한국산학기술학회논문지
Vol. 10, No. 6, pp. 1256-1264, 2009

유비쿼터스 헬스케어를 위한 역할 기반 접근제어 모델의 구현

이유리[1], 박동규[2*]
[1]한국전자통신연구원 보안관제기술연구팀
[2]순천향대학교 정보통신공학과

Implementation of Role Based Access Control Model for U-healthcare

You-Ri Lee[1] and Dong-Gue Park[2*]
[1]Managed Security Research Team, Electronics and Telecommunications Research Institute
[2]Dept. of Information and Communication Engineering, SoonChunHyang University

요 약 유비쿼터스 환경에서의 헬스케어 서비스는 환자의 의무기록 뿐 아니라 각종 검사 자료 등 환자에 대한 대부분의 정보를 데이터화 하게 되므로 인가되지 않은 사용자가 의료 시스템에 접근하여 의료 데이터를 원래의 목적과 다른 목적으로 사용하게 된다면 환자의 생명과 관련된 중요한 정보에 큰 위협을 가져올 수 있다. 따라서 이러한 문제를 해결하기 위해서 사용자의 위치나 시간과 같은 상황정보에 따른 접근제어가 가능하고 사용자의 프라이버시 보호를 가능하게 하는 RBAC for U-healthcare 모델을 설계하고 이를 구현함으로써 유비쿼터스 환경에서의 헬스케어를 위한 접근제어 모델의 유효성을 검증한다.

Abstract When unapproved users access to healthcare system and use medical information for other malicious purposes, it could severely threaten important information related to patients' life, because in ubiquitous environment healthcare service makes patient's various examination results, medical records or most information of a patient into data.
Therefore, to solve these problems, we design RBAC(Role Based Access Control) for U-healthcare that can access control with location, time and context-awareness information like status information of user and protect patient's privacy. With implementation of the proposed model, we verify effectiveness of the access control model for healthcare in ubiquitous environment.

Key Words : Access Control, Context, Obligation, Propose, Condition

1. 서론

유비쿼터스 환경에서의 헬스케어 서비스는 모바일 의료 서비스가 진화된 형태로 공간적, 시간적 제약을 없애고 환자가 생활공간 속에서 다양한 의료 센서 및 기기를 통하여 수집된 생체 정보와 환경 정보를 기반으로 중앙의 헬스케어 시스템을 통하여 언제 어디서나 의료 피드백을 받을 수 있는 서비스를 총칭한다. 이미 국내 뿐 아니라 선진 각국들은 헬스케어 서비스 제공을 위한 보건산업 분야에 투자를 집중하고 있다. 이러한 활발한 연구와 시대적인 추세에 부응하여 유비쿼터스 환경에서의 헬스케어 서비스가 제대로 이루어지게 되면 언제 어디서라도 응급 처치를 위한 치료가 가능하게 된다[1,2].

헬스케어 서비스는 개인의 중요한 의료 정보를 다루기 때문에 개인의 사생활 정보를 보호하기 위한 프라이버시 및 접근제어와 관련된 보안 기술이 필수적이라 할 수 있

이 논문은 2008년도 정부재원(교육인적자원부 학술연구조성사업비)으로 한국학술진흥재단의 지원을 받아 연구되었음 (KRF-2008-313-20080730).
*교신저자 : 박동규(dgpark@sch.ac.kr)
접수일 09년 03월 10일 수정일 (1차 09년 05월 24일, 2차 09년 06월 01일) 게재확정일 09년 06월 17일

다. 기존 헬스케어 시스템의 사용자 인가 방식은 ID, Password 기반으로 사람의 생명을 다루는 헬스케어 시스템에는 적합하지 않다. 본 저자는 유비쿼터스 환경에서의 헬스케어 시스템의 특성을 고려한 접근제어 방식이 필요하여 이를 제안하였다[3]. 본 논문에서는 헬스케어에 적합한 역할기반 접근제어 모델을 RBAC for U-healthcare 라 하고 이를 구현함으로써 유비쿼터스 환경에서의 사용자의 위치나 시간과 같은 상황정보에 따른 접근제어가 가능하고 사용자 프라이버시 보호를 위한 모델임을 구현을 통한 시나리오를 통하여 그 유효성을 검증하고자 한다.

2. 관련 연구

2.1 기존의 접근제어 모델

접근제어는 컴퓨터내의 자원 및 통신자원, 정보자원 등에 대하여 사용, 변경, 조회 등의 작업을 할 수 있는 능력을 가능하게 하거나 제한 할 수 있는 수단으로 식별 및 인증된 사용자만이 허가된 자원에만 접근을 허용하는 기술적 방법으로 임의적 접근제어[4], 강제적 접근제어[5], 역할기반 접근제어를 중심으로 연구되어 왔다[6].

임의적 접근제어는 주체나 또는 그들이 속해 있는 그룹의 신분에 근거하여 객체에 대한 접근을 제한하는 방법으로 정보 보호 보다는 정보의 공동 활용이 더 중요시되는 환경에 적합하며 최소 권한과 의무분리와 같은 무결성 규칙과 관련된 보안 서비스의 제공이 어렵기 때문에 환자의 생명을 다루는 헬스케어 시스템에는 적합하지 않다.

