제18회 한국정보처리학회 추계학술발표대회 논문집 제9권 제2호 (2002.11)

의료정보시스템의 전자서명 적용 모델

이용준*, 오동열*, 정재동*, 오해석*
*숭실대학교 대학원 컴퓨터학과
mail: yjlee@koscom.co.kr

Model for Digital Signature of Hospital Information System

Yong-Jun Lee*, Dong-Yeol Oh*, Jea-Dong Jong*, Hea-Suk Oh*
*Dept of Computing, Graduate School Soongsil University

요 약

인증서기반의 전자서명은 의사의 처방전을 전자문서 형태로 병원의 해당부서로 전달하거나 진료기록의 경우 내용이 임의로 수정되거나 변조되는 것을 방지한다. 전자서명은 내용을 증명하고 처방전을 기록한 의사의 신원을 확인한다. 아직 병원에서 약국까지의 처방전 이용에 전자서명을 이용하고 있는 경우는 없고 병원 자체적인 문서전달 수단으로 전자서명을 활용하는 데 그치고 있다. 그러나 머지않아 의료 전분야에 걸쳐 전자서명이 활성화될 것으로 전망하고 있다. 본 논문에서는 신뢰할 수 있는 의료정보 시스템을 보장하기 위하여 의료정보 시스템에 전자서명 적용 모델을 제안하고자 한다. 제안하는 모델은 의사의 처방전과 진료기록에 대하여 문서형태에 전자서명을 관리하여 판독성과 무결성을 보장한다.

1. 서론

최근 의료정보 시스템에서 진료기록 및 처방전에 전자서명이 적용되고 있다. 현재 종이 진료기록부와 마이크로필름, 광디스크의 전자진료기록은 임의수정이나 변조 가능성 때문에 의무기록으로서의 법적 효력이 제한되고 있지만 전자서명은 이를 보완해줄 기술로 평가받고 있다[1].

인증서기반의 전자서명은 의사의 처방전을 전자문서 형태로 병원의 해당부서로 전달하거나 진료기록의 경우 내용이 임의로 수정되거나 변조되는 것을 방지하고 전자서명을 이용해 내용을 증명하고 처방전을 기록한 의사의 신원을 확인한다[2].

아직 병원에서 약국까지의 처방전 이용에 전자서명을 이용하고 있는 경우는 없고 병원 자체적인 문서전달 수단으로 전자서명을 활용하는 데 그치고 있다. 그러나 머지않아 의료 전분야에 걸쳐 전자서명이 활성화될 것으로 전망하고 있다[3].

본 논문에서는 신뢰할 수 있는 의료정보 시스템을 보장하기 위하여 의료정보 시스템에 전자서명 적용 모델을 제안하고자 한다. 제안하는 모델은 의사의 처방전과 진료기록에 대하여 문서형태에 전자서명을 관리하여 판독성과 무결성을 보장한다[4-7].

본 논문의 구성은 다음과 같다. 2장에서는 의료정보 시스템과 전자서명에 대한 기존연구를 살펴보고, 3장에서는 의료정보 시스템에 전자서명 모델을 제안한다. 4장에서는 본 논문에서 제안한 모델의 기대효과를 평가하고, 마지막으로 5장에서 결론을 맺는다.

2. 관련연구

의료정보시스템은 환자의 인적정보, 처방내역, 검사결과를 기본으로 의사가 기재하는 진료기록과 디지털 의료영상을 전산에 입력하여 보다 진보된 시스템으로 발전하고 있다. 그러나 의료정보의 데이터 무결성과 보안을 제공하는 전자서명에 대해서는 초기단계에 머무르고 있다[8-9].

