DOI: 10.3745/KIPSTC.2010.17C.2.173

u-Healthcare 시스템을 위한 RBAC-WS

이 봉 환[†] · 조 현 숙[††]

요 약

IT 기술의 발달에 힘입어 환자들의 위치에 상관없이 편리하게 진료가 가능한 유비쿼터스 헬스케어시스템이 개발되고 있다. 그러나 사용자의 수가 급증하고 다른 병원의 의사나 연구원 또는 환자의 가족들에게 의료 정보를 공개하도록 의료법이 개정되면서 사용자 관리와 프라이버시 침해라는 문제가 발생하였다. 이러한 문제를 해결하기 위하여 본 논문에서는 역할 기반 접근제어 모델에 기반한 사용자 접근 모델은 제안한다. RBAC 모델은 효율적인 사용자 관리 및 접근 제어를 제공하지만, 악의를 가진 사용자가 권한이 있는 역할을 가지고 정보를 유출하고자 할 경우 막을 방법이 없다. 이러한 RBAC의 취약점을 보완하기 위하여 "working status" 파라미터를 역할 속성과 연동하는 RBAC-WS 모델을 제안하였다. 역할에 working 속성을 연동함으로써 허가를 받은 사용자라 하더라도 업무 외 접근을 원천적으로 봉쇄함으로서 내부자에 의한 정보유출 문제를 해결하였다. 또한 RBAC을 위한 함수를 개발하여 도메인이 서로 다른 헬스케어 시스템에서도 유용하게 사용될 수 있도록 하였으며, RBAC-WS 모델의 기능 분석을 위하여 Healthcare 시스템 중 널리 사용되는 PACS에 적용하였다.

키워드 : 접근제어, u-헬스케어, 정책, 역할기반, 신뢰관리

Role-based User Access Control with Working Status for u-Healthcare System

Bong-Hwan Lee[†] · Hyun-Sug Cho[††]

ABSTRACT

Information technology is being applied to the development of ubiquitous healthcare system, which provides both efficient patient care and convenient treatment regardless of patient's location. However, the increasing number of users and medical information give rise to the problem of user management and the infringement of privacy. In order to address this problem we propose a user access scheme based on the RBAC (Role Based Access Control) model. The preceding trust management model for Grid security, FAS(Federation Agent Server), was analyzed and extended to provide supplementary functions for role-based access control in u-Healthcare system. The RBAC model provides efficient user management and access control, but very vulnerable in case when one with valid role tries to leak confidential inner medical information. In order to resolve this problem, a RBAC-WS (Work Status with RBAC) model has been additionally developed which allows only qualified staffs to access the system while on duty. Th proposed RBAC and RBAC-WS model have been merged together and applied to the PACS (Picture Archiving and Communication System).

Keywords : Access Control, u-Healthcare, Policy, Role-Based, Trust Management

1. 서 론

허가받지 않은 사용자나 외부로부터의 정보 유출을 막기 위해 많은 접근 제어 모델이 연구되었다. 하지만 이러한 접근 제어는 권한을 가진 사용자의 정보 유출에는 매우 취약하다. 대한상공회의소에서 2006년 7월에 등록한 국내기업 400개사를 대상으로 실시한 '국내기업의 산업기밀 유출실태' 조사 결과 국내 기업의 20.5%가 '회사 기밀정보의 외부 유출로 피해를 경험한 적이 있다'고 응답했고 피해 기업의 기밀유출빈도도 평균 3.2회에 이르는 것으로 조사됐다. 또한 2007년 11월 등록된 국내 매출액 1,000 대 기업의 보안담당자를 대상으로 실시한 '국내기업의 기밀 유출 대응실태' 조사결과에서 '내부직원이 기밀유출을 시도할 경우 성공가능성'을 묻는 질문에 '기밀 유출이 가능하다'는 응답(59.7%)이 '적발되거나 원천적으로 불가능하다'는 응답(40.3%) 보다 훨씬 높게 나왔다. 특히 중소기업이 대기업보다 10% 이상 높

※ 본 연구는 교육과학기술부/한국산업기술진흥원의 지역혁신인력양성사업 및 산학협동재단의 학술연구비 지원사업으로 수행된 연구결과임.
† 종신회원 : 대전대학교 정보통신공학과 교수
†† 정 회 원 : 대전대학교 교양교육원 전임강사(교신저자)
논문접수 : 2009년 12월 8일
수 정 일 : 1차 2010년 1월 11일
심사완료 : 2010년 1월 18일

은 것으로 나타나 보안대책 마련이 더욱 시급한 것으로 조사됐다[1].

역할 기반 접근 제어 또한 사용자의 프라이버시 보호와 관리의 편의성을 제공하지만, 권한이 허가된 사용자에게 항상 접근을 허가하기 때문에 역할이 정의된 내부자가 업무 이외의 목적으로 정보를 유출하는 것에 매우 취약한 문제점이 있다. u-Healthcare에 RBAC을 접목한 연구는 위와 같은 내부자에 의한 유출에 더욱 취약하다. 다른 병원이나 웹과 같은 외부에서의 접근을 배경으로 연구되는 만큼 권한이 있는 역할을 가진 내부자에 의한 정보 유출의 가능성이 더욱 높기 때문이다.

u-Healthcare는 환자에게 건강정보를 제공하고 온라인상에서 환자를 진료하며, 건강위험의 측정, 만성 질환의 관리를 위해 인터넷과 같은 정보통신기술을 이용하는 것을 말한다. u-Healthcare 기술의 발달로 환자 의료 정보의 관리와 진료의 효율을 높일 수 있었지만 위에서 언급한 의료법이 의사만이 의료정보에 접근 가능하던 것에서 의료법이나 다른 법령에 따로 규정된 경우에 한하여 특정인에게 공개하도록 바뀌었고, 사용자 또한 급속히 증가함에 따라 의료 정보의 접근 제어 문제는 더욱 중요한 연구 분야로 부각되고 있다. 이러한 접근제어 문제점들은 역할에 기반하여 접근을 제어함으로 많은 부분 해결이 가능하다. 본 연구에서는 작업기반의 접근제어 모델(RBAC-WS)을 정의하고 이를 e-healthcare 시스템 중 하나인 PACS(Picture Archiving Communication System)에 적용하고 그 성능을 비교 분석하였다.

