XML/DTD 전자서명을 이용한 안전한 처방전 전송 시스템에 관한 연구

김형균* · 배용근**

A Study on the Secure Prescription Transmission System using XML/DTD digital signature

Hyeong-Gyun Kim* · Yong-Guen Bae**

이 논문은 2006년도 조선대학교 연구비의 지원을 받아 연구되었음

요 약

본 논문에서는 XML을 기반으로 한 처방전 전송 시스템을 제안하고, XML/EDI의 암호화를 위하여 XML 문서에만 전자서명을 첨부하는 것이 아니라, DTD에 전자 서명을 첨부하는 방법을 사용함으로써 보다 안전한 처방전 전송 시스템을 구축하고자 한다. 처방전 DTD는 앞서 살펴본 처방전의 각 구성요소에 따라 처방전 정보, 환자 정보, 의료기관 정보, 처방내역 정보, 조제내역 정보 엘리먼트를 정의하고 그 하위에 정보 전송에 따른 정보를 관리하기 위한 하위 엘리먼트를 정의하였다. 안전한 처방전 전송을 위하여 DTD파일을 읽어 들이면서 파싱을 하고 여기서 추출되는 엘리먼트나 속성, 엔티티들을 해시테이블에 저장한다. 파싱이 종료되면 해시 테이블을 읽어 들여서 메시지 다이제스트를 수행하고 이를 개인키와 합성하여 전자 서명을 생성한다.

ABSTRACT

We propose a prescription transmission system based on XML in this paper, and it is not to attach a former signature to only a XML document for encoding of XML/EDI, and it is construction, one with the prescription transmission system which is safer with what use a way to attach a digital signature to DTD. I defined sub element to manage information prescription DTD defined prescription information, patient information, medical care organ information, prescription details information, compounding of medicines details information element according to for each a component of a prescription I went along, and to have looked up, and to have obeyed information transmission at he low rank. I read a DTD file for safe prescription transmission, and I do element or property, the entity which I do it, and is extracted here, and Pasing is saved in a table while being a field. If Pasing is finished, I read and lift a hash table and carry out message a digest. I compose it with an early private key and create a digital signature.

키워드

XML, DTD, Digital Signature, Prescription

* 동강대학 컴퓨터인터넷계열

** 조선대학교 전자정보공과대학 컴퓨터공학부

접수일자 : 2006. 11. 1

Ⅰ. 서 론

DTD는 XML을 표현하기 위한 메타 컨텐츠를 가지고 있는 파일로서, 문서내의 데이터에 대한 의미의 구별, 문서의 유효성 검증을 목적으로 한다[2][3]. 그러므로 DTD에 대해서도 XML 자체의 보안에 상응하는 보안 정책이 요구된다. 그러나 하나의 XML 문서는 오직 하나의 DTD를 기반으로 작성되어야 하고 엘리먼트 선언의 확장성이 떨어지는 등의 많은 DTD의 제약 사항으로 인해 효과적인 DTD 보안 정책은 제시되어 있지 않다.

국내 의료분야의 경우 병원의 조직간 전자상거래의 역사는 1994년 5월 의료보험 연합회와 한국통신이 공동으로 의료보험 EDI 시범사업을 통해 진료비 청구와 지불을 위한 의료부문 EDI 시스템의 구축을 통하여 시작되었다. 2000년 7월 의약분업의 실시로 인해 의료기관의 입장에서는 종이처방전 발행과 관리에 따른 비용이 발생하며, 수기로 된 종이처방전을 발행하였을 경우 처방전 발행, 진료기록, 진료비청구자료 작성이라는 작업이 분리되므로 인건비 부담이 증가하게 된다. 약국에서도 처방전 자료의 재입력과 건강보험청구 심사자료 작성의 이중 작업이 생기며, 의료 이용자는 의료기관과 약국을 동시에 방문해야 하고 처방에서 조제에 이르는 시간이 증대되어 시간자원이 낭비될 수 있다. 또한 처방전이 분실되는 경우 조제 지연 및 조제를 포기하는 등 오히려 건강이 악화될 가능성도 있다. 또한 의사의 수기처방전 또는 훼손된 처방전의 판단착오로 약사의 오독으로 인해 잘못된 약을 조제하여 환자의 건강이 문제가 될 수도 있다.