강제적 접근제어는 주체들과 객체들의 보안 등급에 근거하여 주체의 객체에 대한 접근을 통제하는 방법으로 헬스케어 시스템에서 다수의 객체들에 보안 등급을 부여하는 것이 어렵기 때문에 적합하지 않다.

역할기반 접근제어는 조직에 부여된 개인의 직무나 직위에 따라 접근을 통제하는 방법으로 사용자가 다수이고 유동적으로 변화하는 헬스케어 시스템에 적합한 모델이다. 접근주체인 의사 및 환자 등과 같은 헬스케어 시스템 사용자와 접근 객체인 헬스케어 시스템 자원 사이에 역할 계층을 제공하여 사용자는 적절한 역할에 할당됨으로써 권한을 부여 받을 수 있다.

본 논문에서 제안한 유비쿼터스 환경에서의 헬스케어 시스템에서의 접근제어 모델은 유선 환경 뿐 아니라 무선 환경을 고려하여야 한다. 특히 시간과 장소의 제한을 받지 않는 서비스 제공을 위하여 GRBAC[7], xoRBAC[8], CA-RBAC[9]과 같은 상황(context) 개념의 접근제어 모델이 제시되었다.

GRBAC은 접근제어 결정에 사용자 역할, 객체 역할, 환경 역할을 사용하여 전통적인 역할기반 접근제어를 확장하여 시간에 따른 접근제어와 같은 상황 기반 접근제어를 제공한다.

xoRBAC은 역할 기반 접근제어의 제약 사항에 상황정보를 사용하는 것으로 상황 제약 사항이라 한다. 이는 상황정보 속성의 실제 값을 미리 정의된 조건과 체크하여 모든 상황 제약이 참 값을 가질 때 접근을 허용하는 방식으로 속성, 함수, 조건의 튜플을 갖는다.

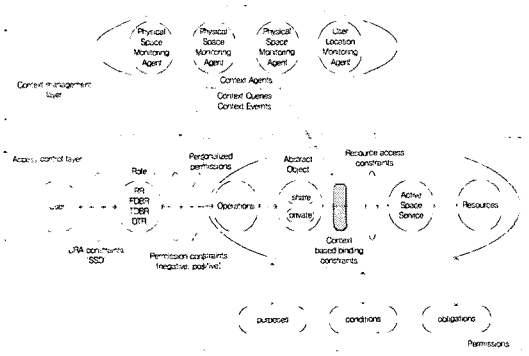
CA-RBAC은 상황관리 레이어와 접근제어 레이어로 나누어 접근제어 레이어에서 역할에 허가를 할당 할 때 상황 관리 레이어의 상황정보를 받아 들여 접근제어 하는 방식으로 본 논문의 접근제어 모델을 위해서 사용되는 기본 모델이다.

이러한 상황 기반 접근제어 모델들은 무선 환경의 특성을 고려하고 있지만 의료 서비스 제공을 위해서 중요한 프라이버시 보호와 같은 다른 의료 환경적 요소들을 고려하고 있지 못하며 또한 유동성 있는 헬스케어 시스템을 위해서는 부분적인 위임이 가능해야 하는데 이를 제공하지 못한다.

따라서 역할의 위임을 고려한 모델의 적용이 필요하다. PBDM[10]은 역할을 일반적인 위임이 불가능한 역할, 고정적으로 위임 할 수 있는 역할, 임시적으로 위임 할 수 있는 역할, 그리고 위임 역할로 네 가지로 나누어 부분적인 위임을 함으로써 헬스케어 시스템에서 세밀한 접근제어가 가능하다. 그러나 이 모델도 무선 환경을 고려하고 있지 않으며 사용자 프라이버시와 관련하여 사용자의 의료 정보를 특정 역할들이나 사용자에게 사용하지 못하도록 하는 부정적 허가[11]를 고려하고 있지 못하다. 또한 헬스케어 시스템에서 가장 중요하게 고려되어야 할 프라이버시 보호를 위한 P-RBAC[12,13]과 같은 보안 요구사항들이 불충분하다.

2.2 유비쿼터스 환경의 헬스케어 서비스에 적합한 RBAC for U-healthcare 모델

그림 1은 RBAC for U-healthcare 모델을 보여준다. 본 모델은 유비쿼터스 환경에서의 헬스케어 시스템에 적합한 역할기반 접근제어 모델을 보여준다. 모델은 크게 상황 관리 레이어(context management layer)와 접근제어 레이어(access control layer)로 나뉜다.



[그림 1] RBAC for U-healthcare 모델

(1) 상황 관리 레이어

상황관리 레이어에서 상황 모델은 상황 정보들을 센서에 의해 데이터 수집을 위하여 설계하는 것으로 상황기반의 상세한 표현한 어플리케이션에 의해서 정의된다. 또한 이의 신뢰도는 요구사항들을 상황기반으로 적절하게 모델화하는가에 따른다. 이런 상황 모델은 센싱 기술의 가능성에 의존적으로 모델화 된다. 예를 들어 간호사의 위치는 병실에 따라서 모델화 될 수도 있고 센싱 기술에 따라서 병실안의 특별한 환자의 근접성을 기반으로 하여 모델화 될 수도 있다. 따라서 센싱 기술은 이러한 위치에 대한 유효한 영역을 결정한다.

