의료 정보 교환 시스템의 정보 보안

홍 동 완[0] 주 한 규
한림대학교 컴퓨터공학과
{dwhong, hkjoo}@sun.hallym.ac.kr

Information Security in Hospital Information Exchange System

DongWan Hong[0] Hankyu Joo
Dept. of Computer Engineering, Hallym University

요 약

국내외적으로 의료 데이터의 전산 자동화 처리에 관심과 노력이 기울여 진 후 대부분의 병원에 의료 정보 시스템이 보급되었다. 의료 데이터가 컴퓨터 시스템에 저장되어 병원 내 각 부서별 자원의 공유가 가능하거나 병원 간 자료 전송이 원활하게 이루어진다면 오프라인으로 처리 및 보관하는데서 발생하는 자료의 관리 노력과 비용을 절감할 수 있다. 또한 인터넷 전용선과 광케이블의 보급으로 인하여 원격 시스템 사용이 원활하게 진행될 전망이며, 의료 정보 시스템의 경우 원격 진료 및 환자 정보 검색이 가능하게 된다. 하지만 의료 데이터가 인터넷을 통해 전송될 경우 환자의 사생활 침해 및 의사와 환자 간의 비밀 보장이 파괴될 우려가 남아있게 된다. 데이터 접근 권한 및 데이터 전송에서 오는 보안 기법이 확립되어야 하나, 국내의 경우 의료 정보 유출에 대한 법령과 체계적인 지침 등이 미흡한 상태이다. 이에 본 논문에서는 전자 문서 교환 표준으로 제안되고 있는 XML을 이용하여 의료 데이터가 전송 공유 가능한 병원 정보 교환 시스템(Hospital Information Exchange System : HIES)을 구축하고, 데이터 접근 및 전송에 적용 가능한 보안 기법을 소개하고 있다.

1. 서 론

의료 행위에서 발생하는 데이터 처리가 전산 자동화됨에 따라 환자들의 기초 정보뿐 아니라 진료 데이터는 디지털 데이터 형태로 병원 정보 시스템에 저장되어, 의료인의 연속적인 진단에 효율적인 도움을 주고 있다. 하지만 이와 같은 의료 데이터가 임의의 한 병원에서 공유, 전송 가능하기 위해서는 PACS(Picture Archiving and Communication System)와 같은 대형 시스템을 구비하여야 한다. 투자의 부담으로 인하여 대형 병원에서만 이 시스템을 도입하여 운영되고 있는 상태이다. 또한 외부 병원으로 환자를 이송 및 수탁진료를 해야 하는 경우 시스템의 이질화로 인한 정보 교환이 어려운 상태이다. 현재 의료 데이터의 전자적 교환 표준으로 HL7(Health Level 7)[1]이 제안되었다. HL7은 데이터 표준, 메시지 표준, 문서 표준으로 이루어져 있으며[2] 2002년 상반기에 발표될 버전 3.0에서는 외부 데이터 전송 및 표현(presentation)을 위한 문서 표준으로 XML(eXtensible Markup Language)[3]문서를 표준으로 지정할 예정이다. HL7을 기반으로 시스템을 구축하는 경우, 시스템 간 의료 정보의 교환이 수월할 뿐 아니라 기존의 시스템을 유지한 채 메시지 교환을 할 수 있는 장점을 가지고 있다. 하지만 HL7을 기존의 시스템에 적용하기 위해서는 HL7 툴킷을 구입하여야 하며, 개발하는데 드는 시간적 비용은 여전히 남아 있는 상태이다. 이에 본 연구실에서는 기존의 시스템을 그대로 유지한 채 정보 공유 기능을 제공하는 HIES[4]를 개발하였다. HIES는 내부 메시지 교환으로 XML 문서를 사용하고 있으며, 웹 브라우저를 이용하여 시스템에 접근 가능하므로 웹을 사용할 수 있는 모든 병원에서 쉽게 사용, 가능하다.