2장에서는 사용자 접근제어의 최근 연구동향과 u-Healthcare와 PACS에 관한 관련 연구에 대해 기술한다. 3장은 RBAC과 u-healthcare 시스템 접목 시 문제점으로 나타나고 있는 내부자의 정보유출을 봉쇄하기 위한 RBAC-WS 연구 내용에 관하여 기술하고 4장은 PACS 구현 및 연동 후 접근 제어 기능 분석에 대하여 기술한다. 마지막으로 5장에서 결론과 향후 연구내용을 기술하고 끝을 맺는다.

2. 관련 연구

2.1 RBAC

Ferrailolo와 Kuhn[1]에 의해 1992년 공식화한 RBAC의 기본 개념은 조직의 역할 함수를 반영한 것이다. 역할의 개념은 정책을 모델화하기 위한 자연스러운 요소로 보안 메커니즘과 정책 사이의 다리로서 역할을 하는 것이다. 과거의 역할은 허가(permission)를 포함하는 개념으로 OS나 DBMS, 메인 프레임이나 서버와 같은 특정 하드웨어나 소프트웨어 플랫폼에 맞추어져 있다. 따라서 역할은 다양한 시스템 환경에서 확장 가능해야만 한다. 이를 해결하기 위한 방법으로 플랫폼 독립적인 역할에 대한 연구가 진행되었으며, 이를 ERBAC(Enterprise Role-Based Access Control) [3, 4]이라 부른다. ERBAC의 기본 요소는 전통적인 RBAC 모델과 같으나 NIST RBAC 표준[5]에서 언급되었던 세션을 지원하지 않는 점이 특징이다. 다른 관점에서 보면[6] ERBAC은 역할을 상속하는데 있어서의 차이점을 들 수 있다. 접근여부를 결정할 때 사용자와 역할, 사용자-역할 할당, 허가-역할 할당, 그리고 역할과 역할사이의 관계 등을 적용하는데 있어서 전통적인 RBAC이 사용했던 고정방식을 탈피해야 하는 문제가 있다. 이러한 측면에서의 엔터프라이즈 RBAC을 Rule-Based RBAC 또는 RB-RBAC[3]이라 부른다.

RBAC의 연구는 롤엔지니어링 (Role Engineering)으로 발전하였고 초기에는 탑다운(top-down) 또는 바텀업(bottom-up)이 주류였으나 그 후 탑다운 접근법을 확장한 시나리오 중심 모델[7]이 나타났다. 이는 워크 프로파일을 포함한 특정 행동에 따른 각각의 워크플로우 파일을 사용하는 것이 기본 아이디어다. 엔터프라이즈 RBAC을 위한 롤엔지니어링에서의 Role Mining Problem[8] 등은 이론적인 연구 관점에서 보면 사용자-허가 매트릭스에서 사용자-역할 그리고 역할-허가 매트릭스로 재구성하는 방법을 다루었다.

RBAC이 발전함에 따라 연구의 키워드는 유동성(Dynamic)과 작업(Task) 기반이다[9]. 워크플로우 기반의 시스템과 같이 시간적 제약을 받는 시멘틱이 필요한 도메인을 위한 접근을 다룬 TBAC(Temporal RBAC)[10]이 그 중 하나이다. TRBAC에서는 "Role triggers"라는 용어를 소개하며 역할에 대한 제한사항에 관해 언급하였다. 전통적인 RBAC의 또 다른 도전과제는 자원의 집합에 따라 변경되는 접근권한에 대한 내용이다. 도메인이 변경되어도 사용 가능한 RBAC 모델이 필요한 것이다.

2.2 u-Healthcare와 PACS

u-Healthcare는 정보 통신기술을 활용하여 최대한의 의학지식과 환자정보를 제공함으로써 환자진료 및 개인건강 관리의 효율적이고 합리적인 의사결정을 위한 정보체계를 지원하는 것을 말한다. u-Healthcare 기술은 전자 의료 기록 시스템(EMR : Electronic Medical Record), 처방정보 전달시스템(OCS : Order Communication System), 의료 영상 저장 전송시스템(PACS : Picture Archiving and Communication System) 및 원격 의료 등과 같은 의료 종합 시스템들로 발전하였다.

PACS는 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. PACS는 영상 획득 기능과 영상을 저장하는 기능, 그리고 영상을 조회할 수 있는 기능으로 구성되며, 의료 영상 데이터를 전송할 수 있는 기능도 있다. 의료 데이터는 PACS에서 데이터와 영상을 효율적으로 관리 및 교환하고 전송 가능하도록 마련한 표준안인 DICOM(Digital Image Communication in Medicine)을 사용하여 저장되고 전송된다. PACS의 도입으로 병원 내에서의 정보흐름 지연 문제를 해소하고 환자에 대한 신속한 진료가 가능해졌다. 또한 필름의 분실 및 보관에 대한 문제(보관을 위한 인력 및 장소 확보 문제)를 해소하고, 자료를

빠르게 검색할 수 있도록 해주어 업무의 효율성을 증가시켜 주었다.

