상황 및 프라이버시를 고려한 역할기반 접근제어 모델

정회원 이 유 리*, 박 동 규**, 황 유 동***, 유 승 엽**

The role-based access control model considering context and privacy

You-ri Lee*, Dong-Gue Park**, Yu-dong Hwang***, Seung-Yeop Yoo** ***Regular Members***

요 약

유비쿼터스 환경에서의 원격 의료 서비스가 제대로 갖춰지게 된다면 언제 어디서라도 응급 처치를 위한 치료가 가능하다. 이것은 사용자가 언제 어디서나 의료 데이터에 접근 할 수 있다는 것을 의미하며 이는 의료 데이터 보안을 위협하는 단점이 될 수 있다. 의료 데이터 보안에 대한 위협은 환자의 생명과 관련된 중요한 정보에 큰 위협을 가져 올 수 있다. 따라서 본 논문에서는 이러한 문제 해결을 위하여 유비쿼터스 환경에서의 원격 의료 서비스에 적합한 접근제어 모델을 제안하였고 이 모델을 이용하여 유비쿼터스 환경에서 원격 의료 서비스를 이용하는 사용자의 프라이버시 보호 및 유동성 있고 세밀한 접근제어가 가능하다.

Key Words : RBAC, Context, Privacy

ABSTRACT

If tele-medical service in ubiquitous environment is equiped properly, treatment for a first-aid treatment is available whenever and wherever. That means that user can approach to medical treatment data always and can get into shortcoming that threaten medical treatment data security. Threat about medical treatment data security can bring big threat to important information connected with life of patient. Therefore, in this paper, proposed suitable access control model in tele-medical service in ubiquitous environment for these problem solution. There is privacy protection and fluidity of user who use tele-medical service in ubiquitous environment using this model and minute access control is available.

Ⅰ. 서 론

유비쿼터스 환경에서의 원격 의료 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 원격 의료 시스템을 통하여 언제 어디서나 의료 피드백을 받을 수 있는 서비스를 총칭한다.

원격 의료는 컴퓨터와 데이터 통신 기술을 이용하여 의료 서비스를 전달하는 기술을 통칭하는 말이다. 1970년대 원격 의료라는 용어가 처음 사용되었으며 이는 원거리에서 환자가 의료 상담을 하는 활동만으로 제안되어 있었다.[1],[2] 그러나 오늘날의 원격진료란 개념은 먼 거리에 떨어져 있는 환자에게 전화선, 전용선(LAN) 등과 같은 데이터 통신을 이용하여 의료의 제공, 진단, 자문, 치료, 의료정보의 전달 그리고 건강교육 등을 실행하는 것이다.

원격 의료 시스템을 제대로 갖춰지게 되면 언제 어디서라도 응급 처치를 위한 치료가 가능하다. 예

※ 이 논문은 2008년도 정부재원(교육인적자원부.학술연구조성사업비)으로 한국학술진흥재단의 지원을 받아 연구되었음(KRF-2008-313-20080730).
* 한국전자통신연구원(thisglass@etri.re.kr) ** 순천향대학교 정보통신공학과(dgpark@sch.ac.kr, yoosy35@nate.com) (교신저자 : 박동규)
*** 순천향대학교 정보보호학과 (hwangyudong@gmail.com)
논문번호 : 09030-0601, 접수일자 : 2009년 6월 1일

를 들어 응급환자가 작은 병원에서 진단을 받은 후에 응급 수술이 필요하여 종합 병원으로 이송되는 경우, 환자가 이송되는 동안 환자에 대한 임상 검사 결과, X선 촬영 사진 등의 각종 의료 정보가 환자가 가고 있는 종합 병원으로 전송 된다면 종합병원에서는 환자가 도착하기 전에 환자에 대한 정확한 정보를 미리 파악하고 응급 수술에 필요한 준비를 할 수 있어서 환자가 도착하는 즉시 수술에 들어갈 수 있다. 그러나 사용자가 언제 어디서나 의료 데이터에 접근 할 수 있다는 것은 의료 데이터의 보안을 위협한다. 유비쿼터스 환경에서의 원격 의료 서비스는 환자의 의무기록 뿐 아니라 각종 검사 자료 등 환자에 대한 대부분의 정보를 데이터화 하게 되므로 인증되지 않은 사용자가 의료 데이터를 원래의 목적과 다른 목적으로 사용하게 된다면 환자의 생명과 관련된 중요한 정보에 큰 위협을 가져올 수 있다. 따라서 이러한 문제 해결을 위하여 유비쿼터스 환경에서의 원격 의료 서비스에 적합한 접근제어 모델이 필요하다.

따라서 본 논문에서는 이와 같은 필요성에 의해서 유비쿼터스 환경과 원격 의료 서비스라는 두 가지 특성을 고려하여 상황(context), 부정적인 허가(negative permission), 프라이버시, 의무(obligation)의 개념을 포함하는 접근제어 모델을 제안한다.