HIES에서 처리되는 데이터는 환자의 기초 정보 및 진단 정보를 포함하는 아스키 형태의 데이터와 의료장비(Modality)로부터 획득된 영상 데이터를 사용한다. 기초 정보는 환자 개인 정보, 진료 기록, 원무 기록 등이 포함되며, 특히 진료 기록의 경우 보안이 유지되어야 한다. 의료 데이터는 환자 진료에 관여한 의사에게 열람이 허용되어져 왔으나, 다른 의사가 활용하거나 환자 개인에게도 열람케 하여 진료에 도움이 될 수 있도록 의료법은 지정하고 있다[5]. 의료 정보 접근 권한, 원격 진료 데이터 교환 등이 확대됨에 따라 의료 정보 보안이 큰 문제로 대두되고 있다. 의료 정보 보안이란 정보의 유출 및 수정, 파괴로부터 데이터를 안전하게 보호하는 것으로 개인 비밀 보장 및 자료의 무결성 보장, 시스템 보안 등이 목적이라 할 수 있다. 이에 본 논문에서는 의료 데이터를 접근할 수 있는 효율적인 액세스 제어 및 인증과 외부로 데이터를 전송할 때 효과적으로 암호화할 수 있는 기법을 제시하고 있다.

2. 관련연구

2.1 HIES[4]

병원 정보 시스템의 경우 개발 형태가 내부 전산 팀의 개발 및 외주 개발 형태를 이루고 있다. 이는 표준화 작업의 결여로 병원 정보 시스템이 각 병원의 환경에 맞게 각각 개발되어 자료의 공유가 어려울 뿐만 아니라 심지어 병원의 각 진료과 간의 데이터 교환도 불가능한 상황이다. 전 세계적인 의료 정보 표준화 작업으로 HL7이 진행되고 있다. HL7 프로토콜은 의료 시스템 사용에서 발생할 수 있는 데이터를 메시지 단위로 처리, 전송하는 형태로 RIM(Reference Information Model)[1,2]에 정의되어 있는 정보들을 기반으로 하여 각 세그먼트 필드로 구성한 표준 메시지들을 사용하도록 권고하고 있다. 정보 공유를 위하여 HL7을 이용하려면 HL7 툴킷을 구입하고 HL7 메시지 전송 및 브라우징에 대한 재개발을 하여야 한다. HL7 벤더들은 개발기간을 2-3개월로 예측하고 있지만[1] 중, 소규모 병원의 경우 시스템 추가, 교환 및 재개발에서 오는 투자비용이 부담되는 상황이다. HIES는 본 연구실에서 개발한 시스템으로, 일반 병원 시스템을 그대로 유지한 채 외부 병원 시스템 및 각 진료과 간에 정보를 전송할 수 있다. HIES는 정보공유관리자, 영상 압축/분할 모듈, 정보추출기 등으로 구성되며 그림 1의 구조를 가지고 있다.

① 정보 추출기(Information Extractor) : 의료 정보 시스템에서 산출된 데이터는 DICOM 형태의 자료인데, 구형 장비인 경우 DICOM 포멧을 지원하지 못하는 경우도 있다. DICOM 형태를 지원하지 못하는 경우 컨버트 게이트웨이(Convert Gateway)를 통하여 DICOM 형태의 변환을 거치게 된다. 이렇게 산출된 DICOM 형태의 자료는 레코드 셋 형태의 헤더 정보

와 이미지 정보로 분할 되는데, 정보 추출기는 의료 정보 저장소에 환자의 진단 정보가 담긴 헤더 부분과 영상 데이터를 추출하여 저장한다.

② 정보공유관리자(Information Sharing Manager) : HL7 메시지 생성 및 전송, 브라우징 모듈의 도입없이 정보 공유 관리자가 기존의 시스템 상황을 유지한 채 데이터 공유를 가능하게 해 준다. 타 병원 및 다른 진료과에서 의료 데이터를 참조(Reference)하기 위하여 자료를 요청할 경우 정보 공유 관리자는 의료 정보 저장소에 저장된 스키마 형태와 자료를 요청한 곳의 저장 시스템 간의 스키마 정보를 검사하게 된다. 이 때 공유 스키마 정보가 저장된 지식 베이스를 기반으로 하여 데이터 교환에 지장이 없이 공유 스키마 추출 정보를 생성한다. 그 후 적절한 질의어를 생성한 후, 외부 시스템과 공유할 수 있는 XML 문서를 생성하여 전송하게 된다. 병원 내 진료과 및 외부 병원과의 시스템 연계에서 데이터 교환으로 XML문서가 HL7 메시지 역할을 대신하므로 HL7 툴킷구입 및 개발노력이 필요 없다. 영상 데이터는 원시 데이터(raw-data) 형태로 전송하여 파일 시스템에 그대로 저장하게 된다.

