e-Healthcare 시스템을 위한 역할기반 사용자 접근제어

민경현, 조현숙, 이봉환
대전대학교 정보통신공학과
e-mail : mkhmungmung@nate.com, chojo@dju.ac.kr, and
blee@dju.ac.kr

A Role-based User Access Control for e-Healthcare System

Kyung-Hyun Min, Hyun-Suk Cho, and Bong-Hwan Lee
Dept. of Information and Communications Engineering , Daejeon University

요 약

본 논문에서는 제 3 자들 간에 디지털 인증서를 교환하여 신뢰를 구축하는 방법인 신뢰관리 시스템을 확장하여 역할에 대한 정책을 정의하고 정의된 역할을 인증서에 입력하여 접근을 제어하는 RBAC 방식을 제안하여 이를 e-Healthcare 시스템에 적용하였다. 정책 문서는 XML 로 정의하고 인증서버를 모듈화하여 e-Healthcare 시스템과의 연동 및 웹에서 사용 가능하도록 확장하였고 다양한 접근 권한이 가능한 PACS 테스트베드를 구현하여 성능을 분석하였다.

1. 서론

개방된 환경에서 인터넷 사용자가 급증함에 따라 컴퓨터 보안은 중요한 문제로 대두되고 있다. 기존에 사용되는 사용자 접근 제어는 사용자의 신원을 기반으로 한 ID/Password 방식이다. 아주 많은 사용자를 수용하는 시스템에서는 모든 사용자의 신원을 가지고 접근을 제어하는 이러한 방법은 관리의 어려움과 개인 프라이버시의 침해를 가져올 수 있다. 이러한 문제점을 해결하기 위하여 사용자의 역할을 기반으로 접근을 제어하는 RBAC(Role-Based Access Control)에 관한 연구가 활발히 진행되고 있다[1-3].

또한, 최근 인터넷과 정보처리 기술의 발전으로 IT 기술을 활용한 의료서비스에 대한 연구도 활발히 진행되고 있다. e-Healthcare 는 건강정보를 제공하고 온라인상에서 환자를 진료하며, 건강위험의 측정, 만성질환의 관리를 위해 인터넷과 같은 정보통신기술을 이용하는 것을 말한다[4]. e-Healthcare 기술의 발달로 환자의 데이터 관리와 진료의 효율을 높일 수 있었지만 사용자가 급증하고 의료 데이터에 대한 접근이 담당 의사만 가능하던 의료법이 환자나 다른 의사가 활용할 수 있도록 바뀌면서 의료 정보의 접근 제어 문제가 대두되었다[5].

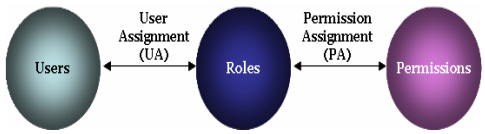
본 논문에서는 역할 간 위임을 통해 좀 더 유연한 접근제어가 가능하도록 인증서를 사용한 RBAC 을 확장한 신뢰협상 모듈을 개발하여 e-Healthcare 시스템의 접근 제어 문제를 해결하고 이를 PACS(Picture Archiving and Communication System)에 적용하여 그 성능을 분석하였다.

2. 역할 기반의 신뢰 관리

2.1 RBAC

RBAC 은 '사용자', '허가' 그리고 '역할'이라는 세 개의 기본 컴포넌트를 가진다. '사용자'는 사람일 수도 있으며, 기계나 컴퓨터 프로세스 또는 자율적인 에이전트로의 확장이 가능하다. '허가'는 하나 또는 그 이상의 보호된 객체 상에 동작을 실행시킬 수 있는 승인을 말한다. '역할'은 허가를 위해 모은 이름으로 간주되기도 하고, 조직 내의 작업 기능으로 간주되기도 한다[6]. RBAC 을 통해 사용자의 신원이 시스템 관리자에게 공개되지 않고도 접근을 제어할 수 있으며, 방대한 사용자 정보를 관리하는데 드는 어려움도 해결할 수 있다.

기본적인 RBAC 모델은 그림 1 과 같다.



(그림 1) 기본적인 RBAC 모델

RBAC 모델은 여러 가지 분야로의 활용방안에 대

해 연구되었는데 본 논문에서는 이 가운데 e-Health care 시스템에 적용한다[7].