PACS는 그 쓰임새에 따라 TelePACS[11]나 WebPACS [12]와 같은 여러 가지 형태로 개발되어 왔지만 환자의 의료 데이터가 허가받지 못한 사용자에 의해 노출될 수 있기 때문에 같은 도메인 안에서만 서로 통신이 가능하며 매우 폐쇄적으로 사용되었다. 의료법이 환자 및 가족 그리고 진료에 활용하고자 하는 의사에게 공개하도록 개정되면서 큰 문제로 대두되었다. 즉, 도메인이 다른 경우에도 통신 가능한 시스템이 요구된 것이다.

3. u-Healthcare 시스템을 위한 RBAC-WS

본 논문에서는 작업 상태에 따른 역할기반 접근제어 (RBAC-WS : RBAC with Working Status) 모델을 제안한다. RBAC-WS는 역할에 업무 중(working) 상태를 속성으로 작업 중인 경우에만 접근을 허가해 주는 방식이다. 접근 권한을 가진 사용자라 하더라도 워킹 상태에 따라 접근을 제어함으로써 작업과 상관없이 정보에 접근하고 정보가 유출되는 것을 방지할 수 있다.

3장에서는 RBAC-WS 모델을 정의하고 u-Healthcare의 접근제어에 적합하게 적용하는 방법을 설명한다. 각 기능을 다른 어플리케이션과 시스템 개발에 활용할 수 있도록 함수로 정의하여 RBAC-WS를 엔터프라이즈 환경에서 서로 다른 도메인에서 유동적으로 사용가능하도록 하였다.

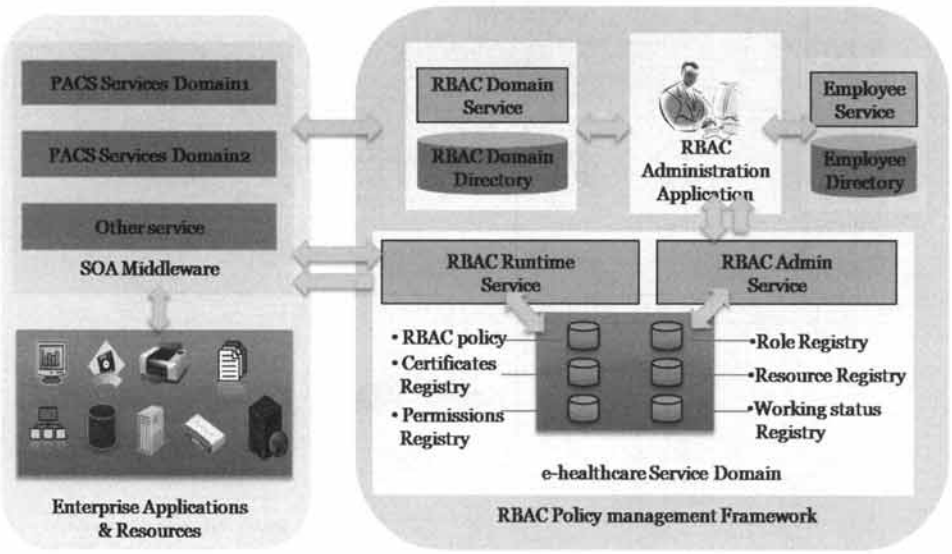
3.1 RBAC-WS의 정의

제안하는 RBAC-WS 모델은 내부 사용자에 의한 정보 유출 방지를 위한 시스템이다. FAS[13] 모델의 취약점을 보완하여 역할 속성에 "working"이라는 속성을 적용한 모델이다. FAS는 역할에 따른 접근제어 시스템으로 기존의 RBAC 시스템에 정책을 적용하여 사용자의 역할에 따라 접근제한을 동적으로 변경하는 시스템이다. RBAC-WS는 접근 권한을 가진 역할이라 하더라도 working 상태에 따라 접근 권한을 제한하는 방식이다. 이 방법으로 업무에 필요하지 않은 경우에 대한 접근을 원천적으로 봉쇄하여 내부자에 의한 정보 유출을 방지할 수 있다. RBAC-WS의 구조는 (그림 1)과 같다.

역할 기반 접근 제어가 사용자의 프라이버시 보호와 관리의 편의성을 제공하지만, 권한이 부여된 사용자에게는 항상 접근을 허용하기 때문에 내부 사용자가 업무 이외의 목적으로 정보를 유출하는 것에 매우 취약한 문제점이 있다. u-Healthcare에 RBAC을 접목한 연구는 위와 같은 내부자에 의한 유출에 더욱 취약하다. 다른 병원이나 웹과 같은 외부에서의 접근을 허용할 경우 권한이 있는 역할을 가진 내부 사용자에 의한 정보 유출의 가능성이 더욱 크기 때문이다. Working 속성은 역할과는 다르게 유동적으로 변화하기 때문에 인증서에 정의하는 것은 불가능하다. 본 논문에서는 인증서 관리 데이터베이스와 워킹 속성을 연동하여 시스템을 구현하였다. 역할을 확인할 수 있는 인증서와 역할에 따른 허가를 나타내는 인증서, 그리고 인증서와 연동하는 워킹 속성을 추가하여 u-healthcare에서 정보유출을 차단할 수 있는 시스템을 구현하였다.