③ 영상 압축/분할 모듈(Image Compression/Partition Module) : 의료 영상 데이터의 경우 저장용량 및 해상도가 상당히 큰 파일 형태로 제공된다. X-ray 영상의 경우 평균 2048×2048 크기를 가지며, 인간이 눈으로 식별할 수 있는 허용치인 8bit resolution을 적용하여 저장할 경우 평균 8-20Mbyte의 소요한다. 다수의 환자들이 진단을 받을 경우 상당히 방대한 저장 공간을 필요로 하게 된다. 이에 HIES는 의료 영상 표준 기술로 제안된 JPEG-LS(ISO/IEC 14495-1)[6] 압축기법을 이용하여 무손실 영상 압축 과정을 거친 의료 데이터를 보관할 수 있다. 또한 고해상도의 의료 영상을 일반 모니터에서 볼 경우 스케일이 조정되어 진단시 정보 손실의 우려를 갖게 된다. HIES에서는 해결 방안으로 2048×2180의 CR 영상이 1024×768의 해상도를 가진 모니터에서 검사되고 있을 때 원영상을 1024×726 영상 크기의 6개 분할(partition)로 제공하여 의사가 원하는 파티션을 선택한 후 스케일 조정 없이 진단을 내릴 수 있다.

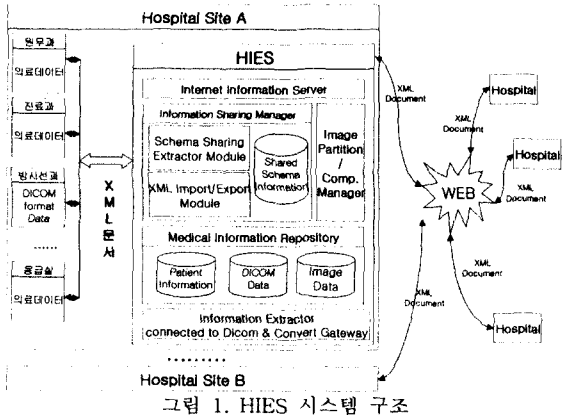

그림 1. HIES 시스템 구조

3. 보안

의료 데이터는 의료인이 환자를 진료한 내용을 포함한 것으로 환자의 생명과 직결될 수 있는 데이터로 함부로 유출되거나 도용될 경우 위험한 결과를 초래할 수 있다. 최근 정부는 의료 정보화 추진 사업 중 의료 정보 전송 표준, 용어 및 코드 등의 표준화, 전자 의무 기록 인증 체계 구축 등의 사업에 있어서 활발한 진행을 보이고 있다. 환자 진료 정보를 보관, 관리, 검색할 수 있는 범위도 의료인에 한정되어 있던 상황에서 일반인에게도 그 범위가 점점 확대되어 가고 있으며, 인터넷 및 고속 통신망의 보급으로 원격 진료 및 의료 데이터의 공유 등이 원활히 수행될 전망이다. 그로 인하여 의료 정보 등이 누출될 수 있는 가능성이 증가하였으나 의료 정보의 보안과 활용에 있어 정보 유출에 대한 법령 및 표준안 등이 정의되어 있지 않은 상황이다. 의료 정보에 대한 보안은 필수 요소로 법, 제도 차원에서의 정의와 기술적인 측면에서의 보안으로 나누어 고려할 수 있다. 첫째 법, 제도 차원에서의 보안을 살펴보면 환자 정보의 사용 기준 및 전산 자료의 관리 및 권한에 대한 제도 등을 정해야 하며 추가적으로 표준 적용 분야, 보건복지부 공통표준 분야, 응용 표준 분야 등으로 분류하여 ISO(the International Organization for Standadization)/IEC(the International Electrotechnical Commission)/SC27(Subcommittee 27)의 표준화를 따르게 해야 한다[7]. 둘째, 기술적인 측면에서 고려할 경우 진료 기록의 접근 통제, 접근 및 사용권한의 분류, 암호화 등이 처리되어야 한다. 이러한 의료 정보 보안 서비스는 키 관리(Key Management), 디지털 서명(Digital Signature), 메시지 인증(Message Authentication), 메시지 암호화(Message Encryption) 등의 정보보안 기술 메커니즘을 이용하여 인증(*Authentication*), 부인봉쇄(*Non-repudiation*), 무결성(Integrity), 기밀성(Confidentiality)을 제공할 수 있다.