2.2 PACS

e-Healthcare 는 정보 통신기술을 활용하여 최대한의 의학지식과 환자정보를 제공함으로써 환자진료 및 개인건강 관리 효율적이고 합리적인 의사결정을 지원할 수 있는 정보체계를 지원한다.

e-Healthcare 를 지원하는 시스템 중 PACS 는 의료영상 저장 및 전송시스템으로 의료 영상을 디지털 데이터로 획득하고 컴퓨터 저장장치에 저장하며, 고속의 통신망을 통하여 의료 영상 데이터를 전송하여 환자의 의료 영상 데이터를 관리하고 환자를 진료하는 포괄적인 시스템을 말한다. PACS 는 90 년대 초반에 실용화 되었으며, 본격적으로 도입되기 시작한 1999 년 이후 대형 병원을 중심으로 도입이 꾸준히 증가하기 시작하였다.

하지만 대형 병원에서 널리 사용되기 시작한 PACS 는 환자들의 수와 사용자가 증가함에 따라 데이터 전송, 스토리지, 데이터 백업 등의 전산 자원적인 문제와 함께 사용자 관리 및 의료 데이터로의 접근제어와 같은 보안 문제를 가지게 되었다. 이와 같은 보안 문제들 때문에 대부분의 PACS 는 병원 내 사설망으로 구축되며, 방화벽과 같은 다양한 안전장치로 외부와 단절되어 있다.

2.3 PACS 에서의 역할 기반 신뢰 관리 모델

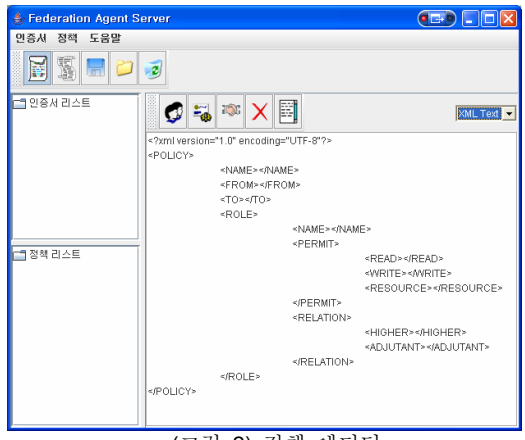
속성에 기반하여 신뢰 문제를 해결하기 위한 시스템을 신뢰 관리 시스템(Trust Management System)이라 한다[8]. 여기서 '신뢰관리'는 사전에 서로 알지 못하는 제 3 자들간에 인증서를 요청하고 인증서를 교환하는 일을 반복하여 신뢰를 협상하고 최종적으로 신뢰를 구축하는 과정을 말한다.

본 논문의 주안점은 환자의 데이터에 접근하는 권한을 제어하는 것이다. 역할 기반의 접근 제어를 위해 X.509v3 인증서의 확장 필드에 역할을 정의하여 사용하였고 PACS 사용자는 역할이 정의된 인증서를 통해 사용자임을 인증 받고 PACS 에 저장되어 있는 의료 데이터를 요청하게 된다.

본 연구에서는 선행 연구된 FAS(Federation Agent Server)[6]의 개념적 모듈을 확장하여 기능별 모듈을 구현하고 PACS 테스트베드를 통해 성능을 입증한다. FAS 에서는 인증서를 이용하여 역할을 결정하는 RDM(Role Decision Module)과 각 자원에 대한 접근 권한을 결정하는 PCM(Permission Control Module), 그리고 인증서를 발행하는 CCM(Credential Control Module)을 각각 구현하였다.