따라서, 본 논문에서는 XML을 기반으로 한 처방전 전달 시스템을 제안하고, XML/EDI의 암호화를 위하여 XML 문서에만 전자서명을 첨부하는 것이 아니라, DTD에 전자 서명을 첨부하는 방법을 사용함으로써 보다 안전한 처방전 전달 시스템을 구축하고자 한다.

Ⅱ. 관련 연구

보안에 대한 요구사항 중 기밀성, 무결성, 인증에 관련된 사항은 암호화 방법을 이용하여 해결이 가능하다. 그러나 부인 봉쇄에 대해서는 전자 서명(digital signature)을 이용한다[4]. 전자 서명이란 상대방에게 송신자의 신뢰성을 증명해주는 방법이다. 즉 임의의 공격으로 인한 문서 위조를 방지하기 위한 기법으로, 상대방에게 전자적으로 작성된 서명이 첨부된 형태의 문서를 전송하여 수신자로 하여금 확인 가능하게 한다.

XML 전자 서명은 XML문서의 해시 값을 계산하고 이것을 서명자의 개인키로 암호화한 결과를 서명 값으로 활용한다.

그림 1은 전자 서명이 삽입된 XML문서를 보여주고 있다. <sign>요소의 내용이 원 문서에 대하여 삽입된 전자 서명이다.

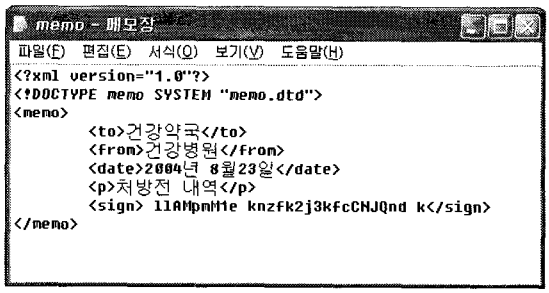

그림 1. 전자서명이 삽입된 XML문서
Fig.1. XML document that digital signature is inserted

XML 전자 서명의 중요한 고려사항은 공백 문자 처리, 속성 기본 값, 문자 인코딩이 다른 XML 문서에 대해서도 논리적으로 내용이 동일하다면 같은 서명 값을 생성해야 한다는 점이다. 이에 대한 해결 방안으로 정규형 XML과 DOMHash 기법이 있다. XML 문서는 DTD 또는 XML 스키마에 기반을 두어 작성된다. 그림 2는 DTD 기

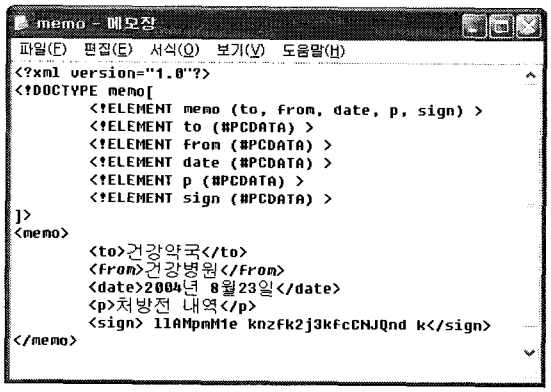

그림 2. DTD 기반의 XML 문서
Fig. 2. XML document of DTD base

반 하에 작성된 XML문서를 보여주고 있다. XML 문서의 데이터를 표현하는 메타 데이터 집합인 DTD는 여러 계층에서 공유되고 있다. 그런데 이러한 DTD의 공유 및 메타 컨텐트 관리 측면에서 DTD의 보안 기법은 매우 중요함에도 불구하고, 현재의 연구는 XML 문서의 데이터 암호화에 초점이 맞추어져 있다.