PACS와 같은 의료 장비 시스템의 경우 데이터 정의 및 전송에 표준으로 사용하고 있는 DICOM 3.0[8]에서도 보안에 대한 정책 정립이 미루어져 있던 상황이였다. 하지만 DICOM 2000[8]에서 보안 측면의 Part15(Security Profiles)가 추가되었다. 보안의 표준화 사업에 참여하고 있는 단체는 유럽의 CEN TC 251(Comite Europe de Normalisation-Technical Committe 251-Medical Informatics), 일본의 JIRA(Japan Industries association of RAdilogical systems), MEDIS-DC(Mediacal Information System Development Center), 미국의 IEEE, HL7, ANSI로 보안기술 뿐만이 아니라 정책 정의도 진행 중이다. 외부 병원과 같은 분산 및 이질의 시스템에 자료를 전송하는 경우 새로 정립된 DICOM 2000에서도 차후로 정의를 미룬 상황으로 정책 수립 및 구현이 시급한 상황이다.

이 장에서는 웹을 이용한 의료데이터 정보 교환 시스템에 적용할 수 있는 정보 보안 방안으로 사용자가 시스템 사용 및 권한에 대한 접근 제어 및 의료 데이터 전송 시 누출에 대한 보안을 유지하는 암호화 기법에 대하여 기술하겠다.

3.1 접근 제어 및 정보 보안

HIES 사용 시 시스템 접근에 적용할 수 있는 접근 제어 및 데이터 전송에 요구되는 사항을 다음과 같이 6개 항목으로 분류한다.

① 사용자 인증

현재 널리 사용되고 있는 사용자 인증 방법은 패스워드를 이용한 인증이다. 이러한 인증 방법은 패스워드에 대한 추측이나 패스워드에 대한 전수 조사에 취약한 단점을 보인다. 이러한 단점을 해결하기 위하여 HIES에서는 전자서명에 기반한 challenge-response 기법[9]을 사용한다. 이러한 방법을 사용하여 비밀키를 물리적으로 소유한 사용자만이 접근할 수 있으므로 단점을 보완할 수 있다. 사용자는 공개키 암호화 기법에 사용되는 자신의 공개키, 비밀키 쌍을 가지고 있어야 하며, 비밀키를 안전하게 가지고 있다고 가정한다. 공개키 알고리즘은 RSA(Rivest-Shamir-Adleman)[10]를 사용하며 해쉬 알고리즘은 SHA-1[11]을 사용한다. 사용자 인증을 위한 프로토콜은 다음과 같다.

C→S : connect
S→C : randomS
C→S : randomC, S_IP, Sc(randomS, randomC, S_IP), certC

C는 클라이언트, S는 서버, randomS, randomC는 서버와 클라이언트가 생성한 랜덤 정수, S_IP는 서버의 IP주소, Sc는 클라이언트가 자신의 비밀키로 생성한 전자서명(SHA-1 해쉬 후 RSA사용), certC는 클라이언트의 인증서를 의미한다. 클라이언트가 서버에 접속하면 서버는 *randomS*를 생성하여 클라이언트에게 전송한다. randomS를 받은 클라이언트는 randomC를 생성한 후, randomS, randomC, S_IP를 SHA-1으로 해쉬한 후 자신의 RSA 비밀키를 이용하여 해쉬된 결과를 암호화한다. 클라이언트는 생성한 randomC, S_IP와 그에 근거하여 생성한 전자서명, 그리고 자신의 인증서를 서버에 전송한