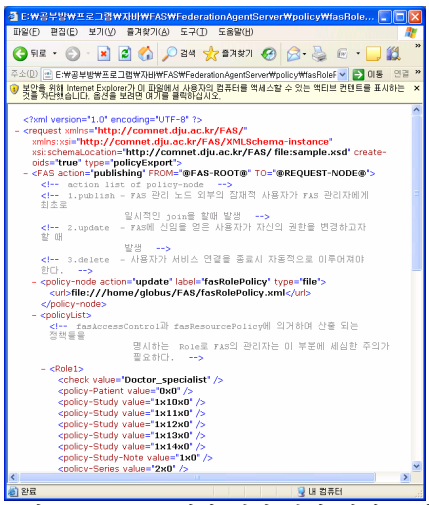
PACS 는 이러한 모듈들을 이용하여 정책과 사용자 인증서에 정의된 역할을 확인하고 사용자에게 접근 권한을 부여한다. 역할 기반 신뢰 협상 모델의 확장성을 위하여 자원에 접근하기 위해 필요한 정책을 XML 형식으로 정의하였으며, 관리자가 XML 문서에 대한 전문 지식이 없더라도 정책을 생성, 수정, 삭제할 수 있고 정책 리스트를 관리할 수 있도록 정책 에디터(Policy Editor)를 구현하였다.

구현한 정책 에디터의 UI 는 그림 2 와 같다.



(그림 2) 정책 에디터

정책들은 인증 서버에 저장되며 필요한 사용자에게 공개되고 접근 권한을 부여할 때 참고된다. 정책 문서는 확장성을 고려하여 접근 권한을 정의한 'AccessControl.XML' 문서와 접근 가능한 자원을 정의한 'ResourcePolicy.XML'문서, 그리고 역할을 정의한 'RolePolicy.XML'문서로 나누어 정의하였다. PACS 에 필요한 역할과 자원 그리고 접근 권한에 대해 분석하고 성능 검증을 위하여 그림 3 과 같이 XML 정책 문서를 정의하였다.

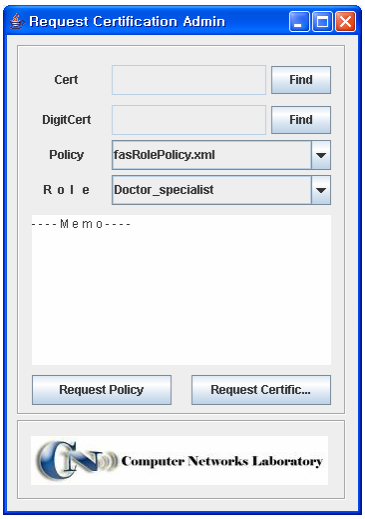


(그림 3) PACS 를 위한 신뢰 관리 정책 문서

사용자는 신뢰 협상을 통해 역할이 정의된 인증서를 발급받으며 신뢰 협상 과정은 다음과 같다.

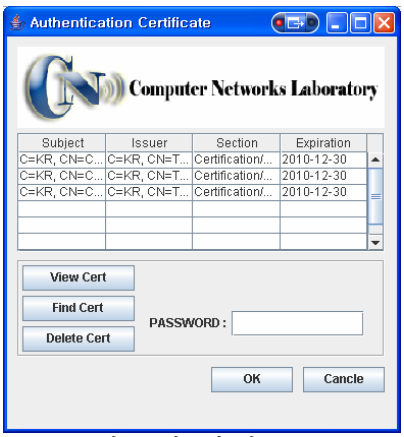
먼저 자신이 필요로 하는 자원과 역할이 정의된 정

책이 있는지 확인한다. 사용자는 이를 위해 관리자에게 정책을 요청하며, 관리자는 사용자를 확인한 후 정책을 공개 한다. 사용자는 공개된 정책에서 역할에 관한 정보를 확인하고 자신의 인증서와 자신의 역할과 관련된 인증 자료를 제출하여 자신에게 적합한 역할을 선택한다. 관리자는 사용자의 인증서와 관련 자료를 확인 후 사용자가 선택한 역할이 정의된 인증서를 발급 할 수 있다. 사용자가 인증서 요청이 편리하도록 인증서 요청 모듈을 그림 4 와 같이 구현하였다.



(그림 4) 인증서 요청 모듈

사용자는 발급받은 인증서를 자신의 컴퓨터에 저장하고 인증서 유효 기간 동안 PACS 의 자원을 요청할 수 있다. 발급받은 인증서를 이용해 PACS 에 로그인하여 자원에 접근할 수 있도록 그림 5 와 같이 인증서 인증 모듈을 구현하였다. 인증 모듈의 인증서 본인 확인과정은 한국정보보호진흥원에서 정의한 “식별번호를 이용한 본인확인 기술규격”[7]을 참조하였다.