Ⅲ. XML 기반의 안전한 처방전 전달 시스템

3.1. 안전한 처방전 전달 시스템의 개요

본 논문에서 제안한 시스템에 의해 전달되는 처방전 정보의 흐름은 그림 3과 같다. 환자가 병원을 방문하여 진료를 받게 되면 처방전이 생성된다. 다음으로 환자가 약국을 방문하면 해당 병원에 처방전 요구를 하게 되고 전달된 처방전에 의해 약을 조제한 후 조제하였다는 정보를 병원에 전달하여 병원에서 다른 약국으로 동일한 처방전을 전달하지 못하게 한다. 또한 병원과 약국은 국민건강보험관리공단으로 처방내역과 조제내역을 전달하여 보험청구 심사를 받아 그 결과를 제공받는다.

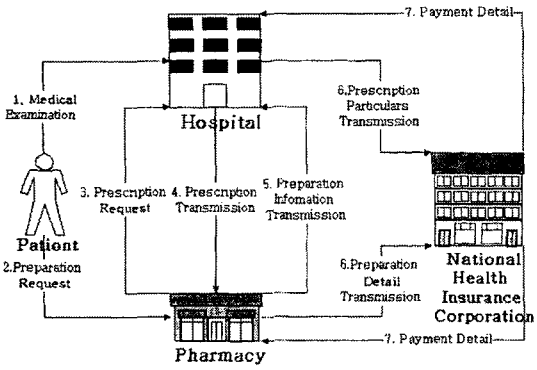

그림 3. 처방전의 흐름도
Fig. 3. Flowchart of Prescription

3.2. 처방전 DTD 설계

처방전 DTD는 처방전의 각 구성요소에 따라 처방전 정보, 환자 정보, 의료기관 정보, 처방내역 정보, 조제내역 정보 엘리먼트를 정의하고 그 하위에 정보 전송에 따른 정보를 관리하기 위한 하위 엘리먼트를 그림 4와 같이 정의하였다.

대표 엘리먼트들을 구성하는 각각의 엘리먼트에 대하여 특성표를 작성하여 엘리먼트의 반복 횟수에 따른 특징을 구분하고, 그림 4와 같이 계층 구조도를 작성하여 대표 엘리먼트와 하위 엘리먼트의 계층성을 파악하여 DTD를 설계하여, 설계된 DTD를 기반으로 XML 파일을 구성하였다. 그리고 엘리먼트들 사이에는 선택적 연산자를 이용하여 필요한 사항만 수시로 입력할 수 있도록 하였다.

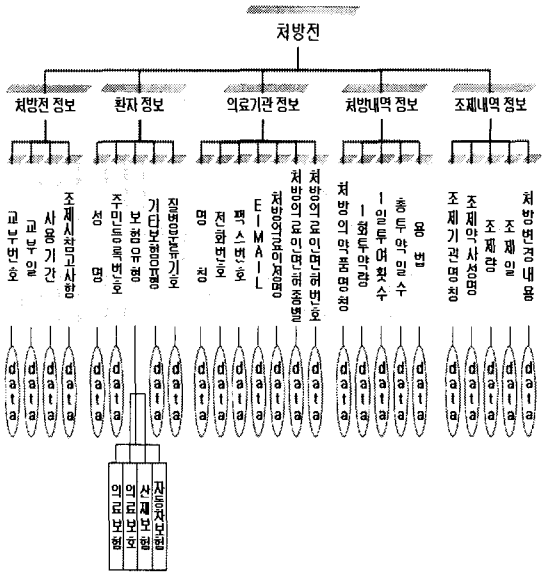

그림 4. 처방전 엘리먼트 구조
Fig. 4. Structure of Prescription Element

3.3. 안전한 처방전 전달

안전한 처방전 전달을 위하여 XML/ EDI 과정에서 XML 문서에만 전자서명을 첨부하는 것이 아니라, DTD에도 전자 서명을 첨부한다. 원본 DTD 문서의 메시지 다이제스트 값을 첨부함으로써 DTD 문서에 대하여 신뢰성을 부여한다. 애플리케이션에서 XML 문서 처리 전에 서명 값을 검증함으로써 정보 유출 등의 문제를 극복할 수 있다. 문제점은 DTD 내에 존재하는 엘리먼트 선언들의 순서문제이다. 전자 서명 시, 메시지 다이제스트 과정에서 바뀐 순서에 대해서는 검사하지 못하기 때문에 논리적으로 같더라도 전혀 다른 다이제스트 값을 생성하기 때문이다. 이 문제는 XML 전자 서명에서 나타난 것과 동일한 것으로 XML 정규화를 DTD에 적용시키는 정규 DTD 생성 등이 해결책으로 제시될 수 있다. 그러나 이는 DTD 파서가 따로 요구되며 DTD의 정규화를 위해

또 다른 구문법의 정의가 요구되는 등 많은 시간과 노력이 소요된다. 따라서 본 논문에서는 DOM을 이용하여 DTD의 전자 서명을 생성하는 방법을 그림 5와 같이 제안한다.

