XML보안 기술을 적용한 환자의뢰시스템

노형규° 김항찬* 김일곤* 조훈** 곽연식**
경북대학교 정보보호학과
*경북대학교 컴퓨터과학과
**경북대학교 의과대학 의료정보학교실
akira400°@hanmail.net, khc9510@cs.knu.ac.kr, ikkim@knu.ac.kr, hunecho@knu.ac.kr, yskwak@knu.ac.kr

Patient Referral System using XML Security Technology

Hyungkyu Roh° Hangchan Kim* Ilkon Kim* Hune Cho** Yeonsick Kwak**
Graduate School of Information Security, Kyungpook National University
*Department of Computer Science, Kyungpook National University
**Department of Medical Informatics, Kyungpook National University School of Medicine

요 약

최근 XML 문서가 여러 분야의 시스템에서 정보 교환과 메시지 전송을 위한 표준으로 자리 잡으면서 의료계에서도 응용 프로그램 간의 메시지 전송 혹은 병원 간 환자의료정보를 교환하기 위한 XML기반의 정보 교환 프로토콜 표준화가 계속 진행 중에 있다. 하지만 이러한 환자의료정보가 인터넷을 통해 병원간에 이동할 때, 여러 보안상의 위협에 노출될 수 있다. 이에 본 논문에서는 기존의 보안 메커니즘의 한계점을 보완하면서 XML 기반의 정보를 보호하기 위한 가장 효율적인 메커니즘으로 인정받는 XML 보안기술을 적용한 환자의뢰시스템을 시스템을 구현하고 보안 메커니즘 적용 시 부득이하게 발생할 수 있는 성능 저하 정도를 알아보기 위해 성능 평가 테스트를 실시한다.

1. 서 론

컴퓨터 및 정보통신 기술의 급속한 발전으로 인해 의료계에서도 병원전산화 작업이 활성화되고 있으며 개별의료기관의 정보 디지털화 작업도 상당히 진척되고 있다[1]. 또한 이러한 병원 시스템을 기반으로 HL7(Heath Level 7)과 같은 의료정보 전송표준을 이용해서 부서 및 의료기관 간의 의료정보를 교환해서 환자 진료 수준의 질을 높이고 의뢰기관 업무의 효율화를 꾀하고자 하는 움직임이 일고 있다[2].
특히 1, 2차 의료기관에서 3차 의료기관으로 환자의 진료를 의뢰할 경우, 환자는 이전 의료기관에서 시행했었던 검사들을 다시 받아야 하는 경우가 많고 환자가 이전에 받았던 검사기록들을 가지고 간다고 해도 피의뢰 기관에서 활용되는 검사 항목은 아주 제한적이어서 효율적인 업무처리가 되지 못하고 있다. 근래 들어 일부 3차 의료기관들이 인터넷 등을 통하여 환자들의 진료를 의뢰 할 수 있는 환자 의뢰 시스템을 구축하는 경우가 늘고 있지만 이 또한 일부 협력 병원만을 그 대상으로 하는 경우가 많고 대부분이 환자를 의뢰하는 원무적 차원에서 그치기 때문에 1, 2차 의료기관에서 3차 의료기관으로 진료를 의뢰한 환자에게 양질의 진료를 통해 중증을 경감시킨 후 당초 의뢰한 1, 2차 의료기관으로 환자를 회송하여 계속 진료를 받을 수 있게 해 준다는 원래의 취지에는 부합하지 못한 실정이다.
이에 본 논문에서는 의료 환경에서 전자적 데이터 교환을 위한 표준 프로토콜인 HL7(Health Level 7) 메시지를 이용해서 병원들의 이기종 시스템 간에 임상 또는 행정상의 데이터를 송수신할 수 있는 환자 의뢰 시스템(Patient Referral System)을 구축하였다. 또한, 이러한 표준 프로토콜에 환자의 의료정보를 실어서 인터넷을 통해 병원들 사이에 주고받을 경우, 부득이하게 발생하는 보안상의 위협 요소들을 해결하기 위해 XML 보안기술을 적용하였다. 특히, XML 보안기술 중 현재 표준화가 완료되어 있는 XML Signature와 XML Encryption을 적용해서 사용자 인증, 데이터 무결성 및 기밀성 보장, 송수신 부인봉쇄 등의 보안요구사항을 해결하고자 한다. 그리고 사용자 인증, 문서의 서명과 암호화 과정으로 인해 추가적으로 발생하는 오버헤드로 인한 처리속도의 저하를 알아보기 위해 트랜잭션 처리속도를 측정하였다.