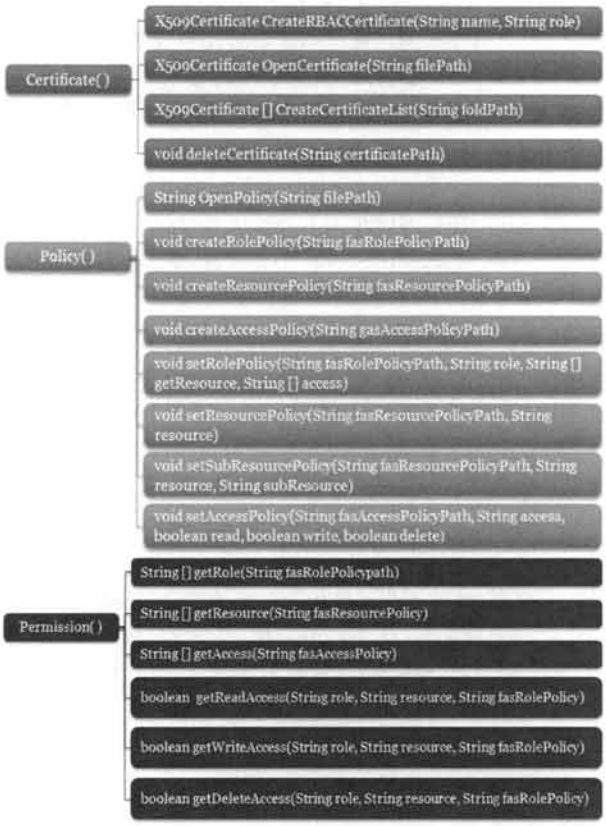
3.2 RBAC-WS의 함수 정의

함수는 각 모듈에 따라 Certificate(), Policy(), Permission()으로 구분하여 정의하여 플랫폼이 서로 다른 시스템에 구현하고 적용할 경우 효율성을 제고하였다. 본 함수를 이용함으로서 응용 도메인이 달라지거나 자원의 집합이 다른 경우에도 시스템에 적용하는 것이 가능하다. 인증 과정에 필요한 서버와 클라이언트의 통신은 소켓 통신을 사용하여 별도의 함수 정의를 하지 않았다.



(그림 1) RBAC-WS 구조도

〈표 1〉 RBAC-WS 함수 목록



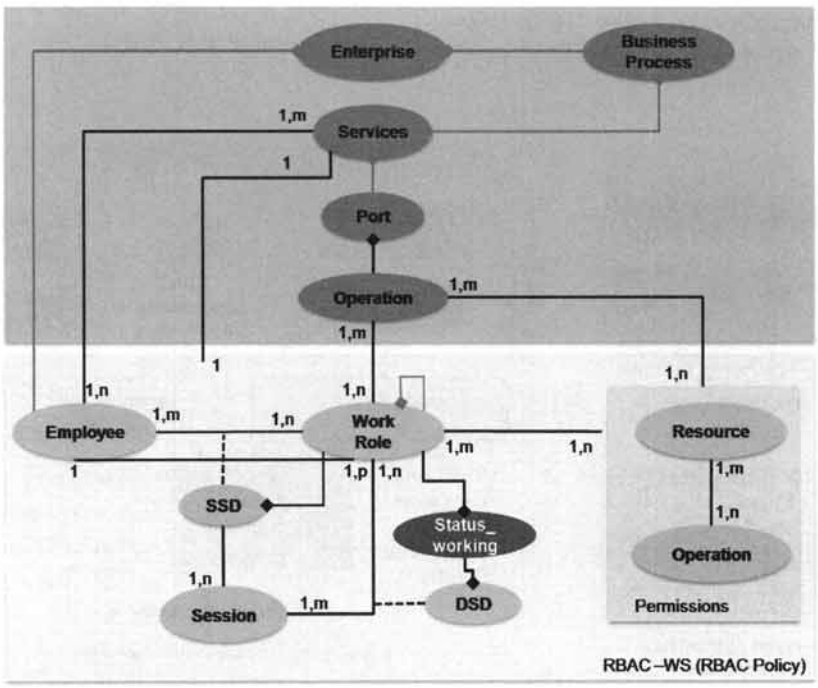
3.3 RBAC-WS의 정책

시스템에 대한 사용자의 접근 제어를 위해서는 주체와 객체의 관계를 구체적으로 정의할 수 있는 정책(policy)이 필요하다. NIST[14]에서 정의한 상업용 RBAC 모델은 사용자(employee), 역할(role)과 자원(resource), 그리고 허가(permission) 사이의 관계로 나타내었다. Basic RBAC 모델에서 사용자(employee)는 SSD(Static Separation of Duty) 역할 집합의 역할 중 하나 이상의 역할과 연결될 수 없으며, 세션(Session)은 사용자와 런타임 RBAC 시스템과의 관계를 나타내는 항목으로 DSD(Dynamic Separation of Duty) 제한 사항과 연결되는 항목이다. 역할(Work Role)은 특정 동작을 실행할 경우 허가(Permission)를 할당하는 항목이다. 상업용 RBAC을 위한 확장된 RBAC 모델을 UML로 나타내면 (그림 2)와 같다. 엔터프라이즈를 위한 확장 버전에서는 비즈니스 프로세스, 서비스, 포트, 그리고 동작(operation)이 추가된다.

RBAC 정책은 접근권한이 없는 사용자가 요청하는 자원, 서비스, 그리고 포트를 보호할 수 있도록 정의해야한다. 본 논문에서는 '접근 가능한 자원'에 관한 정책, '접근 권한 정의'에 관한 정책, 그리고 '역할에 따른 접근 권한'에 관한 정책으로 RBAC 정책을 구현하였으며, 확장성과 시스템 구현 시 연동의 유연성을 고려하여 XML 문서 형식으로 정의하였고 확장된 엔터프라이즈 RBAC 모델에 working 상태를 추가하였다.