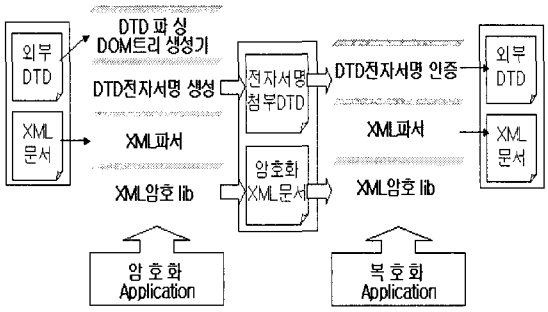

그림 5. DTD전자서명을 이용한 XML암호화 과정
Fig. 5. XML encryption process that use DTD digital signature

본 논문에서 DOM구조를 바탕으로 DTD를 파싱하는 방법을 이용하여 해결하려는 이유는 DOM은 구조에 대하여 표준화가 되어 있으며 문서 전체에 대한 트리구조를 구현할 수 있다는 점에서 문서 구조의 정규화에 유리한 장점을 가지고 있기 때문이다.

3.4. 시스템 평가

정보 교환시 중요 고려 사항은 정보의 신뢰성과 보안에 있다. 그리고 보안의 생명은 정보 탈취 또는 서비스 거부와 같은 공격에 효과적으로 대처하여 안전한 정보 제공 및 서비스 이용에 있다. 본 논문에서 제안한 방법은 XML 암호화 기법과 XML 전자 서명 기법이 합성된 방법으로 기존의 XML 엘리먼트 암호화 기법과의 비교 및 XML 전자 서명 방법에 대한 비교로 구분하여 평가하였다.

3.4.1 XML 엘리먼트 암호화 기법의 비교

XML 엘리먼트 암호화 기법에 있어 본 논문에서 제시한 방법과 기존의 방법과의 차이는 그림 6에 제시하였다. 기존의 방법은 IBM-XMLenc(Element-wise XML Encryption), sXML(secure XML)로 명명하였다.

제안한 방법의 경우 기존의 연구에 비해 가장 큰 장점은 유효성을 유지할 수 있다는 점이다. IBM- XMLenc의 경우 정형 XML에 대해서만 암호화 기능을 제공하고 있다. 이는 엘리먼트에 대해 암호화 기능을 제공한다는 장점은 있지만 현실과는 맞지 않는 DTD에 기반하지 않은 XML문서만을 지원하므로 정보 교환에 있어 XML 애플리케이션이 문서의 구조를 이해하지 못하는 한계를 가지고 있다.