상황 관리 레이어에서는 환경의 여러 종류의 다양한 컨디션을 센서를 통하여 끊임없는 실시간 데이터 수집을 요구하기 위하여 상황 에이전트를 하나 이상 만들어 실행 시킨다. 이 상황 에이전트들이 수집하는 데이터는 어플리케이션에서 요구되어지는 상황 정보를 포함함으로 상황 에이전트들의 데이터의 신뢰성을 위해서 인증과정은 반드시 필요하다. 또한 접근제어 레이어의 역할과 객체 사이의 데이터 교환을 위한 인터페이스를 제공하여야 한다.

(2) 접근제어 레이어

본 모델이 다른 접근제어 모델과 다른 주요한 구분은 이 접근제어 레이어에 있다. 사용자의 집합체(USER)는 헬스케어 시스템에서 다른 자원들 사이의 접근할 때 필요한 사용자의 집합이다. 역할의 집합체(ROLE)은 헬스케어 시스템에서의 역할의 구성원에게 부여된 책임과 권한과 관련되어 연관된 의미를 가진 헬스케어 시스템 내의 직무 기능이나 직무 명칭을 말한다. 허가의 집합체(PERMISSION)는 헬스케어 시스템 내에서 하나 이상의 객체로의 접근을 승인하는 것이다. 허가에서의 객체는 헬스케어 컴퓨터 시스템 내의 자원뿐만 아니라 데이터로의 표현되는 자원들도 포함된다. 역할 기반 접근제어의 기본적인 개념은 사용자가 역할에 할당되고, 역할에 허가가 할당되며 사용자는 역할의 멤버가 됨으로써 허가를 얻는다. 즉, 다른 역할 멤버들에 의해서 실행되는 하나의 허가의 실행의 결과는 항상 같게 된다.

그러나 그림 1에서 보여지는 바와 같이 접근제어 레이어는 기존의 역할 기반 접근제어 모델과는 다르게 정의된다.

첫째, 허가는 각 역할의 멤버들을 위해 개인화된다. 하나의 역할은 개인적인 역할 멤버들의 상황 정보와 목적, 의무사항, 조건들을 기반으로 하는 다른 객체의 오퍼레이션에 의해서 실행된다.

둘째, 역할은 의료 상황에 따라서 역할 위임 시 동적이고 부분적인 위임을 위하여 하나의 역할을 4개의 부역할로 나누어진다.

셋째, 허가-역할 할당시 긍정적인 허가와 부정적인 허가를 제약 조건으로 주어 환자가 공개하길 원치 않는 정보에 대한 접근은 부인되어야 한다.

넷째, 상황 관리 레이어에 의존적으로 상황 이벤트 발생 시 상황 정보를 객체 및 역할의 조건으로 지정된다.

본 논문에서 제안하는 모델은 개인적인 허가를 지원한다. 위 그림 1에서 보여지는 바와 같이 목적에 의하여 서비스와 자원으로 구분된다. 서비스는 수많은 자원들에 대한 특별한 타입의 하나로 관리되어진다. 상황 조건을 기반으로 하여 자원들의 한 부분을 한 역할 멤버들의 접근을 제어 할 필요가 있다. 예를 들어 환자 정보 시스템에서 데이터베이스 서비스는 상황 조건이 무엇인지 접근하고자하는 사람이 누구인지에 따라서 데이터베이스 테이블들에 대한 접근을 제안할 수 있다. 그 하나의 데이터베이스에는 의사 기록, 수행된 테스트, 마지막 체크한 시간, 환자의 병실 등과 같은 환자의 정보들이 저장되어있다. 따라서 의사 데이터와 같은 한 개의 자원과 의사기록, 수행된 테스트, 마지막 체크 시간, 환자의 병실들의 자원이 함께 묶여있는 서비스들은 서로 구분되어야 한다.

위에서 언급한 자원과 서비스들은 자원 접근 제약을 가지게 되면 상황기반 바인딩 제약 조건들을 상황 관리 레이어에 의해 제공 받음으로써 추상객체가 된다. 예를 들어 자원 접근 제약이 '환자의 병실에 최근 방문한 간호사만이 환자에 레코드에 접근이 가능하다'라고 하면 상황 정보를 제공 받아서 환자의 병실에 최근 방문한 기록이 있는 간호사의 환자에 레코드가 추상 객체가 될 수 있다.

이러한 추상 객체는 공유(shared) 객체와 개인적인(private) 객체로 구분되어지며 공유 객체는 모든 역할에 모든 멤버들에 공통적인 반면에 개인적인 객체는 한 역

할에 특정하고 다른 멤버들과는 구분되어서 관리되어진다. 각 추상 객체들은 오퍼레이션들에 할당되며, 조건들과 의무들과 같은 프라이버시 보호를 위한 요소들을 추가하여 개인화된 허가들이 제공된다. 이 허가들은 긍정적인 허가, 부정적인 허가와 같은 허가-역할 할당 제약조건을 고려하여 역할들에게 할당되게 된다. 이렇게 할당된 역할들은 의무 분리와 같은 사용자 역할 할당 제약 조건들을 고려하여 사용자에게 할당된다.