2. 관련 연구

2.1 HL7(Health Level 7)

HL7은 서로 다른 보건의료분야 소프트웨어 애플리케이션간 정보가 호환될 수 있도록 하는 규칙의 집합으로 1987년에 처음으로 개발되었으며, 현재 북아메리카에서는 의료정보의 전자적 교환을 위한 사실상의 표준이다[3]. 2000년10월 HL7 Version 2.4가 ANSI 표준으로 인정되었으며, 현재 객체지향 개발 방법론과 RIM(Reference Information Model)을 사용한 Version 3.00이 초안으로 발표된 상태이다[4]. Version 3.0 초안은 XML 인코딩을 사용하고 있다. 그리고 HL7의 또 다른 표준인 CDA(Clinical Document Architecture)는 문서 교환을 목적으로 한 임상문서를 구조적으로 정의한 문서 표준으로 2000년 11월에 CDA release 1이 ANSI 표준으로 승인되었다. CDA문서는 XML로 표현하고 RIM에서 derive되었으며 HL7 version 3 data type을 사용하고 완전한 CDA는 계층적인 구조를 포함한다. CDA문서는 HL7메시지의 한 element로써 MIME type으로 인코딩 되어 포함되어 교환된다. 본 논문에서는 MIME 인코딩된 CDA 문서를 HL7 V2.4 메시지의 OBX 세그먼트의 특정필드에 실어서 전송하도록 했다.

2.2 XML 보안

W3C(World Wide Web Consortium)은 XML 보안 기술과 관련해서 XML Signature, XML Encryption, XKMS(XML Key Management Specification)의 3가지 Working Group을 결성해서 표준화 작업을 진행해 왔다. XML Signature는 XML 문서에 대해 데이터 무결성과 메시지 인증 또는 서명자 인증의 서비스를 제공하며, 2002년 2월 12일에 "Recommendation"으로 제정되었다. XML 문서 교환의 기밀성을 위해 제정한 XML Encryption은 XML 리소스와 XML 문서의 컨텐츠를 일부 혹은 전부 암호화하고 복호화하는데 필요한 정보를 표현하기 위한 XML 문법을 정의하고 있으며, 2002년 12월 10일 "Recommendation"으로 제정되었다. XKMS 워킹그룹은 클라이언트가 웹서비스로부터 키 정보를 얻도록 XML 애플리케이션과 프로토콜 명세를 개발하는 일을 하며, 현재 "Working Draft"상태이다. 본 논문에서는 이 중 표준화가 완료된 XML Signature와 XML Encryption 기술을 이용하였다.

3. 시스템 설계

3.1 환자의뢰 시스템

그림 1은 본 논문에서 구현한 환자의뢰시스템의 전체적인 시스템 구조를 나타낸다. 의뢰 기관의 HL7 Interface Engine에서 version 2.4 메시지를 생성하여 인터넷을 통해 환자 정보를 송신하면 피의뢰 기관의 HL7 Interface Engine이 메시지를 수신해 Patient Administration Management module과 Treatment Management module를 통해 예약일정과 진료 등을 처리하고 환자 정보는 XDB에 저장된다. 보통은 피의뢰 기관에서 환자의 진료가 끝난 뒤 인터페이스 엔진을 통해 퇴원요약정보를 의뢰기관으로 회신을 한다. 하지만, 의뢰기관에서 인터페이스 엔진을 가지고 있지 않을 경우, 환자를 의뢰하고자 하는 주치의는 Web을 통해서 환자를 의뢰하고 퇴원요약정보를 확인할 수 있다.

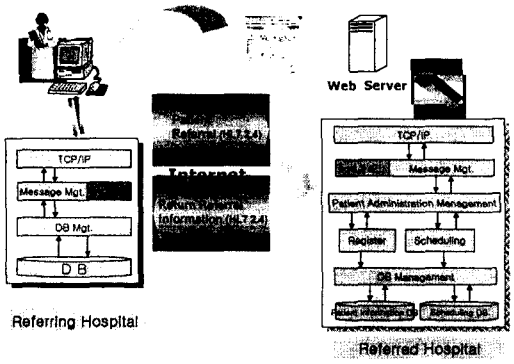

그림 1 환자의뢰 시스템의 전체적인 프레임워크

의료정보가 인터넷을 통해 공유되었을 때 반드시 필요한 것이 보안 솔루션이다. 본 논문에서는 인터넷의 악의적인 공격자들에게 정보가 노출되는 것을 막기 위해 의료정보를 인터넷으로 전송하기 전 암호화 과정을 거친다. 첫 번째 전송 방법인 인터페이스 엔진을 통해 TCP/IP프로토콜로 전송될 때는 XML 암호 기술을 사용했고, 두 번째 방법인 웹 서버를 통해서 전송이 이루어질 경우, SSL 보안 프로토콜을 사용해서 의료정보를 암호화해서 전송한다.