다. 서버는 자신이 생성하여 보관하고 있는 randomS와 클라이언트로부터 수신한 randomC, S_IP를 이용하여 클라이언트의 전자 서명을 확인한다. 즉, 수신한 전자 서명을 클라이언트의 공개키로 복호화하여 그 결과가 randomS, randomC, S_IP를 SHA-1으로 해쉬한 결과와 동일한가를 검사한다. HIES의 경우 외부 병원으로 데이터를 전송할 경우 HTTP 프로토콜을 사용하여 데이터를 전송한다. HTTP는 스테이트리스(stateless) 프로토콜이므로 하나의 웹 페이지에 접근한 후 다른 페이지로 이동할 때 매번 인증을 다시 해 주어야 한다. 이러한 불편을 해소하기 위하여 세션을 사용한다.

② 사용자 권한

의료 정보를 액세스하기 위하여 로컬이나 리모트 상황에서 접근할 경우 사용자의 등급에 따라 액세스 설정 및 접근 범위를 설정해야 한다. 사용자 등급이란 의료 정보 접근 권한을 지정한 것으로 의료 정보 시스템 사용자를 세분화하여 각 등급의 사용자에 따라 사용범위를 한정한 것이다. 의료 정보 접근 권한은 표 1과 같이 정의할 수 있다. 표 1은 프랑스의 Health Card 95에서 발표된 내용을 국내 실정에 맞게 변환한 내용을 기반으로 하고 있다.

표 1. 의료 정보 접근 권한

(R : Read, W : Write, M : Modify, D : Deny)

	의사	간호사	환자	원무관리자	시스템관리자
기초환자정보	R	R	R	R/W/M	D
진단정보	R/W/M	R	R	D	D
환자건강정보	R/W/M	R/W/M	R	D	D
보험정보	R	R	R	R/W	D
처방전	R/W/M	R	R	D	D
시스템사용자 인증정보	D	D	D	D	R/W/M

③ 데이터 전송에서의 보안

HIES는 의료 데이터 전송에서 인증 및 암호화 통신을 위해 SSL(Secure Socket Layer)/TLS[12]를 사용한다. SSL은 netscape사에서 웹 보안을 위해 개발되었으나 일반적인 프로토콜의 보안에도 이용될 수 있다. TLS는 IETF(Internet Engineering Task Force)에서 개발한 프로토콜인데 SSL v3.0을 표준화하는 단계에서 생성한 것으로 거의 동일하다. SSL은 네트워크 프로토콜의 TCP 계층과 HTTP나 Telnet과 같은 응용 계층의 사이에 위치하여 응용 계층의 교신 내용을 네트워크를 통하여 교신할 때에 암호화하여 기밀성을 제공한다. SSL은 보안 단위로 세션을 이용한다. 세션 동안에는 보안 서비스를 위한 세션키 등을 서로 공유해야 하며 레코드 프로토콜에서 실질적인 보안서비스를 제공한다[12]. 레코드 프로토콜은 실제 소통되는 자료를 암호화하는데 사용되며 대칭키 암호기법을 사용한다. SSL은 키 교환을 위해 사용되는 handshake protocol, 교환된 키 및 관련 정보 확인을 위한 change cipher spec protocol, SSL 사용 시 문제가 발생한 경우 이를 상대방에게 알리기 위한 alert protocol, 실제 소통되는 자료를 암호화하는데 사용되는 레코드 프로토콜로 구성된다[12].

④ 무결성 및 부인봉쇄

현재 의사는 진료 후 환자 진단 정보에 서명을 하여 자신이 진료하였음을 증명한다. HIES에서도 의사는 진단 정보를 작성한 후 자신의 비밀키를 이용하여 전자 서명하도록 하여 자료의 무결성과 메시지 인증 그리고 발생 가능한 부인 봉쇄의 기능을 준다. 전자 서명은 진료 내역에 대해서 SHA-1(Secure Hash Algorithm)[9]를 이용한 해쉬 후 해쉬 된 값을 의사의 비밀키로 RSA 암호 알고리즘을 이용하여 암호화하는 방법을 사용한다. 환자가 자신의 자료를 보는 경우 또는 환자가 다른 병원으로 이송되어 다른 병원에서 환자 진단 정보가 필요한 경우는 의사의 전자서명이 부착된 진단 정보를 제공한다.