제안된 모델에서 기본적인 역할 허가 할당은 역할에 긍정적인 허가가 할당되면 사용자는 역할의 멤버가 됨으로써 허가를 얻지만 역할에 부정적인 허가가 할당되면 사용자는 역할에 멤버가 될 수가 없다. 즉 허가는 긍정적인 허가(PP : Positive Permission)와 부정적인 허가(NP : Negative Permission)로 이루어져 있다. 부정적인 허가는 접근을 부여하는 것보다 부인하는 개념으로 헬스케어 시스템에서 환자는 자신의 차트를 보지 않기를 원할 수 있다. 예를 들어 Bob은 내과의사인 Alice의 환자로, 이때 이 내과에 있는 모든 간호사들은 환자의 진단 정보를 볼 수 있는 권한을 가지고 있다고 가정하자. 그러나 Bob은 암에 걸렸고 이 사실을 가족인 누구에게도 아직은 알리지 않고 싶어 하는데, Bob의 가족 중 한명이 이 내과의 간호사라면 Bob은 이 간호사에게 자신의 진단 정보에 대해서 부정적인 허가를 부여함으로써 자신의 프라이버시를 침해 받지 않을 수 있다. 이렇듯 헬스케어 시스템에서 환자의 프라이버시를 지켜주기 위해서 부정적인 허가는 필수적인 요소라 할 수 있다.

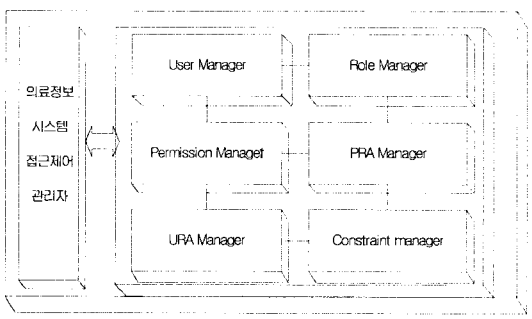
역할 계층은 긍정적인 허가를 부여 받은 역할과 부정적인 허가를 부여 받은 역할로 이루어져 있다. 따라서 역할 상속시에 충돌이 발생 할 수 있으며 이 때 역할 기반 접근제어의 최소 권한의 원칙에 의해서 헬스케어 시스템에서는 긍정적인 허가보다는 부정적인 허가를 우선으로 상속 받는다. 또한 자식 노드를 확인한 결과 마지막 까지 상속 받을 수 있는 허가가 없다면 마찬가지 이유로 접근을 부인한다.

역할 계층은 상속 뿐 아니라 위임도 이루어진다. 위임은 전체적인 위임과 부분적인 위임이 있으며 좀 더 유동성 있는 헬스케어 서비스를 위해서 부분적인 위임이 가능해야 한다. 따라서 본 모델에서는 위임을 위한 역할을 일반적인 역할(RR : Regular Roles), 고정적으로 위임할 수 있는 역할(FDBR : Fixed Delegatable Roles), 임시적으로 위임 할 수 있는 역할(TDBR : Temporal Delegatable Roles) 그리고 위임 역할(DTR : Delegation Role) 네 가지로 분류 할 수 있고 이렇게 분류함으로써 부분적인 위임이 가능하게 된다. RR은 위임 할 수 없는 역할이며 FDBR과 TDBR은 위임할 수 있는 역할들이며 DTR은 위임 역할로 사용자가 아닌 역할에다가 위임을 해주는 것이다. 따라서 이를 통해서 역할 대 역할 위임이 이루어진다. 환자는 좀 더 유동적으로 자신을 돌봐 주기 위해서 환자가 가지고 있는 권한을 위임한다. 그러나 다른 한편으로 그의 프라이버시를 보호하기 위하여 그의 건강 데이터의 제어 권을 잃지 않기를 원한다. 이 문제는 권한의 충돌을 가져온다. 예를 들어서 의사들은 환자의 건강 데이터에 대하여 읽기 권한을 가지고 있다. 그러나 환자 Alice는 그녀의 건강 정보와 관련된 모든 정보를 그녀의 직계 가족에게는 공개하지 않기를 원할 수 있다. 의사 Bob은 그녀의 직계 가족인 경우 Bob은 두 가지 권한을 부여 받고 권한 충돌이 일어나게 된다. 즉 긍정적인 허가와 부정적인 허가의 충돌이 발생할 수 있다. 이와 같은 문제는 헬스케어 시스템의 특징상 응급 상황을 위하여 정보를 공개 할 것인지 사용자의 프라이버시를 고려할 것인지의 권한 정책을 수립함으로써 해결 할 수 있다.

3. RBAC for U-healthcare 모델 구현

유비쿼터스 환경에서의 헬스케어 서비스를 위한 시스템에서 사용자 권한에 맞는 안전한 서비스를 제공하기 위하여 헬스케어 서비스를 위한 접근제어 모델의 프로토타입을 구현하였다. 구현 환경은 Windows XP, 사용자 시뮬레이션 및 사용자 GUI를 위해 Visual Basic.net을 사용하였고 MySQL Server 6.0을 이용하여 데이터베이스를 구축하였다.

유비쿼터스 환경에서의 헬스케어 서비스를 위한 접근제어 모델의 관리를 위한 다음 그림 2와 같이 User, Role, Permission, URA, PRA, Constraint 모듈로 구성된 관리자 모듈을 갖는다.