3.2 데이터베이스 설계

그림 2는 기존병원의 환자 퇴원요약정보를 생성하기 위한 기본적인 정보를 가지고 있는 병원 데이터베이스 구조를Entity Relation Diagram으로 설계한 것이다. 본 논문에서 생성한 환자퇴원요약 정보(Patient Discharge Summary)는 기존의 병원 관계형 데이터베이스에서 추출하는 것으로 가정한다. 'adinfo' 엔티티는 특정 환자가 해당 병원에 입원할 때마다 생성되는 데이터로서 환자 퇴원요약정보와 관련된 모든 엔티티는 'adinfo'와 Relationship을 갖는다. 그리고 ICD9CM, ICD10, LOINC Entity들은 병명 및 진단코드를 나타낸 것인데 편의상 모든 attribute를 표기하지는 않았다.

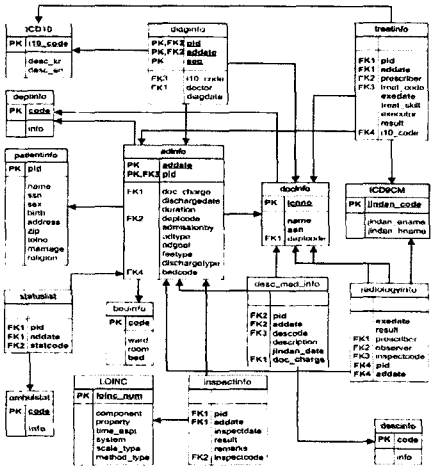

그림 2 ER Diagram of Legacy Hospital Database

그림 3은 퇴원요약정보를 XDB 에 저장하기위해 객체지향적으로 설계된 클래스 다이어그램이다. 이 클래스 다이어그램은 퇴원요약정보 생성에 필요한 데이터를 기존 병원 시스템의 데이터베이스로부터 추출해서 XDB에 XML 문서 형태로 저장하고, XML 문서로 데이터를 추출하기 위한 형태로 작성되었다. PDS(Patient Discharge Summary) 클래스는 환자 퇴원요약정보를 나타내고, PBInfo 클래스는 환자의 기본정보, PAInfo 클래스는 환자의 입원정보를 나타내며, PXInfo, PTInfo, PMInfo, DTInfo, PDInfo는 환자의 진료 및 치료에 대한 정보를 나타낸다. 편의상 클래스의 세부 애트리뷰트는 생략하였다. PDS 클래스에서 전술한 5가지 환자 진료 및 치료에 대한 데이터는 리스트 형태로 데이터를 가지므로 PDS 클래스와 일대다의 관계를 갖는다.

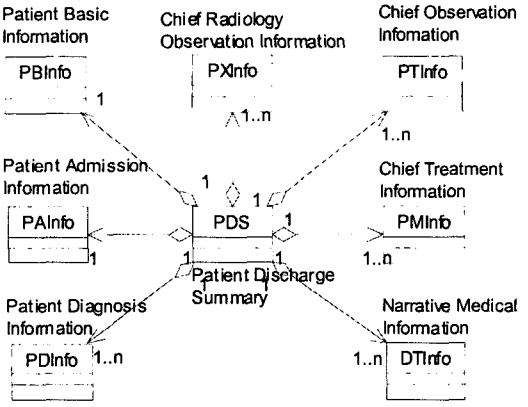

그림 3 환자퇴원요약정보 Class Diagram

병원 데이터베이스에서 환자퇴원요약정보에 필요한 데이터를 추출해서 XDB의 환자퇴원요약 정보 클래스에 mapping하여 XDB에 저장하고, 필요한 경우 XML 포맷의 환자의료정보를 생성해서 XML 암호화와 서명 과정을 거친다음 HL7 메시지에 포함시켜 환자를 의뢰한 병원시스템으로 전달된다. 만약 의뢰한 병원의 시스템이 HL7 메시지를 처리하지 못할 경우 의사는 Web을 통하여 환자의 퇴원요약 정보를 확인해 볼 수 있다.