3.4 RBAC-WS의 u-Healthcare 적용 시나리오

u-Healthcare에서 "working" 속성은 병원 직원(의사, 간호사 등)의 업무 스케줄에 따라 변경한다. 환자의 의료 정보는 진료실과 같이 지정된 곳에서 열람이 가능하며 의사의 경우 대부분 본인의 진료실을 가진다. 때문에 의사가 업무 시간 이외에 본인의 진료실에서 개인적으로 환자 정보에 접



(그림 2) RBAC-WS 정책 적용 모델

근하려 하는 경우 이것을 막을 수 없다. 또한 다른 병원이나 다른 의사의 진료실에서 환자 진료를 할 경우 환자의 의료 정보에 접근하기 위해 인증과정을 위한 별도의 절차를 밟아야 하는 문제점도 있다. RBAC-WS는 이러한 문제점을 해결하기 위하여 접근제어 정책을 다양화하였다. 의사와 간호사는 환자 의료정보를 열람 할 수 있는 곳이라면 본인의 역할에 따라 접근제어를 할 수 있다. 예를 들면, 다른 병원이나 다른 의사의 진료실에서 환자를 진료하게 될 경우 자신의 신원을 공개한 별도의 회원 가입이 필요할 것이다. 하지만 역할기반 접근제어를 사용하면 역할이 정의된 인증서만 있다면 인증을 위한 별도의 절차 없이 바로 인증이 가능하다. 또한 업무 중에만 접근을 허가하므로 의사가 업무시간 이후에 자신의 진료실에 남아 개인적으로 환자 정보에 접근하는 것을 어느 정도 해결할 수 있다.

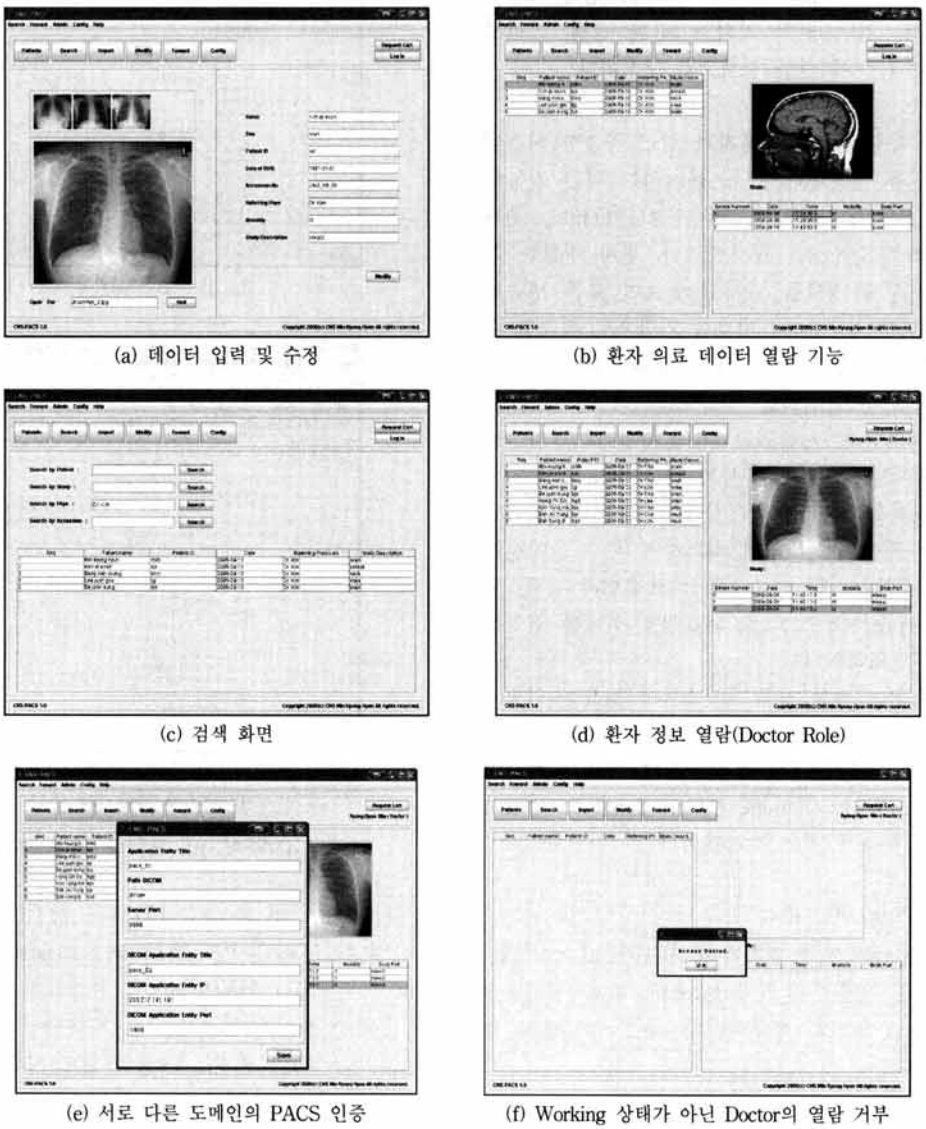
u-Healthcare에 RBAC-WS를 사용하는 경우 한 가지 문제점이 발생한다. 의료법에 의하면 가족에게 의료 기록을 공개해야 하는데 가족의 경우에는 업무 중이란 속성을 적용할 수 없기 때문이다. 때문에 u-Healthcare에 적용할 RBAC-WS에서의 역할을 환자를 포함한 환자가족과 그 이외의 사람들로 구분하여 적용하며 환자를 포함한 환자 가족은 working 속성에 업무 중을 적용한다.