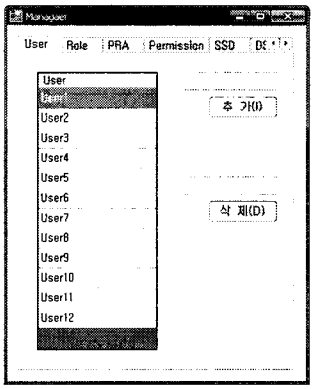


[그림 2] RBAC for U-healthcare 모델 관리자 모듈 구성도

관리자 모듈은 다음과 같이 동작한다. User manager에

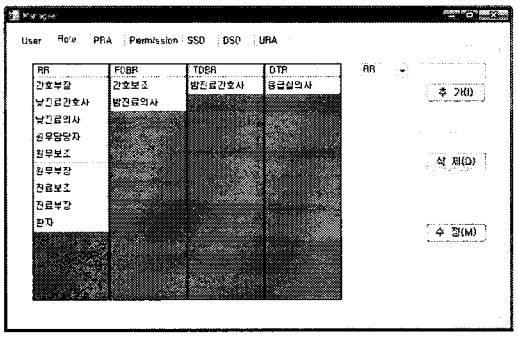
서 사용자에 대한 관리를 하며 Role manager에서 사용자의 역할을 등록하고 Permission manager를 통하여 권한을 설정한다. 설정된 권한은 PRA manager를 통하여 역할에 할당되며 할당된 역할은 URA를 통하여 사용자에게 할당되게 된다. 이렇게 할당받은 역할을 통하여 사용자는 자신의 권한에 맞는 서비스를 제공 받을 수 있다.

사용자는 헬스케어 시스템을 사용하는 사용자로 다음 그림 3과 같이 추가 삭제 될 수 있다.



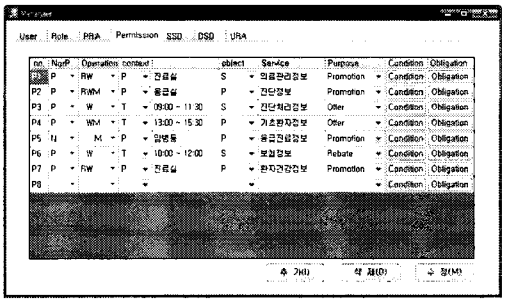
[그림 3] 사용자 관리

역할은 헬스케어 시스템에서의 역할의 구성원에게 부여된 책임, 권한과 관련되어 연관된 의미를 가지는 헬스케어 시스템 내의 직무 기능이나 직무 명칭을 말하는 것으로 제안한 모델에서는 좀 더 유동성 있는 헬스케어 서비스를 위해 부분적인 위임이 가능하다. 따라서 위임을 위해서 역할을 일반적인 역할, 고정적으로 위임할 수 있는 역할, 임시적으로 위임 할 수 있는 역할 그리고 위임 역할 네 가지로 분류 한다. 역할은 다음 그림 4와 같이 추가 삭제 될 수 있고 응급실 의사의 역할은 역할 대 역할 위임이 가능하게 된다.



[그림 4] 역할 관리

자원과 서비스들을 사용하기 위해서 허가가 필요하며 이는 상황 정보 제약 조건이 존재할 때 상황 정보 관리 레이어에 의해서 조건에 대한 검사를 통해서 추상객체가 된다. 본 논문에서 제안한 모델에서의 객체는 공유와 개인으로 나누어지며 그림 5와 같이 공유 객체는 S(share)로 설정되어 모든 역할에 모든 멤버들에 공통적인 반면에 개인적인 객체는 P(private)로 설정되어 한 역할에 특정하고 다른 멤버들과는 구분되어서 관리되어 진다. 이 객체들은 오퍼레이션에 할당됨으로 인해서 허가가 정의된다. 다음 그림 5와 같이 허가들을 관리 할 수 있다.



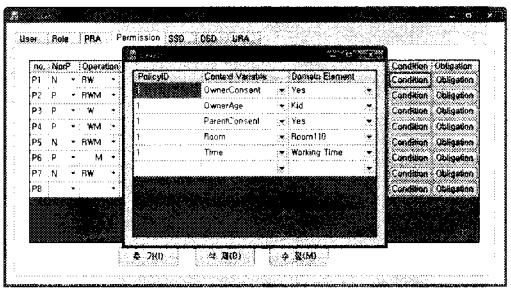
[그림 5] 허가 관리

그림 5는 허가 관리창을 보여주고 있다. no.는 허가들의 이름으로 중복 될 수 없는 Primary Key 값을 가진다. NorP는 허가의 종류에 대해서 설정하는 부분이다. 본 논문에서 제안한 접근제어 모델에서는 긍정적인 허가 뿐 아니라 사용자 프라이버시와 관련하여 부정적인 허가도 고려하고 있다. 따라서 P(Positive Permission)는 긍정적인 허가이고 N(Negative Permission)은 부정적인 허가를 의미한다. 예를 들어 P5의 경우 P5를 할당받은 역할을 가진 사용자는 암병동에서 응급진료 정보에 대한 수정할 수 없다는 것을 보여준다. 또한 본 논문에서 제안하고 있는 접근제어 모델은 서비스와 추상 객체 사이에 상황기반 바인딩 제약 조건을 두어서 상황관리 레이어에 있는 센서로부터 상황정보를 데이터를 수집하여 객체에 대한 오퍼레이션을 할당하게 된다. 그림 5에서 상황(context) 요소의 P(place)는 장소 T(time)는 시간을 의미한다. P와 T 옆의 요소는 value 값을 말하며 장소와 시간을 각 각 적어주어 상황 제약 조건을 설정할 수 있다.