3.3 보안 설계

3.3.1 암호키 설정과 상호 인증 프로세스

본 논문에서는 문서의 서명을 위해서 공개키 기반구조(PKI)의 공개키와 개인키를 사용하고, 문서의 암호화를 위해서는 시스템의 성능을 고려해서 공개키 암호화를 지양하고 대칭키 암호화를 위한 공유키를 결정한다. 일반적으로 대칭키 암호화의 경우, Key Distribution Center(KDC)라고 불리는 믿을만한 중개자(trusted intermediary)를 이용해서 이루어지지만, 공개키 기반구조의 공개키와 개인키를 사용한다면 KDC를 사용하지 않고도 대칭키 암호화에 필요한 공용키를 확보할 수 있다.

Referral Client와 Referral Server가 암호화 공용키를 생성하고 상호 인증하는 과정은 다음과 같다.

① 임의의 one-time session key, R1을 생성한다.
② R1을 서버의 공개키로 암호화한다.
③ 서버의 공개키로 암호화된 R1(EKs(R1))을 서버로 전송한다.
④ 서버의 개인키로 EKs(R1)을 복호해서 R1을 추출한다. (R1은 향후 서버에서 클라이언트로 전송하는 메시지에 대한 암호키로 사용된다.)
⑤ 서버는 임의의 one-time session key, R2를 생성한다.
⑥ 서버는 R1, R2를 클라이언트의 공개키의 암호화한다. EKc(R1, R2)
⑦ 서버는 EKc(R1, R2)를 클라이언트로 전송한다.
⑧ 클라이언트는 EKc(R1, R2)를 클라이언트 개인키로 복호화해서 R1, R2를 추출한다.(R2은 향후 클라이언트에서 서버로 전송하는 메시지에 대한 암호키로 사용된다.)
⑨ 클라이언트는 추출한 R1을 이용해서 서버를 인증한다.
⑩ 클라이언트는 서버의 공개키를 이용해서 R2를 암호화 한다. EKs(R2).
⑪ 클라이언트는 EKs(R2)를 서버로 전송한다.
⑫ 서버는 EKs(R2)를 서버의 개인키를 이용해서 복호화해서 R2를 추출한다.
⑬ 서버를 추출된 R2를 이용해서 클라이언트를 인증한다.

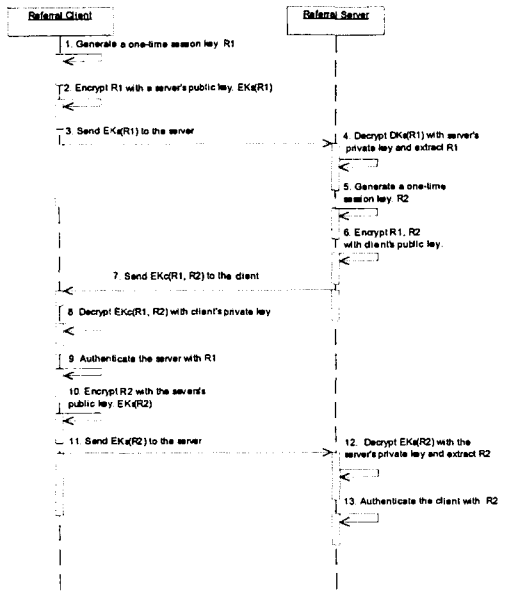

그림 4 암호키 설정과 상호인증 프로세스

위의 과정에서 알 수 있듯이 클라이언트와 서버의 상호 인증은 전형적인 Challenge and Response 프로토콜을 사용하고 있다.

3.3.2 서명 및 암호화 프로세스

아래 그림은 환자의뢰 시스템에서 1, 2차 병원의 담당의사가 3차 의료기관에 환자퇴약정보(Patient Discharge Summary)를 요청했을 경우, 3차 의료기관의 XDB에서 CDA 표준에 준하는 XML 문서가 생성되어 의뢰 기관의 RDB에 문서가 저장되기까지의 전체적인 과정을 순차적으로 보여주고 있다.

이 과정 중에 XML 문서에 대한 서명과 검증, 암호화와 복호화 과정을 거치게 된다. 서명과 검증을 위해서는 공개키 기반구조의 비대칭키가 사용되고, 암호화와 복호화를 위해서는 클라이언트와 서버간의 상호인증 과정에서 사용된 임의의 공유키(one-time session key) R1, R2가 사용된다.