본 논문의 구성은 다음과 같다. 2장에서는 기존의 접근제어 모델과 관련된 연구들을 살펴보고 3장에서는 원격 의료 접근제어 시스템에 적합한 접근제어 모델을 제시하고 4장에서 RBAC 적용 예를 들고 5장에서 기존 모델과의 비교를 하며 6장에서 결론을 내린다.

Ⅱ. 관련 연구

정보 기술의 발달로 인하여 유선 환경에서의 원격 의료 시스템 뿐 아니라 무선 환경에서도 원격 의료 서비스를 받을 수 있는 유비쿼터스 환경에서의 원격 의료 시스템은 데이터의 누출, 데이터의 수정 등으로부터 원격 의료 시스템의 데이터가 안전하게 보호 되어야 한다. 이것은 개인 정보 및 시스템의 안정을 가져옴으로 원격 의료 시스템의 의료 데이터에 대한 접근을 제어하기 위한 효과적인 접근제어 방법에 대한 연구가 중요하다고 할 수 있다.

접근제어 방법 중의 하나인 역할 기반 접근제어 모델은[1]-[3] 조직에 부여된 개인의 직무나 직위에 따라 접근을 통제하는 방법으로 사용자가 다수이고 유동적으로 변화하는 원격 의료 시스템에 적합한 모델이다. 이는 접근제어 주체인 원격 의료 시스템 사용자와 접근 객체인 원격 의료 시스템 자원 사이에 역할 계층을 제공하여 사용자는 적절한 역할에 할당됨으로써 권한을 부여 받을 수 있게 된다.

이러한 접근제어 모델은 무선 인터넷의 발달로 인하여 무선 환경에 적합하게 확장되었다. 특히 무선 디바이스의 특징인 시간과 장소의 제한을 받지 않는 서비스 제공을 위하여 GRBAC[4], xoRBAC[5], CA-RBAC[6]과 같은 상황(context) 개념의 접근제어 모델이 제시되었다. 이러한 상황 기반 접근제어 모델들은 모바일 환경의 특성을 고려하고 있지만 의료 서비스 제공을 위해서 중요한 보안 요소인 프라이버시에 대해서 고려하지 못한다는 단점을 가지고 있다. 이후 프라이버시 보호를 위하여 제약(constraint) 조건을 포함하는 모바일 헬스 케어를 위한 역할 기반 접근제어 모델에 대한 연구가 이루어졌다.[7] 그러나 이 또한 헬스 케어 데이터의 프라이버시 보호를 위해 제약 조건으로만 고려함으로써 목적(purpose), 조건(condition), 의무사항(obligation) 등과 같은 프라이버시 보호 요구 사항들이 불충분하다.

P-RBAC[8] 모델은 목적, 조건, 의무 사항들을 포함하여 사용자의 프라이버시를 보호하는 접근제어 정책을 사용한다. 그러나 이는 유비쿼터스 환경에서의 원격 의료 데이터를 보호하는 중요한 상황정보 기반 접근제어를 고려하고 있지 않으며 또한 유동성 있고 세밀한 접근제어를 위한 허가-역할 제약과 의료 상황에 따른 역할 위임과 같은 다른 접근제어 요소들을 고려하고 있지 않고 있다.

따라서 본 논문에서는 유비쿼터스 환경에서의 원격 의료 시스템을 사용하는 사용자의 프라이버시 보호 및 유동성있고 세밀한 접근제어를 위한 요구사항을 분석하고 이에 적합한 접근제어 모델을 설계한다.

Ⅲ. 유비쿼터스 환경에서의 원격 의료 접근제어 시스템

2.1 접근제어 모델 요구사항

유비쿼터스 환경에서의 원격 의료 시스템의 접근제어를 위해서는 다음과 같은 조건을 만족 할 수 있는 접근제어 모델이어야 한다.

– 유비쿼터스 환경에서의 접근제어를 위해서 시간과 장소 같은 상황정보 접근제어가 가능해야 한다.

– 좀 더 세밀한 접근제어를 위하여 허가 역할

제약을 고려 할 수 있어야 한다.

– 의료 상황에 따른 역할 위임시에 동적이고 부분적인 위임을 할 수 있어야 한다.

– 사용자의 프라이버시 보호를 위하여 목적, 조건, 의무사항 들을 고려하여야 한다.

– 환자의 원치 않은 정보 공개를 막기 위하여 환자가 공개하길 원치 않는 정보는 접근이 부인 되어야 한다.

따라서 본 논문에서 제안하는 유비쿼터스 환경에서의 원격 의료 접근제어 시스템을 위한 접근제어 모델의 특징은 다음과 같다.