2.1 처방전달시스템

처방전달시스템 (OCS : Order Communication System)

은 진료행정시스템과 진료정보제공시스템으로 크게 나눌 수 있으며 과거 행정 중심에서 현재 진료지원 중심으로 변해가는 추세다. 각종의학정보 및 환자들의 진찰자료를 보관한 데이터베이스와 의사가 환자를 진단한 후 처방전을 통신망을 통해 각 해당 진료부서로 전달해주는 시스템이다. 이 시스템은 환자의 등록에서 진료, 수납까지 원내의 모든 데이터를 관리 전달하는 것은 물론 병원의 모든 행정을 효율적으로 관리할 수 있도록 하는 통합의료 정보시스템이다.

2.2 전자의무기록

전자의무기록 (EMR : Electronic Medical Record)은 병원에서 사용되는 종이문서 대신 데이터를 전산매체에 저장하는 방식이다. 현재의 종이 의무기록은 일정기간 이후에는 관리 및 보관상에 한계가 오기 때문에 마이크로필름 또는 광디스크 등에 저장하여 관리한다. 처방전달시스템 환경에서는 환자의 인적상황, 처방내역, 검사결과 등이 텍스트형태로 입력되어 진료 중에 활용하고 있다. 이에 더하여 의사가 기재하는 진료기록만을 전산에 입력하여 보다 진보된 전자의무 기록이 구축한 시스템이다.

2.3 의료영상저장전송시스템

의료영상저장전송시스템(PACS : Picture Archiving & Communication System)은 의료영상 특히 방사선학적 진단 영상들을 디지털 상태로 획득한 후 고속의 네트워크를 통하여 전송한다. 과거의 필름의 보관 대신에 데이터로 의료영상을 저장하며, 진단방사선과 의사와 임상의사의 기존의 필름 판독 대신에 전산단말기의 영상을 이용하여 환자를 진료하는 포괄적인 디지털 영상저장 및 전송시스템을 말한다. PACS의 궁극적인 목표는 필름이 없는 의료정보 시스템을 구축하는 것이다.

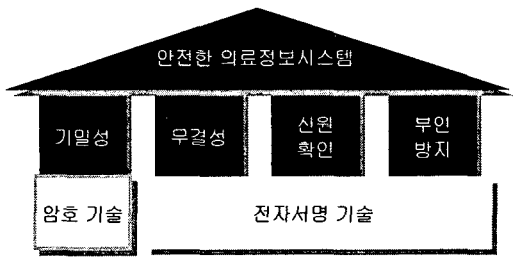
2.4 전자서명

OCS, EMR, PACS는 의료정보에 대하여 전송과 운영에 발전을 하였으나 의사에 대한 인증과 데이터의 무결성은 보장하지 못한다. 따라서 안전한 의료정보시스템을 위해서는 전자서명 적용이 요구된다.

인증서 기반의 전자서명은 개인키의 소유자만이 할 수 있으며, 전자서명의 진위여부를 확인하는 절차를 전자서명검증이라고 한다[6-7]. 전자서명검증은 개인키의 소유자 확인과 개인키에 합치하는 공개키의 획득, 그리고 전자서명값 자체에 대한 확인절차를 수행하게 된다[8]. 개인키 소유자 확인과정은 인증서 상태 검증을 통해서 이루어지게 되는데 인증서는 개인키에 해당하는 공개키를 가지고 있기 때문이며, 공개된 사용자의 공개키가 그 소유자와 대응되는지를 확신할 수 있어야 한다[10-12].

[그림 1]에서 기술한 것처럼 안전한 의료정보시스템을 위해서는 4가지 기능이 요구된다[9-12].