허가들은 조건, 의무, 목적과 같은 프라이버시 보호를 위한 요소들을 추가하여 개인화된 허가들을 제공 할 수 있어야 한다. 따라서 그림 5와 같이 아이들의 개인 의료 데이터 정보 수집을 위해서 소유자 동의가 필요하다거나 소유자 나이에 대한 조건과 어떤 오퍼레이션이 실행되기 전에 아니면 실행 후에 일어날 의무사항 그리고 시스템

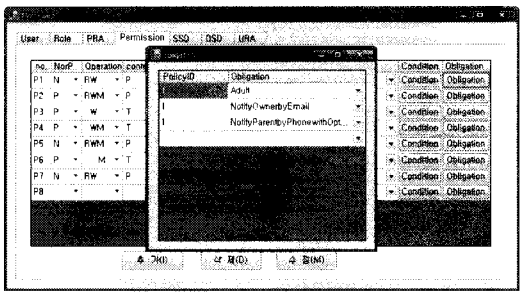
사용 목적이 고려되어야 한다. 그림 5의 purpose 항은 목적을 설정하는 부분 사용자의 승인이나 환불과 같은 목적에 대한 제약 조건이 필요할 때 설정하는 부분이다.

본 논문에서 제안한 모델에는 의료 시스템을 다루고 있기 때문에 만약 사용자가 환자이고 어린 아이라면 아이의 데이터를 사용하는데 있어서 부모의 승인이 필요할 수 있다. 이러한 제약들은 조건으로 보고 그림 5의 condition을 선택하여 그림 6과 같이 설정할 수 있다.



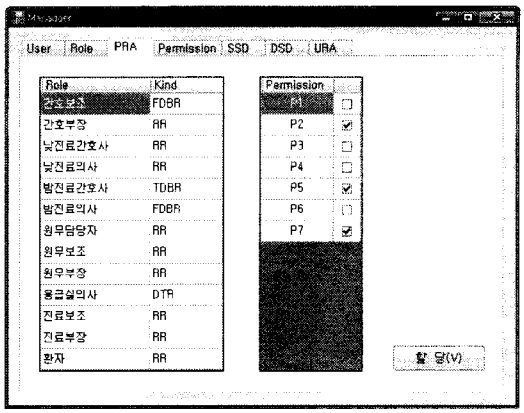
[그림 6] 조건 제약 설정

또한 의무 사항과 관련하여 환자의 상태 정보를 알기 원하는 부모에게 환자의 동의가 있었을 때 진료 후나 아니면 진료 전 환자에 상태에 대해서 알려주어야 하는 의무 사항이 있다면 그림 7과 같이 설정 가능하다.



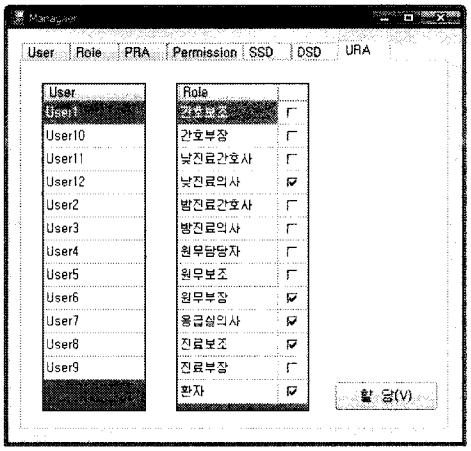
[그림 7] 의무사항 정보 설정

역할 기반 접근제어에서 허가는 역할에 할당되고 허가를 할당받은 역할은 사용자에게 할당됨으로써 사용자는 자신의 권한을 부여 받을 수 있다. 따라서 그림 5, 6, 7과 같이 허가에 대한 설정이 끝나면 설정된 허가는 사용자에게 할당되어야 한다. 허가가 역할에 할당되는 것은 허가-역할 할당이라고 한다. 이는 그림 8과 같이 볼 수 있다.



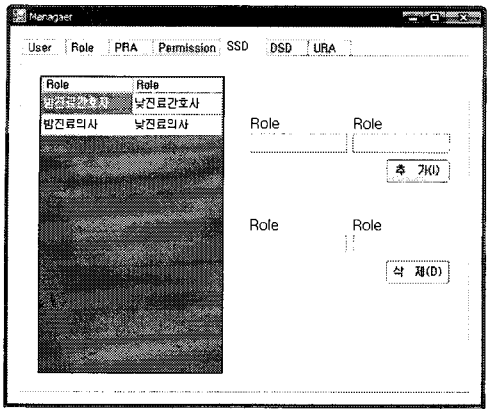
[그림 8] 허가 역할 할당

허가를 할당 받은 역할은 사용자에게 할당되어지며 이 과정은 사용자-역할 할당이라고 한다. 이것은 그림 9에서 보여 진다.