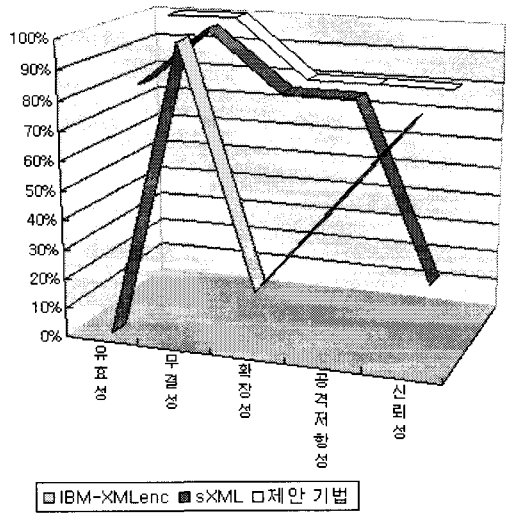

그림 6. XML 엘리먼트 암호화 기법의 비교
Fig. 6. comparison of XML element encryption method

3.4.2 XML 전자 서명 관점에서의 비교

본 논문에서 제안한 방법 중 일부인 전자서명 기법에 대한 비교는 그림 7에서 제시하였다. 비교 대상은 XML 전자 서명에 많이 사용되는 방법 중에서 중간 과정인 정규화 기법과 DOMHash를 이용한 방법이다. 비교한 내용은 본 논문에서 제안한 방법인 XML 전자 서명은 그대로 지원하면서 동시에 DTD 전자 서명까지 지원하는 경우의 장단점을 항목별로 분석한 것이다. 먼저 정규화 기법은 문자 인코딩에서 다른 두 가지 방법에 비해 UTF-16 유니코드를 지원하지 못하는 단점을 나타내었다. 그리고 DOMHash 의 경우는 빠르고 정확한 서명 값을 생성할 수 있는 장점이 있는 반면, 정형 XML 문서만을 지원한다는 단점을 가지고 있다. 본 논문에서 제안한 방법은 이러한 문제에 대하여 DOM에 기반한 해시 함수를 사용하여 DOMHa sh의 장점과 앞에서 비교하였던 내용인 XML스키마를 이용하는 방법으로 정형 XML문서 뿐만 아니라 유효한 XML 문서에 대해서도 전자서명이 가능하도록 지원하는 장점을 가지고 있다. 그러나 문서에 대한 전자서명을 XML문서 외에 DTD에도 적용함으로써 처리속도가 늦어지는 단점이 있다.

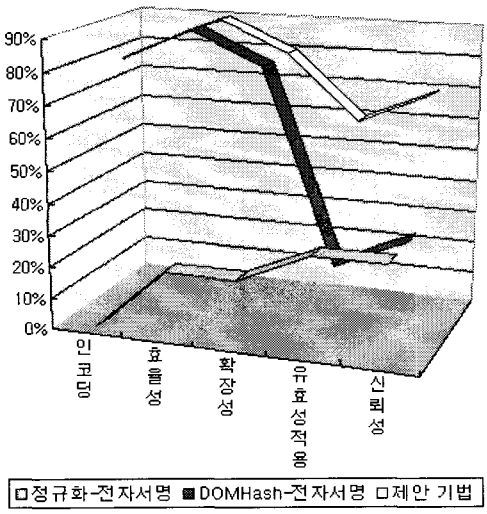

그림 7. XML 전자 서명 기법의 비교
Fig. 7. comparison of XML digital signature method

Ⅳ. 결 론

본 논문에서는 XML을 기반으로 한 처방전 전달 시스템을 제안하고, XML/EDI의 암호화를 위하여 XML 문서에만 전자서명을 첨부하는 것이 아니라, 처방전 DTD에 전자 서명을 첨부하는 방법을 사용함으로써 보다 안전한 처방전 전달 시스템을 구축하였다. 처방전 DTD는 처방전의 각 구성요소에 따라 처방전 정보, 환자 정보, 의료기관 정보, 처방내역 정보, 조제내역 정보 엘리먼트를 정의하고 그 하위에 정보 전송에 따른 정보를 관리하기 위한 하위 엘리먼트를 정의한다. 안전한 처방전 전송을 위하여 DTD파일을 읽어 들이면서 파싱을 하고 여기서 추출되는 엘리먼트나 속성, 엔티티들을 해시테이블에 저장한다. 파싱이 종료되면 해시 테이블을 읽어 들여서 메시지 다이제스트를 수행한다. 이를 개인 키와 합성하여 전자 서명을 생성한다.