- 기밀성(Confidentiality)
  적법한 의료인 외에는 열람 불가
- 무결성(Integrity)
  전자처방, 검사결과의 송수신 문서의 위,변조 불가
- 신원확인(Authentication)
  의료인의 신원 확인
- 부인방지(Non-repudiation)
  전자처방, 검사결과 행위의 부인봉쇄



[그림 1] 안전한 의료정보시스템

3. 제안하는 의료정보 시스템의 전자서명 모델

3.1 의료정보시스템의 구성요소

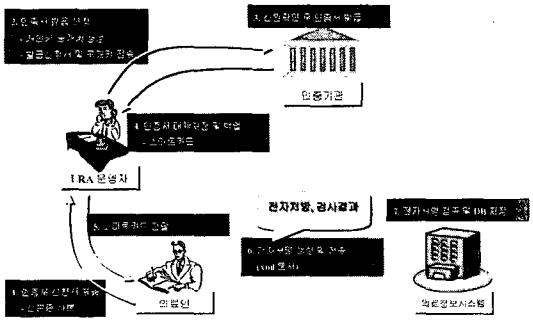
제안하는 의료정보시스템의 구성요소는 PKI 기반의 표준을 수용하고 있으며 의료인은 의료정보시스템에 인증서기반의 인증을 거친 이후 전자처방과 검사결과 정보에 대하여 전자서명을 수행한다[10].

- 인증기관 (CA : Certificate Authority)
  의료인에게 인증서의 발급과 분배를 담당한다. 또한 인증서와 관련된 정보를 공개하는 것도 주요한 업무이다. 인증서의 상태가 유효한지 폐지와 정지를 통해 무효 처리된 인증서인지에 대한 상태정보를 제공한다.

- LRA운영자 (LRA : Local Registration Authority)
  LRA운영자는 의료인의 인증서 정보를 등록하고 발급 신청을 대행을 담당한다.

● 의료인
실질적으로 인증서를 신청하고 발급 받아 인증서를 이용해 전자서명을 수행하여 인증서 기반의 의료정보를 생성하는 의료인을 말한다.

● 의료정보시스템
의료정보서비스 제공자로써 의료인의 전자서명에 대하여 검증을 수행한다. 의료정보시스템은 인증서의 유효성, 인증서 상태, 전자서명 데이터 검증을 수행한다.



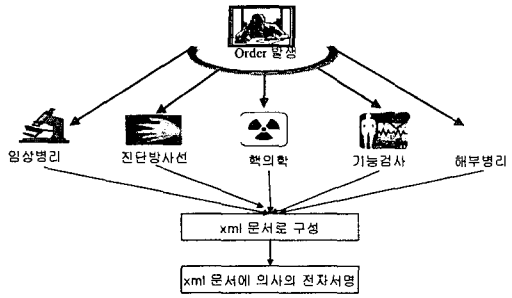
[그림 2] 제안하는 의료정보시스템의 구성요소

[그림 2]는 제안하는 의료정보시스템의 전자서명 과정을 나타낸다. 의료인은 LRA운영자에게 신원확인정보를 제공하면 LRA운영자는 인증기관에 인증서 등록을 처리한다. 발급받은 개인키와 인증서는 스마트카드의 저장매체를 통해 의료인에게 전달한다. 의료인은 전달받은 개인키를 이용하여 의료정보에 대하여 XML문서에 전자서명한다.

3.2 전자서명의 범위

[그림 3]에서 기술한 것처럼, 제안하는 의료정보시스템의 전자서명의 범위는 의사의 처방과 검사결과이며, 전산화된 각 데이터는 서버의 데이터베이스에 저장되어 있다. 의사는 최종의 전자서명이전에 의료정보시스템은 각 의료데이터를 종이 처방의 형태인 XML문서로 구성한다. XML문서로 구성된 전자처방에 대하여 의사는 자신의 개인키로 전자서명을 한다.

전자서명의 의사 처방전을 전자문서 형태로 병원의 해당부서로 전달하거나 진료기록의 경우 내용이 임의로 수정되거나 변조되는 것을 방지하고 전자서명을 이용해 내용을 증명하고 처방전을 기록한 의사의 신원을 확인한다.