[그림 9] 사용자 역할 할당

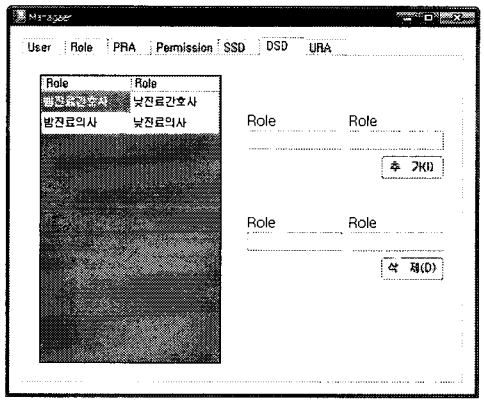
특히 사용자에게 역할을 할당 할 때는 정적의무분리와 동적 의무분리의 제약 조건에 따른다. 정적의무분리는 한 사용자에게 두 역할이 할당될 수 없으며 동적 의무분리는 한 사용자에게 두 역할이 할당되나 한 역할에 대한 세션이 이루어지고 있을 때 다른 한 역할을 사용 할 수 없는 제약 조건을 말한다. 그림 10은 정적 의무 분리를 보여준다.



[그림 10] 정적 의무 분리

정적 의무 분리의 역할로 설정된 밤 진료 간호사와 낮 진료 간호사는 한 사용자에게 할당 될 수 없다.

그림 11은 동적 의무 분리를 보여준다.



[그림 11] 동적 의무 분리

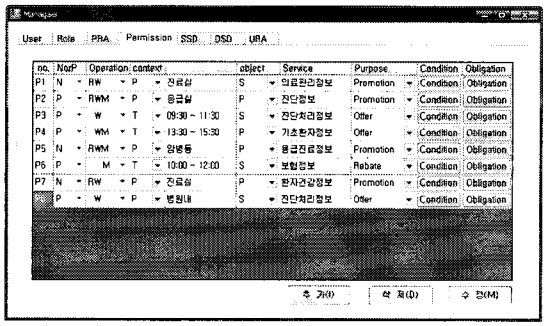
밤 진료 의사와 낮 진료 의사는 동적 의무 분리로 설정되어 있다. 즉, 밤 진료 의사와 낮 진료 의사는 한 사용자에게 역할이 할당될 수는 있으나 동시에 같은 역할로 접속하여 서비스를 이용 할 수는 없다.

4. 시나리오를 통한 접근제어 모델의 유효성 검증

본 논문에서 제안한 RBAC for U-healthcare 모델은 사용자 프라이버시 보호를 위해서 조건, 목적, 의무사항에 대한 제약 조건의 요소를 포함하고 있다. 다음 시나리오를 통하여 사용자의 조건, 목적, 의무사항이 포함된 접근제어 시스템을 시뮬레이션 하였다. 시나리오는 다음과 같다. 의사는 아이를 진단하고 진단 처리 정보의 제출을 목적으로 하는 허가를 가진다. 그 아이의 진단 정보를 처리하려고 하니 조건 제약에 의해서 부모의 승인이 있어야 하고 의무사항 제약에 있어서 진단하기 전에 전화를 하여 진단 정보에 대해 아이의 부모에게 알려야 할 의무가 있다. 또한 다른 조건으로 아이의 진단 정보를 작성하는 것은 의사 자신의 방에서 근무시간에 이루어져야 한다. 이 시나리오의 유효성 검증은 다음과 같다.

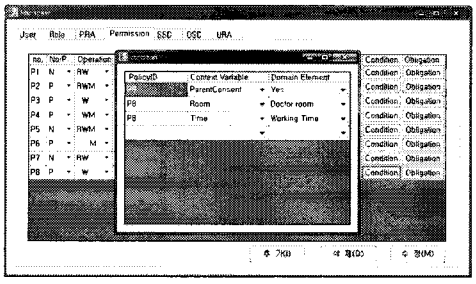
첫 번째, 의사에 대한 허가와 조건, 의무, 목적 제약 조건을 설정한다.

그림 12는 허가 할당과 목적 제약 할당을 나타내고 그림 13은 조건 제약 할당을 나타내며 그림 14는 의무 사항과 관련된 제약 조건을 할당한다.



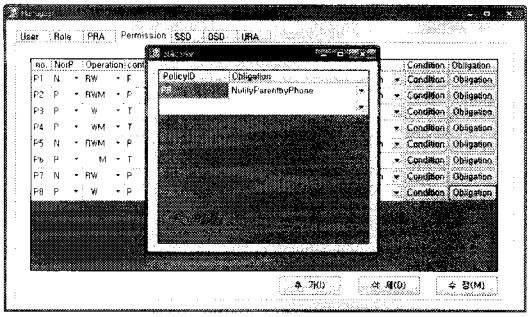
[그림 12] 허가 할당과 목적 제약 할당의 예

그림 12의 P8을 보면 의사에게 할당될 허가가 정의되고 있다. 상황정보로 P는 장소를 나타내며 value로 병원내로 할당되어 있다. 또한 목적 제약 할당과 관련하여 제출을 목적으로 하는 제약 조건이 할당됨을 볼 수 있다.



[그림 13] 조건 할당의 예

그림 13은 의사의 허가의 조건을 할당한다. 부모 승인이 있어야하며 자신의 방에서 근무시간에 허가가 가능하게 할당된다.