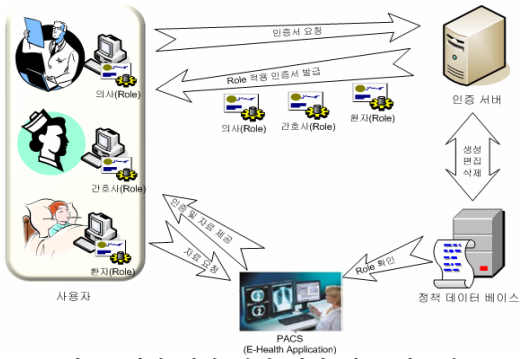


(그림 5) 인증서 인증 모듈

위의 각 모듈은 모두 독립적으로 실행되며 시스템 호환 및 확장성을 고려하여 JAVA 로 구현하였고, API 형식으로 각 모듈의 기능을 제공하여 PACS 와 연동이 편리하도록 하였다.

위에서 설명한 일련의 신뢰 협상 과정을 통해 사용자는 관리자에게 자신의 개인 정보는 공개하지 않아도 되며 자신의 역할만을 공개하여 자원으로의 접근 권한을 얻을 수 있다. 또한 사용자가 급속히 증가하더라도 관리자는 역할과 정책의 관리만 하면 되므로 사용자 관리에 필요한 과부하를 줄일 수 있다.

역할 기반 신뢰 협상을 통한 전체 인증 시스템 구조는 그림 6 과 같다.



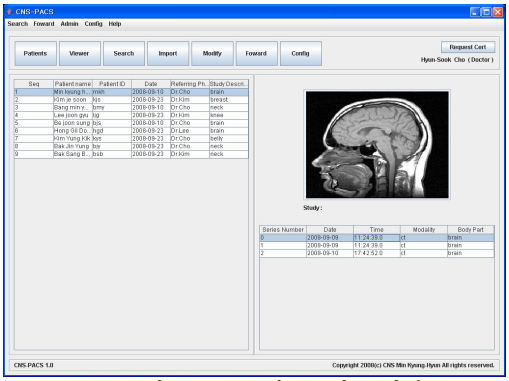
(그림 6) 역할 기반 신뢰 협상 인증 시스템 구조

2.4 PACS 테스트베드 구현 및 연동

Freeware 로 제공되고 있는 PACS 로는 K-PACS 나 PACSONE 등이 있다. 하지만 위 PACS 들은 사용자에 따른 다양한 접근 권한 기능을 가지고 있지 않고, 프로그램 소스를 공개한 것도 아니기 때문에 연동 테스트가 불가능하다.

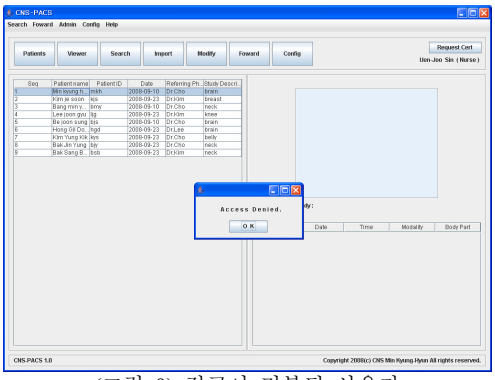
따라서 본 논문에서는 제안한 RBAC 확장 모듈의 연동 테스트 및 성능 분석을 위하여 PACS 테스트베드를 구현하였다. PACS 테스트베드는 환자의 의료 영상 데이터와 의료 정보의 입력, 수정, 삭제가 가능하며, PACS 테스트베드 간의 의료데이터 전송 기능을 제공한다. 사용자는 역할이 정의된 인증서와 인증 모듈을 통해 로그인하며 사용자의 역할에 따라 의료 데이터로의 적절한 접근 권한을 얻게 된다.

PACS 테스트베드 구성은 그림 7 과 같다. 정의한 정책을 통해 사용자의 역할을 부여하고 각 역할에 따른 적절한 의료 데이터로의 접근제어가 이루어지는지 테스트 하였다.



(그림 7) PACS 테스트베드 화면

그림 8 은 접근권한이 없는 사용자의 접근이 거부되는 것을 보여준다.