4. RBAC-WS 구현

4.1 PACS 구현

본 논문에서 제안한 모델과 기능을 분석하기 위하여 헬스케어 시스템 중 널리 사용되는 PACS를 구현하였다. 본 논문에서 구현한 PACS는 크게 환자 정보, 검색, 입력, 수정, 전송 및 설정 기능을 가진다. 구현한 PACS의 주요 화면을 (그림 3)에 나타내었다.

- 환자 의료 데이터 열람 : 입력한 환자의 의료 데이터를



(a) 데이터 입력 및 수정

(b) 환자 의료 데이터 열람 기능

(c) 검색 화면

(d) 환자 정보 열람(Doctor Role)

(e) 서로 다른 도메인의 PACS 인증

(f) Working 상태가 아닌 Doctor의 열람 거부

(그림 3) RBAC-WS의 PACS에의 적용

열람하는 기능을 제공한다. 환자의 정보는 크게 'Patients' 정보와 'Study' 정보를 함께 보여주는 리스트와 Series 정보를 보여주는 리스트 그리고 'Series'에 해당하는 이미지를 보여주는 창으로 이루어져 있다.

- 환자 의료 데이터 검색 : 환자의 정보를 검색하는 기능을 한다. 검색은 Patient ID(환자ID), Study Description (분과), Attending Physician(주치의), Accession Number (진료기록 고유번호)를 기준으로 이루어지며 검색 결과를 환자의 'Patient' 정보와 'Study' 정보 리스트로 나타내었다.
- 시스템 환경 설정 : 다른 도메인에 있는 PACS와 데이터 전송을 위한 환경 설정을 한다. 기본적으로 데이터를 내보내는 PACS와 받는 PACS로 구분되며, 보내는 PACS의 타이틀, 전송 포트, 파일저장 위치와 받는 PACS의 타이틀, IP, 전송 포트를 설정한다.

4.2 RBAC-WS 모델과 PACS 연동을 위한 정책 구현

본 논문에서 구현한 정책은 모두 세 종류로 '접근 가능한 자원'에 관한 정책, '접근 권한 정의'에 관한 정책, 그리고 '역할에 따른 접근 권한'에 관한 정책으로 구성된다.

- 접근 가능한 자원 정책 : 사용자가 접근 가능한 시스템의 모든 자원을 정의한다. 본 논문에서는 접근 가능한 자원을 PACS에서 사용하는 환자정보(Patients), 분과(Study), 시리즈(Series)로 구분하였다. 환자 정보는 각 환자에 대한 상세 정보를 가지고 있으며 모든 병증과 치료 기록들로의 접근은 이 정보를 기반으로 접근할 수 있다. 시리즈는 각 환자들의 진료를 분류하는 카테고리로 하위 시리즈를 포함하는 중간계층이며 골절, 출산, 외상 등을 정의한다. 시리즈는 각 병증에 대한 산출물로 X-ray 이미지나 CT 사진 등과 같은 정보를 가진다.
- 접근 권한 정의를 위한 정책 : 사용자가 자원에 접근할 때 적용되는 권한들에 대하여 정의하며 본 논문에서는 보기, 쓰기, 삭제하기를 기준으로 의료정보의 열람, 의료정보 입력이나 처방전 작성, 의료정보 삭제를 결정하는 형식으로 정의하였다.
- 역할에 따른 접근 권한 정책 : 시스템에 필요한 역할을 정의하며 각 역할의 접근 가능한 자원과 정의된 접근 권한이 명시된다. 본 논문에서 사용자의 역할은 Doctor, Doctor_intern, Nurse, Patient, Patient_family로 정의하고 의료 정보에 대한 접근을 제어한다.

4.3 RBAC 응용 모델 비교 분석

RBAC은 응용 분야와 접근 환경에 따라 TRBAC, GRBAC, NIST RBAC 등의 형태로 발전되어왔으며, 의료 정보로의 적용을 위한 연구도 활발히 이루어졌다. 주요 모델들을 살펴보면 다음과 같다.

- PACM(Privacy Access Control Model)

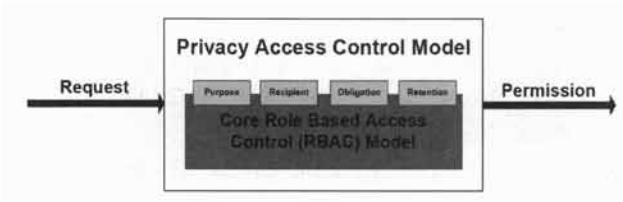
(a) 접근 가능한 자원 정책

(b) 접근 권한 정의를 위한 정책

(c) 역할에 따른 접근 권한 정책

(그림 4) RBAC-WS 모델과 PACS 연동을 위한 정책

Patrick C. K Hung은 RBAC을 확장하여 개인의 정보보호에 향상된 모델인 PACM(Privacy Access Control Model)[15]을 정의하고 e-Healthcare에 적용하는 방안을 제안하였다. 사용자는 자원에 접근을 요청하기 위해 RBAC 모델을 기반으로 '접근하는 목적', '정보를 받는 사람', '사용자의 의무', '정보의 유지' 속성에 따라 사용자의 접근을 강력하게 제한하며 구성은 (그림 5)와 같다.