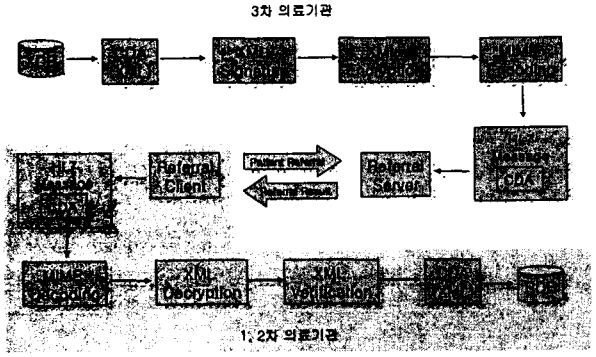

그림 6 환자퇴원요약 정보의 전체적인 흐름

4. 시스템 구현과 성능 평가

이 논문의 환자의뢰 시스템의 구현 환경은 표 1과 같다. HL7 인터페이스 엔진으로 사용된 Chameleon v3.211은 HL7 v2.4를 지원한다. 그래서 본 시스템에서는 CDA 문서를 MIME 인코딩하여 HL7 v2.4 메시지의 OBX세그먼트에 실어서 전송했다.

표 1 구현 환경

	Server	Client
운영체제	Windows 2000	Windows 2000
사용언어	C#	C#
암호, 서명 라이브러리	XMLSafer 1.0	XMLSafer 1.0
DBMS	Cache v5.0, Oracle 9i	Oracle 9i
HL7 Interface Engine	Chameleon v3.211	Chameleon v3.211

그리고 성능 평가 테스트의 결과, 보안 기술의 적용 시 가장 우려가 되는 성능의 저하는 그다지 염려할만한 수준이 아닌 것으로 나타났다.

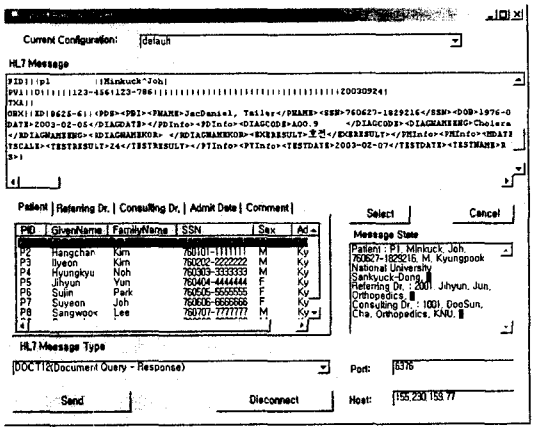

그림 7 환자의뢰시스템 클라이언트 구현 화면

5. 결론

본 논문에서는 의료 환경에서 전자적 데이터 교환을 위한 표준 프로토콜인 HL7(Health Level 7) 메시지를 이용해서 병원들의 이기종 시스템간에 임상 또는 행정상의 데이터를 송수신할 수 있는 환자 의뢰 시스템(Patient Referral System)을 구축하였다. 특히, 임상 데이터의 경우 CDA release 1을 준하는 XML 문서의 형태로 전송이 이루어진다.

이러한 임상 문서가 인터넷을 통해 이동할 때 필연적으로 발생하는 보안 문제를 해결하기 위해서 XML 암호화와 서명 기술을 적용하여 문서의 기밀성과 무결성, 시스템의 인증과 부인방지의 보안요구사항을 해결하였다. 그러나 이러한 보안 기술의 적용 시 부가적인 암호화와 서명 프로세스로 인해, 부득이하게 나타나는 성능 저하를 완화시키기 위해서 공개키 암호화를 지양하고 대칭키 암호화 기술을 적용하여 시스템의 성능 저하를 완화시켰다.

향후 연구로는 HL7 Version 3과 CDA 표준이 완성된 후, 그 표준에 준하는 Version 3 인터페이스 엔진과 CDA Builder를 이용한 환자의뢰시스템을 구축하는 것이다.

참고 문헌

1. Mandle KD, Kohane IS. Healthconnect: Clinical grade patient-physician communication. In Proceedings, AMIA Annual Symposium 1999
2. Sooyung Yoo, Boyoung Kim, Jinwook Choi, Jaeheon Cheong, Jonghoon Chun, "Development of HL7 Message Server with Laboratory Common View Layer", Proceedings of The 29th KISS Spring Conference, 2002
3. HL7 Korea, http://www.hl7korea.org/
4. HL7 Standards, http://www.hl7.org/
5. H. X. Mel, Doris Baker, "CRYPTOGRAPHY DECRYPTED", Addison-Wesley, 2001
6. James F. Kurose, Keith W. Ross, "Computer Networking", Addison-Wesley, 1999
7. XML Signature Specification, http://www.w3.org/TR/xmldsig-core/