본 논문에서 제안한 방법은 기존의 XML 엘리먼트 암호화 기법과 XML 전자 서명의 관점에 중점을 두었으며 XML 접근 제어 관점에서는 DTD 접근 제어의 적용 가능성을 제시하였다. XML 문서의 암호화를 통해 얻을 수 있는 가장 큰 효과는 XML 명세가 갖고 있는 한계인 데이터의 내용과 표현의 분리에만 치중하여 보안상의 헛점을 가지고 있던 단점을 극복할 수 있게 되었다는 점이다. 그러나 유효한 XML문서를 제대로 지원하지 못하는 문제를 가지고 있었다. 이러한 문제를 해결하고자 본 논문에서 제시한 방법은 다음과 같은 특징을 가지고 있다. 첫째, 유효성을 고려한 XML 문서의 암호화 및 복호화 처리를 가능하게 하여 웹 상에서의 XML문서 교환시 브라우저에서 발생할 수 있는 DTD에 기반한 원활한 정보 공유를 지원할 수 있다는 점이다. 기존 연구의 한계인 정형 XML 문서에만 적용할 수 있었던 XML 엘리먼트 암호화를 유효한 XML 문서에까지 적용할 수 있는 장점을 갖는다. 둘째, 기존의 XML 전자 서명 기법에서도 문서의 유효성 유지 기능을 지원하고, 동시에 DTD에 전자서명을 부여하는 방법을 지원함으로써 XML문서의 무결성을 DTD에까지 확장 가능하게 하였다. 결과적으로 XML 데이터 교환에 대한 신뢰성이 높아지는 효과를 얻을 수 있다. 마지막으로 DTD의 접근 제어 측면을 고려해 보면 기존의 시스템에서 발생할 수 있는 DTD의 파괴와 같은 문제점을 접근 권한 부여 기법을 이용하여 보완함으로써 보다 강력한 보안 기능의 지원이 가능하다는 점이다. 또한, XML 접근 제어 측면에서 본다면 DTD 접근 제어를 가능하게 하였다. 그러나 유효성 유지를 위해 XML 스키마를 생성하는 등의 복잡한 작업이 수행되어야 하며, 자바로 구현되어 다른 언어로 구현된 시스템과 비교했을 때 느린 속도를 극복하기 어려운 단점이 있다. 또한 XML 명세의 제약으로 인해 애플리케이션으로만 해결할 수 밖에 없는 한계점을 지니고 있다. 추후 연구과제로 느린 속도 문제를 극복할 수 있는 방안과, 실험 결과 미해결 상태로 남아 있었던 스타일 시트에서 보안 기능을 지원하는 방법 등이 있다. 또한, 접근 제어에 관련하여 XML 스키마에 적용할 수 있는 XML 접근 제어 기법 또한 해결해야할 과제일 것이다.

참고문헌

[1] ST I- SECURITY Technologies Inc, "J/LOCK - Java Cryptography Package", March , 2000.

[2] Takeshi Imamura, Hiroshi Maruyama, "Specification of Element - wis e XML Encryption ", W3C XML-Encryption Workshop, November , 2000.

[3] Michiharu Kudo, Satoshi Hada, "XML Document Security based on Provisional Authorization",

Conference on Computer an d Communication Society , Athens . Greece, Nov ember . 2000.

[4] E. Damiani, S Vimercati, S. Paraboschi, P. Samarati, "Design and Implementation of an Access Control Process or for XML Documents ", Proceedings of 9th International World Wide Web Conference, Amsterdam, May , 2000.

[5] E. Bertino, M, Braun , S. Castano, E. Ferrari, M. Mesiti, "Aurhor - χ: a Java - Bas ed System f or XML Data Protection ", Proceeding of th e 14th IFIP WG 11.3 Working Conference on Database Security , Schoorl. Netherlands , August . 2000.

[6] H. Maruyama, K.Tamur a, N. Uramoto, "XML and Java, Developing Web Applications ", Addison Wesley , May, 1999

[7] William J .Pardi, "XML in Action, Web Technology ", Microsoft Press , 1999.

[8] Jonathan Knudsen , "Java Cryptography ", O'REILLY, 1998.

저자소개

배 용 근(Yong-Guen Bae)

1984년 2월 조선대학교 컴퓨터 공학과 공학사
1987년 2월 조선대학교 대학원 공학석사
1993년 2월 원광대학교 대학원 공학박사
1997년~2007년 현재 조선대학교 컴퓨터공학부 교수
※관심분야 : 마이크로프로세서, 프로그래밍언어

김 형 균(Hyeong-Gyun Kim)

1998년 2월 조선대학교 대학원 공학석사
2004년 2월 조선대학교 대학원 컴퓨터공학과 공학박사
2002년~ 2007년 현재 동강대학 컴퓨터인터넷과 초빙전임강사
※관심분야 : 임베디드 리눅스, 모바일컨텐츠, P2P