[그림 14] 의무 사항 할당의 예

그림 14는 허가 P8에 의무사항인 부모에게 전화를 하여 허가를 수행하기 전에 미리 알려주라는 의무사항을 할당하고 있다.

위의 시나리오를 통하여 유비쿼터스 환경에서의 헬스케어 서비스를 이용하고자 하는 사용자는 RBAC for healthcare 모델을 적용하여 위치와 시간과 같은 상황 인식이 가능하며 사용자의 프라이버시 보호가 가능하게 된다.

5. 결론

본 논문에서는 유비쿼터스 환경에서의 헬스케어 서비스에 적합한 접근제어 모델인 RBAC for U-healthcare 모델을 구현함으로써 유비쿼터스 환경에서의 상황 정보 기반의 접근제어가 가능함을 보였다. 또한 헬스케어 서비스에 필요한 프라이버시 보호를 위한 목적, 의무, 조건들을 고려함으로써 유비쿼터스 환경에서의 헬스케어 서비스를 사용하는 사용자의 프라이버시 보호가 가능함으로 보였다.

따라서 본 논문에서 구현된 시스템을 통하여 유비쿼터스 환경에서의 헬스케어 서비스 제공시 사용하는 사용자의 유동성있고 세밀한 접근제어 및 프라이버시 보호가 가능하다. 향후 RBAC for U-healthcare 모델의 관리를 위한 관리 모델이 필요할 것으로 사료된다.

참고문헌

[1] R.L.Bashshur, T.G.Reardon, and G.W.Shannon, "Telemedicine : a New Health Care Delivery System" Ann. Rev. Public Health, vol. 21, 2000, pp.613-617.

[2] R.S.H. Istepanian, E.Jovanov, and Y.T.Zhang, "Guest Editorial Introduction to the Special Section on M-Health: Beyond Seamless Mobility and Global Wireless Health-Care Connectivity" IEEE Trans. Info. Tech. Biomed., vol.8, no. 4, 2004, pp. 405-414.

[3] 이유리, 박동규, "유비쿼터스 원격 의료 시스템에서의 사용자 프라이버시를 고려한 접근제어 모델", 한국정보보호학회 동계학술대회, pp. 171~175, 2008.

[4] C.P.Pfleeger, "Security in Computing", second edition, Prentice-Hall Inte rnational Inc., 1997.

[5] E.G.Amoroso "Fundamentals of Computer Security Technology", PTR Prentice Hall , pp. 253-257, 1994.

[6] Ravi Sandhu, David Ferraiolo, and Richard Kuhn, "The NIST model for role-based access control: Towards a unified standard." In Proceedings of 5th ACM Workshop on Role-Based Access Control, pp. 47-63, July, 2000.

[7] Matthew J. Moyer, Mustaque Ahamad, "Generalized Role-based Access Control", In IEEE International Conference on Distributed Computing Systems(ICDCS2001), pp.391-398, Mesa, Arizona, USA, April, 2001.

[8] Gustaf Neumann, Mark Strembeck., "An Approach to Engineer and Enforce Context Constraints in an RBAC Environment", Symposium on Access Control Models and Technologies(SACMAT 2003), pp. 65-79, June, 2003.

[9] Devdatta Kulkarni, Anand Tripathi, "Context-aware Role Based Access Control in Pervasive Computing Systems", Proc. 13th ACM Symposium on Access Control Models and Technologies (SACMAT 2008), pp.113-122, June, 2008.

[10] Dong Gue Park, You ri Lee, "A Flexible Role Based Delegation Model Using Characteristics of Permissions", Proc. 16th International Conference, DEXA 2005, pp.310-323, August, 2005.

[11] David Ferraiolo, Ravi Sandhu, Serban Gavrila, Richard Kuhn, Ramaswamy Chandramouli, "Proposed NIST standard for role-based access control", ACM TISSEC Vol. 4, No.3, pp.224-274, August, 2001.

[12] Qun Ni, Alberti Trombetta, "Privacy-aware Role Based Access Control", Symposium on Access Control Models and Technologies(SACMAT 2007), pp. 41-50, June, 2007.

[13] Qun Ni, Elisa Bertino, Jorge Lobo, "An Obligation Model Bridging Access Control Policies and Privacy Policies", Symposium on Access Control Models and Technologies(SACMAT 2008), pp. 133-142, June, 2008.

이 유 리(You-Ri Lee) **[정회원]**

- 2002년 2월 : 순천향대학교 정보통신공학과 (공학학사)
- 2004년 2월 : 순천향대학교 정보통신공학과 (공학석사)
- 2009년 2월 : 순천향대학교 정보통신공학과 (공학박사)
- 2009년 3월 : 한국전자통신연구원 (Post-Doc)

<관심분야>
접근제어, 유비쿼터스 컴퓨팅 보안

박 동 규(Dong-Gue Park) **[정회원]**

- 1992년 2월 : 한양대학교 전자공학과 (공학박사)
- 1999년 3월 ~ 2004년 2월 : 전기전자공학부 (부교수)
- 2004년 3월 ~ 현재 : 순천향대학교 정보통신공학과 (교수)

<관심분야>
네트워크보안, 유비쿼터스 컴퓨팅 보안