(그림 9) 접근이 거부된 사용자

시스템 성능 테스트 결과 사용자 인증과 접근 제어를 위한 각 모듈의 연동에는 문제가 없었으며, 역할에 따른 적절한 접근제어 또한 가능하였다. 접근제어를 위하여 관리자에게 사용자의 신상정보를 제공하지 않아도 됨을 확인하였고 각 역할에 따른 접근 제어를 통해 환자와 의사 등 사용자의 효율적인 접근 제어가 가능하였다.

3. 결론 및 향후 연구 내용

본 논문에서는 사용자의 역할을 인증서에 명시하는 모듈과 PACS 에 적합한 정책 파일을 정의하고, 사용자가 PACS 의 자원에 접근하고자 할 때 정책 파일과 인증서의 역할을 참고하여 사용자마다 서로 다른 접근 권한을 가지고 접근하는 모델을 제안하였다.

PACS 와의 연동과 웹으로의 확장을 고려하여 XML 문서로 정책을 정의하였고 정책을 관리할 수 있는 모듈을 개발하였다. PACS 시스템과의 직접적인 연동을 위하여 인증서 요청 모듈과 인증서 인증 모듈을 구현하였고, 각 기능을 API 형식으로 지원하도록 하였다. PACS 테스트베드에 권한별 제한적인 접근이 안전하게 지원되며, 자원으로의 접근을 위해 개인의 신상정보를 공개할 필요가 없어 개인의 프라이버시 침해 문제를 해결 할 수 있음을 입증하였다. 또한 관리자는 역할과 정책에 따른 사용자 관리만 하면 되므로 사용자 급증으로 인한 관리자의 과부하를 방지할 수 있다.

향후 연구 내용으로 보다 편한 정책 관리를 위한 그래픽 기반 인터페이스가 필요하며, 정책을 공개하고 신뢰하기 위한 정책에 대한 추가 연구가 필요하다. 또한 서로 다른 역할 간에 의료 데이터의 효율적인 활용을 위해 역할 간 위임에 대한 구체적인 정책과 기능이 필요하며, 보안 관리가 병원 환경이라는 점을 감안하여 자동으로 관리해줄 수 있는 별도의 방법이 요구된다.

Acknowledgement

본 연구는 한국산업기술재단의 지역혁신인력양성사업 및 정보통신연구진흥원의 대학 IT 연구센터 지원사업(IITA-2008-C1090-0801-0014)의 연구 결과로 수행되었음.

참고문헌

[1] D.F. Ferraiolo and D.R. Kuhn , "Role Based Access Control," In Proc. of the 15th National Computer Security Conference, Oct, 1992.

[2] R. S. Sandhu, E.J. Coyne, H.L. Feinstein, and C.E. Youman, "Role-Based Access Control Models", *IEEE Computer* 29(2): 38-47, 1996.

[3] D.F. Ferraiolo, R. Kuhn, and R. Sandhu, "RBAC Standard Rationale: comments on a Critique of the ANSI Standard on Role Based Access Control', *IEEE Security & Privacy*, vol. 5, no. 6, pp.51-53, Nov/Dec 2007.

[4] 진기남, e-Health 워크샵, 보건복지 학술대회 연제집, Vo1.2 No.1, 2005.

[5] 이유리, 박동균, “헬스케어 정보시스템에서의 동적 문맥 기반 접근제어”, 순천향산업기술연구소 논문집 제 10 권 2 호, 2004.

[6] 조현숙, “그리드 보안을 위한 웹서비스 기반의 신뢰 협상 모델”, 대전대학교 대학원 박사학위 논문, 2008.2.

[7] Lorenzo D. Martino, Qun Ni, Dan Lin, and Elisa Bertino, "Multi-domain and privacy-aware Role Based Access Control in e-Health," In Proc. of the 2nd International Conference on Pervasive Computing Technologies for Healthcare,” Tampere, Finland, Jan. 30-Feb.1, 2009.

[8] M. Blaze, J. Feigenbaum, J. Ioannidis, and A. Keromytis, "The Role of Trust Management in Distributed Systems," LNCS, Vol. 1603, pp.185-210, Springer, Berlin, 1999.

[9] 한국정보보호진흥원, 식별번호를 이용한 본인확인 기술규격 V1.11, 2002. 9.