[그림 3] 전자서명의 범위

4. 기대효과

본 논문에서는 신뢰할 수 있는 의료정보 시스템을 보장하기 위하여 의료정보 시스템에 전자서명 적용 모델을 제안하고자 한다. 제안하는 모델은 의사의 처방전과 진료기록에 대하여 XML문서형태에 전자서명을 관리하여 판독성과 무결성을 보장한다. 따라서 단지 의료데이터만을 저장하는 기존의 OCS, EMR, PACS 시스템에 전자서명을 적용함으로써 의료분쟁시 의사의 처방에 대하여 히스토리를 관리함으로써 무결성 및 신뢰할 수 있는 의료정보시스템을 제공한다. 이와 함께 전자서명의 데이터 형태를 XML로 구성함으로써 문서양식을 제공한다. 이러한 문서양식에 대한 전자서명은 의료기관간이나 약국의 처방전으로 확대가 가능하고 판독성이 우수하기 때문에 향상된 확장성을 제공한다.

5. 결론

인증서기반의 전자서명은 의사의 처방전을 전자문서 형태로 병원의 해당부서로 전달하거나 진료기록의 경우 내용이 임의로 수정되거나 변조되는 것을 방지하고 전자서명을 이용해 내용을 증명하고 처방전을 기록한 의사의 신원을 확인한다. 아직 병원에서 약국까지의 처방전 이용에 전자서명을 이용하고 있는 경우는 없고 병원 자체적인 문서전달 수단으로 전자서명을 활용하는 데 그치고 있다. 그러나 머지않아 의료 전분야에 걸쳐 전자서명이 활성화될 것으로 전망하고 있다. 본 논문에서는 신뢰할 수 있는 의료정보 시스템을 보장하기 위하여 의료정보 시스템에 전자서명 적용 모델을 제안하고자 한다. 제안하는 모델은 의사의 처방전과 진료기록에 대하여 문서형태에 전자서명을 관리하여 판독성과 무결성을

보장한다. 따라서 단지 의료데이터만을 저장하는 기존의 OCS, EMR, PACS 시스템에 전자서명을 적용함으로써 의료분쟁시 의사의 처방에 대하여 히스토리를 관리함으로써 무결성 및 신뢰할 수 있는 의료정보시스템을 제공한다. 이와 함께 전자서명의 데이터 형태를 xml로 구성함으로써 문서양식을 제공한다.

참 고 문 헌

[1] David A. Cooper "A More Efficient Use of Delta-CRLs" IEEE Symposium on Security and Privacy, 2000.

[2] ANDRE ARNES. "Public Key Certificate Revocation Schemes" Kingston, Ontario, Canada, February 2000.

[3] Eugenio Faldella & Marco Prandini "A Novel Approach to On-Line Status Authentication of Public-Key Certificates", IEEE, 2000.

[4] Ray Hunt. "PKI and Digital Certification Infrastructure", IEEE, 2001.

[5] Andre Arnes, Svein J. Knapskog. "Selecting Revocation Solutions for PKI", NORSEC 2000, Sep 25.

[6] Irene Gassko, Peter S.Gemmell, and Philip Mackenzie "Efficient and Fresh Certification" PKC 2000.

[7] Barbara Fox & Brian LaMacchia. "Online Certificate Status Checking in Financial Transaction : The Case for Re-issuance" financial Cryptography, 1999.

[8] Radia Perlman. "An Overviews of PKI Trust Model", IEEE, 1999.

[9] Albert Levi & M. Ufuk Caglayan. "An Efficient, Dynamic and Trust Preserving Public Key Infrastructure", IEEE, 2000.

[10] Patrick McDaniel & Sugih Jamin. "Windowed Certificate Revocation", IEEE Infocom, 2000.

[11] Hanane EI Bakkali & Bahia Idrissi Kaitouni. "A Logic-based Reasoning About PKI Trust Model", IEEE, 2001.

[12] Vishwa Prasad & Sreenivasa Potakamuri & Michael Ahern. "Scalable Policy Driven and General Purpose Public Key Infrastructure(PKI)", IEEE, 2000.