(그림 5) PACM 모델

▪ MIPS

MIPS(Design and Implementation of Medical Information Protection System based on RBAC)[16]는 RBAC에 기반한 의료 정보 보호 시스템 설계 및 구현을 목적으로 연구되었으며 'User role associations, Role hierarchies', 'Conflict of interest', 'Separation of duty constraints'와 같은 사항을 만족하도록 제안하였다. 사용자 역할은 {UserID, UserName, Domain} 속성에 의해 결정되어지며 각 속성은 사용자 ID와 이름, 그리고 그룹이나 지위를 나타낸다. 각 역할은 그룹에 속하게 되며 그룹의 권한을 상속받는 개념이다. 또한 권한간 충돌과 역할간 충돌에 유연하게 대처하기 위해 역할과 권한과의 관계(Role-Permission Relationship)를 정의하였다. 위와 같은 개념을 기반으로 MIP에서는 사용자 식별 및 인증, 접근 제어 및 권한 부여, 감사, 세션관리의 서비스를 제공한다.

▪ RBAC05

RBAC05[17]는 의료정보환경에 적합하도록 제안된 모델로 사용자, 역할, 허가권한, 제약사항 등을 구체화하여 설계하고 역할을 작업과 태스크로 세분화한 후 태스크 기반의 접근제어기법을 적용하고, 시스템에 따른 모델의 적합한 환경을 구현하기 위해 역할을 계층에 따라 단계별로 세분화한 후 직급에 따라 세부적인 작업으로 분류하였다. 또한 응급상황에 대비한 긴급환경에 맞는 상황정보를 설정하여 응급상황에 대처할 수 있도록 설계하고 개인 프라이버시를 위해 절대적 허가권한을 설정하도록 하였다. RBAC05에서 의료 정보 환경을 접수부터 진료까지 고려하여 매우 세부적으로 역할과 권한을 분류하였으며, 역할의 제약조건으로 사용자, 자원, 허가권한, 장소정보, 시간, 주체가 관리하는 사용자 상황, 시스템 상황, 우선순위와 같은 세부적인 조건을 정의하였다.

지금까지의 연구들은 RBAC가 가지는 단점을 보완하고 역할 계층이나 권한 허가 또는 상황에 따른 접근제어의 효용성이 증가할 수 있음을 보여주었다. 그러나 기존의 연구는 헬스케어 등의 응용 도메인에 적용하기 위한 개념적인 시스템 모델들이 주류를 이루고 있다. 또한 역할이 정의된 사용자에겐 접근을 허가하는 기본 구조 때문에 내부 사용자에 의한 정보 유출에 매우 취약하다. 특히 어플리케이션을 통해 환자의 정보를 접근할 수 있는 시스템 환경이 요구되면서 접근 허가를 가진 내부자가 악의를 가지고 정보를 유출할 경우에 더욱 취약하다는 단점을 가진다. 의사나 간호사가 외부의 웹을 통해서, 또는 개인이 가지고 있는 어플리케이션을 통해서 악의를 가지고 정보에 접근하면 이를 막을 방법이 없기 때문이다.

본 논문에서는 시스템 개발에 RBAC 적용 시 작업의 효율을 높이기 위하여 RBAC을 적용하기 위한 기능을 함수로 정의하였다. 각 함수는 역할이 정의된 인증서와 역할기반 접근제어에 필요한 정책 관리를 도와주고 정책과 인증서를 통한 허가가 가능하도록 해준다. e-Healthcare 시스템의 환자와 가족처럼 내부자에 의한 정보 유출이 우려되지 않으며 항상 접근이 가능해야하는 역할을 위하여 사용자/가족 역할은 구분하여 정의하고 Working 속성을 항상 true로 반환하는 방법도 추가 적용하였다.

〈표 2〉 기존의 RBAC 모델과의 비교

분류	특징	장점	단점
RBAC	-사용자 역할에 따른 접근제어	-사용자 프라이버시 보호 -사용자 관리 편의	-내부자에 의한 유출 가능 -상황에 따른 변화 필요
TRBAC	-Task 기반 접근제어	-접근제어 위임의 부분 상속을 통한 신뢰성	-내부자에 의한 유출 가능 -융통성 저하
GRBAC	-제약사항 기반 접근제어	-다양한 상황에 적합하도록 변화 가능	-내부자에 의한 유출 가능 -각 상황에 따른 제약사항 분석 선행
PACM	-purpose, recipient, obligation, retention에 기반 -Core RBAC	-프라이버시 보호 강화	-내부자에 의한 유출 가능 -별도의 접근제어 응용 방안 미비
MIPS	-속성(id, name, domain)을 통해 역할을 결정하고 역할과 권한의 관계 정의	-역할을 그룹으로 묶어 비슷한 권한 간 상속 -역할 간 권한의 충돌 방지	-내부자에 의한 유출 가능 -역할을 역할로 묶는 형태 -세부적인 상속 제한 불가능
RBAC05	-테스크 기반 접근제어 확장 -응급 상황의 접근 권한우선순위 적용 제약조건에 따른 역할 제어	-돌발 상황에 따른 접근제어 -제약조건에 따른 강력한 접근제어	-내부자에 의한 유출 가능 -복잡한 구조로 인한 관리의 어려움 -명시적인 제약조건으로 인해 병원 시스템 적용의 어려움
RBAC-WS (제안모델)	-Working 속성 기반 접근제어 -RBAC 기반 신뢰 협상 -인증서/정책 관리 기능 제공	-의료 시스템 분석 -내부자에 의한 정보유출 방지 -시스템 개발 시 효율성 제공 -인증 과정의 신뢰성 -사용자 관리 효율 제공	-사용자와 관리자의 정책 이해 필요 -상황에 따른 정책 분석을 위한 선행 분석 필요 -업무 스케줄 관리 -전산시스템과 연동 필요

5. 결론 및 향후연구

본 논문에서는 RBAC-WS 모델을 정의하고 u-healthcare 도메인에 적용하는 방안을 제안하였다. 또한 용용 도메인이 다른 시스템에 적용이 용이하도록 RBAC 모델 적용에 필요한 기능을 함수로 정의하였다. RBAC은 사용자가 권한이 있는 역할을 가지고 개인적으로 정보를 유출하고자 할 경우 방지할 방법이 없다. 이러한 RBAC의 취약점을 보완하기 위하여 역할에 working 속성을 추가하여 자원에 대한 접근 허용 여부를 결정하도록 하여 내부 사용자의 악의적 접근을 원천적으로 봉쇄하였다.

