figure 4: The scenario of Hospital B

4. Experimental Results

4.1. Provide and Register EMR of Hospital A

Hospital A packages CDA R2 and DICOM document into MIME envelope then uploads to Repository of Hospital A and registers to Registry EMR center. Part A of figure 5 shows the encrypted MIME header and Figure 6 shows the encrypted MIME body. After successfully uploaded to the Registry EMR center and signature verification success. It indicates that this transaction has non-repudiation.

4.2. Hospital B Retrieve EMR from Hospital A

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 6 presents the patient's EMR record which successfully retrieved from Hospital A to Hospital B using RESTful service.

Table 2: 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 3: 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)

5. Conclusion and Discussion

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

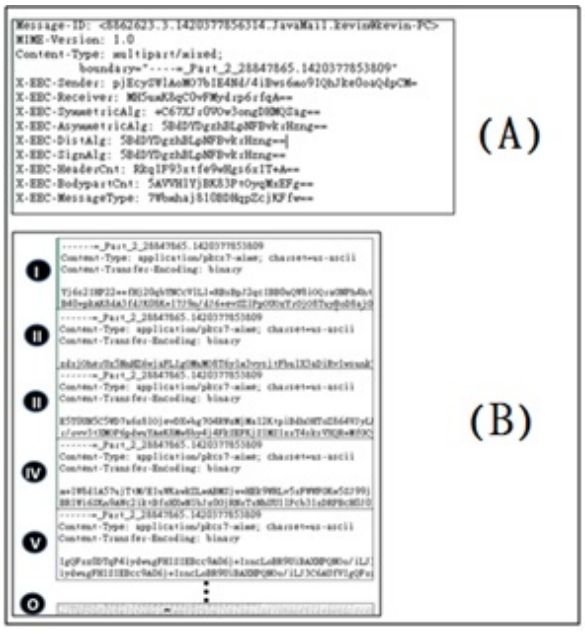

Figure 5 Secure MIME of SEMRS

Figure 6 Retrieved EMR document from Hospital A

References

[1] Ministry of Health and Welfare , Health Care Platinum program. Available:

http://www.mohw.gov.tw/news/448238669, 2009.
[2] National Helth Insurance Administration , Healthcare Information Network Service System (VPN) User Manual, 2012.
[3] Ministry of Justice , Law & Regulations Database of The Republic of China., Available: http://law.moj.gov.tw/LawClass/LawAll.aspx?PCode=L0020021, 2014.
[4] H. G., Hwang, C. H. Lu, J. L. Hsiao and R. F. Chen , "Factors Influencing Benefits of Electronic Medical Records Exchange : Physician Perspectives"., Journal of e-business., 11(1), pp. 95-118, 2009.
[5] Health Level Seven International , About HL7., Available: http://www.hl7.org/about/index.cfm?ref=nav, 2017.
[6] American National Standards Institute , HL7 V3 Normative ., Available: http://webstore.ansi.org/RecordDetail.aspx?sku=HL7+V3+Normative-2011, 2011.
[7] ISO , Data Exchange Standards -- HL7 Clinical Document Architecture, Release 2., Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44429, 2015.
[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), 2015.
[9] NEMA ,. "DICOM PS3.1 2014c - Introduction and Overview"., Available: http://medical.nema.org/medical/dicom/current/output/pdf/part01.pdf, 2013.
[10] T. F. Roy , "Architectural Styles and the Design of Network-based Software Architectures"., Ph.D. dissertation, University of California, Irvine, USA, 2000.
[11] SoftwareAG , "MIME-S/MIME Developer's Guide Version 8.2 "., 2011.
[12] Internet Engineering Task Force , "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message specification" , RFC 5751, 2010.
[13] OASIS , "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, 2006
[14] S. Gabriel, S. D. O. Anderson, M. Julien and R. Yves , "Enabling Message Security for RESTful Services"., IEEE 19th International Conference on Web Services (ICWS 2012) , Hawaii, USA, 2012.
[15] P. Gesare, Z. Olaf and L. Frank , "RESTful Web Services vs. "Big" Web Services: Making the Right Architectural Decision"., 17th International World Wide Web Conference (WWW 2008) , Beijing, China, 2008.