메시지의 송신자가 그 메시지를 송신할 때 환자의 진단 정보만을 전송할 경우에는 담당 의사의 전자서명이 필요하지만, 연구용 등으로 샘플링한 결과들을 전송할 경우 병원의 비밀키로 전자 서명을 하게 된다.

전자서명은 메시지의 무결성, 작성자 인증(message origination authentication), 그리고 부인 봉쇄의 기능을 준다.

⑤ 키 관리

공개키 시스템은 공개키와 비밀키로 이루어져 있는데 파일형태의 비밀키는 개인이 보관을 하고 공개키는 인증기관에 의해 인증이 되어야 한다. 비밀키는 안정성을 높이기 위해 대칭키 암호화 기법에 의하여 다시 한 번 암호화 되어있다. 이런 비밀키를 사용하기 위해서는 사용자로부터 패스워드를 받아 해쉬하고 해쉬된 값을 키로 하여 암호화된 비밀키로 복호화하여 사용한다.

⑥ 감사추적

감사추적(audit trails)은 컴퓨터 시스템에서 사용자들이 임의의 사용자들이 액세스한 기록들을 보인다. 감사추적은 보안을 유지하거나 손실된 트랜잭션에 대한 회복기법에 대해서도 유용함을 보이고 있는데, 컴퓨터 시스템 자체나 데이터베이스 시스템에서 제공해 주는 감사추적을 이용하여 모니터링 기능을 수행할 수 있을 뿐 만 아니라 의료 정보 시스템에서 행한 기록까지 추적 가능하다.

4. 결론 및 향후 연구과제

현재 국내외적으로 의료정보보안에 대한 연구가 활발히 진행되고 있다. 의료 정보 시스템은 인터넷 및 초고속 통신 등을 이용하여 원격 진료 같이 의료 행위 범위가 확대되고, 이 때 전송되는 데이터들은 환자의 생명과 결부된 데이터로 안정된 보안기법이 요구되기 때문이다. 본 논문은 현재 프로토타입이 가동중인 HIES에 적용가능한 보안기법에 대하여 논하였다. 현재 데이터 전송 측면에서의 보안이 정립되어져 있으며, 향후 데이터베이스 해킹에 대비하여 의료 데이터를 암호화하여 저장하는 기법과 교환 메시지로 사용하고 있는 XML 문서 내부에 대해 암호화하는 방법을 연구 수행 중에 있다.

참고문헌

[1] "Health Level 7," http://www.hl7.org

[2] Dolin, R.H., Rishel, W., Biron, P.V., Spinosa, J., Mattison, J.E., "SGML and XML as interchange formats for HL7 messages," JAMIA Fall Symposium Suppl., pp. 720-724, 1998.

[3] "Extensible Markup Language(XML) 1.0," http://www.w3.org/TR/1998/REC-xml-19980210

[4] 홍동완, 윤지희, 남궁숙, "XML문서를 이용한 병원정보교환 시스템," 대한의료정보과학회지, Vol. 7, No. 2, 2001.

[5] "의료정보화와 보안의 필요성," http://www.mediface.com/pds_bbs/soc_pds/download.jsp?idx=21

[6] http://idt.net/~dclunie/spie_mi_2000_compression.pdf

[7] 이 필중, "ISO/IEC JTC1/SC27 표준 (Standards)," 한국통신정보 보호 학회지, 제3권 2호, pp.29-35, 1993.

[8] http://medical.nema.org/dicom.html

[9] ISO/IEC 9798-3, Information Technology - Security techniques - Entity authentication mechanism - Part 3: Entity authentication using a public-key algorithm, Internation Organization for Standardization, 1993.

[10]Rivest, R., Shamir, A., Adleman, L. M., "A method for digital signature and public-key cryptosystems," Communications of the ACM, Vol. 21, pp. 120-126, 1978.

[11]FIPS 180-1, "Secure hash standard," Federal Information Processing Standards Publication 180-1, U.S. Dept. of Comerce / NIST, 1995.

[12]A. Freier, P. Karlton, and P. Kocher, "The SSL Protocol Version 3.0," Internet draft, 1996.