RBAC 함수와 RBAC-WS 모델 적용 및 기능 분석을 위하여 Healthcare 시스템 중 널리 사용되는 PACS를 구현하였다. PACS 시스템은 입력/수정/정보열람/검색/전송/설정 기능을 포함하도록 하였으며, 구현한 PACS와 본 논문에서 정의한 함수를 이용해 역할에 따른 접근 제어와 업무 중 속성에 따른 접근제어가 가능함을 보였다. 이를 통해 사용자의 효율적인 접근 관리와 내부자에 의한 정보 유출을 막을 수 있음을 확인하였으며, 시스템에 RBAC 적용을 위해 정의한 함수의 유용성도 입증하였다.

향후 RBAC-WS의 적용을 위한 출·퇴근 전산 시스템과의 연동 테스트가 요구되며 다른 병원의 의사에게 직접 접근권한을 줄 수 있는 권한 위임 모델에 대한 연구가 필요하다. 또한, RBAC-WS 모델과 함수를 이용한 다른 분야에의 응용 연구가 필요하다.

참 고 문 헌

[1] http://www.korcham.net/EconNews/KcciReport/CRE01101L.asp

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

[3] David F. Ferraiolo, D. Richard Kuhn, and Ramaswamy Chandramouli. *Role-Based Access Control. Information Security and Privacy Series*. Artech House, 2 edition, 2007.

[4] Axel Kern and Claudia Walhorn. "Rule Support for Role-Based Access Control." In Proc. of the Tenth ACM Symposium on Access Control Models and Technologies (SACMAT '05), pp 130-138, New York, NY, USA, 2005.

[5] National Institute of Standards and Technology, http://csrc.nist.gov/groups/sns/rbac/case studies.html

[6] A. Kern. "Advanced Features for Enterprise-Wide Role-Based Access Control," In Proc. of the 18th Computer Security Applications Conference, pp.333-342, 2002.

[7] Gustaf Neumann and Mark Strembeck. "A Scenario-Driven Role Engineering Process for Functional RBAC Roles," In Proc. of the Seventh ACM Symposium on Access Control Models and Technologies (SACMAT '02), pp.33-42, New York, USA, 2002.

[8] Jaideep Vaidya, Vijayalakshmi Atluri, and Qi Guo, "The Role Mining Problem: Finding a Minimal Descriptive Set of Roles," In Proc. of the 12th ACM Symposium on Access Control Models and Technologies (SACMAT '07), pp 175-184, New York, NY, USA, 2007.

[9] Ruslan Dimov, Sean W. Smith, and Sara Sinclair, "Making RBAC Work in Dynamic, Fast-Changing Corporate Environments," Technical Report of Dartmouth College Computer Science, 2008.

[10] J.B.D. Joshi, E. Bertino, U. Latif, and A. Ghafoor, "A Generalized Temporal Role-Based Access Control Model," IEEE Transactions on Knowledge and Data Engineering, 17(1):4-23, Jan., 2005.

[11] Seoncheol Hwang et al., "Development of WWW-based TelePACS using Satellite Data Communication System," In Proc. of the 20th Annual International Conference of the IEEE, Vol.3, pp.1281-1283, Oct.29-Nov.1, 1998.

[12] WebPACS, http://www.methodist.healthsystem.org/

[13] 조현숙, 이봉환, "그리드 보안을 위한 역할기반의 신뢰 협상 모델", 한국정보처리학회논문지 제15-C권, 제6호, pp.455-468, 2008. 12.

[14] http://www.w3c.org/TR/REC-xml

[15] Patrick C. K. Hung, "Towards a Privacy Access Control Model for e-Healthcare Services," In Proc. of 3th Annual Conference on Privacy, Security and Trust, 2005. 10.

[16] Reid, J. Cheong, I. Henricksen, and M. Smith, J. "A Novel Use of RBAC to Protect Privacy in Distributed Health Care Information Systems," In Proc. of Lecture Notes in Computer Science, Vol.2727, No.1, pp.403-415, 2003.

[17] 최준, 김남현, 유선국, "다중 환자 정보 저장소에 대한 웹기반 보안 접근", 대한의료정보학회지 제 10권 3호, 2004. 9.

이 봉 환

e-mail : blee@dju.kr

1985년 서강대학교 전자공학과(학사)

1987년 연세대학교 전자공학과(공학석사)

1993년 Texas A&M 대학교 전기 및 컴퓨터공학과(공학박사)

1995년~현 재 대전대학교 정보통신공학과 교수

관심분야 : 클라우드컴퓨팅, 유비쿼터스헬스케어, 네트워크보안 등

조 현 숙

e-mail : chojo@dju.kr

1996년 대전대학교 수학과(학사)

2001년 대전대학교 정보통신공학과(공학석사)

2008년 대전대학교 정보통신공학과(공학박사)

2006년~현 재 대전대학교 교양교육원 전임강사

관심분야 : 분산컴퓨팅, 네트워크보안, 헬스케어 보안 등