2.2 접근제어 모델 특징

– 대칭형 접근제어

전통적인 역할 기반 접근제어 모델은 사용자-역할 관계에 제약 조건을 사용하여 임무의 분리가 이루어져야하는 역할들을 한 사용자에게 할당하지 못하게 할 수 있다. 마찬가지로 권한-역할 관계에서도 대칭적으로 이를 적용하여 분리되어야 되는 허가 및 선행되어야 하는 허가 등을 제약 조건으로 적용한다. 이 때 역할 계층, 임무분리, 동적인 권한 특성, 공유 제한 등의 개념을 추가로 고려하여 제약 조건을 적용 하였을 때 발생 할 수 있는 문제점을 해결하고 권한 할당의 오류를 줄일 수 있다.

– 부분적인 위임

원격 의료 접근제어 시스템에서 부분적인 위임은 중요하다. 예를 들어 한 의사는 그의 역할의 전부를 위임해 줄 수 있으나 상황에 따라서는 자신이 가지고 있는 역할 중에서 몇 가지의 허가만을 위임 할 수도 있어야 할 것이다. 따라서 본 모델에서는 역할을 4가지의 부역할들로 나누어 위임 할 수 있는 역할과 위임 할 수 없는 고정적인 역할로 나누어 부분적인 위임이 가능하게 한다.

– 부정적인 허가(negative permission)

전통적인 역할기반 접근제어에서는 사용자에게 할당된 역할들은 긍정적인 권한들만 가질 수 있다. 그러나 원격 의료 접근제어 시스템에서 사용자의 프라이버시와 관련되어 사용자의 의료 정보를 특정 역할들이나 사용자에게 부인 할 수 있도록 하는 부정적인 허가가 필요하다. 따라서 본 모델에서는 긍정적인 허가와 부정적인 허가를 사용하여 사용자에게 허가를 부여하거나 허가를 부인하는 권한을 줄 수 있다. 이를 통하여 원격 의료 시스템의 유동성 있는 접근제어가 가능하게 된다.

– 상황 정보 기반 접근제어

전통적인 역할 기반 접근제어에서는 허가들이 고정되어 왔으나 의료 정보 시스템에서의 역할의 허가는 항상 정적인 것이 아니다. 때때로 허가들은 그들이 최근하고 있던 일이나 장소, 시간과 같은 상황정보에 의존하게 된다. 이는 유비쿼터스 환경에서의 원격 의료 시스템 환경에서의 상황정보에 의한 접근제어는 필수적이다.

– 목적(purpose), 의무사항(obligation), 조건(condition)

목적은 의료 데이터를 사용하는 사용자의 프라이버시 규칙을 명세하기 위해 이용되어지며 의무사항은 의료 데이터의 액션이 실행된 후 반드시 뒤따라야 하는 액션으로 가장 일반적으로 의료 데이터에 접근할 때마다 로그를 기록하는 것이다. 이렇게 로그를 기록하는 것은 프라이버시 정책들에 대하여 의무사항 일 수 있다.[9]

어떤 액션이 실행되기 전에 만나게 되는 조건은 의료 데이터를 다루는 시스템에서는 매우중요하다. 어린이 의료 데이터의 경우가 이 중 하나이다. 아이로부터 의료 데이터를 수집하고 이용하거나 어떤 다른 곳에 노출 하는 경우에는 아이의 부모로부터 동의 여부를 반드시 확인하여야 한다.

2.3 유비쿼터스 환경에서의 원격 의료 시스템에 적합한 RBAC 모델

그림 1에서 유비쿼터스 환경에서의 원격 의료 시스템에 적합한 RBAC 모델을 보여준다. 모델은 크게 상황 관리 레이어(context management layer)와 접근제어 레이어(access control layer)로 나뉜다.

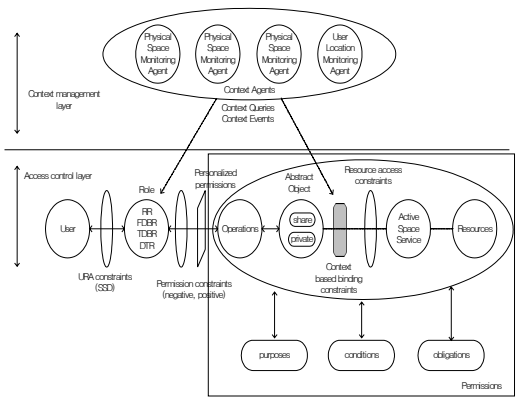

그림 1. 유비쿼터스 환경에서의 원격 의료 시스템에 적합한 RBAC 모델

2.3.1 상황 관리 레이어(context management layer)

상황 관리 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 센싱기술의 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.

2.3.2 접근제어 레이어(access control layer)

본 논문에서 제안하는 모델이 다른 접근제어 모델과 다른 주요한 구분은 이 접근제어 레이어에 있다.

역할 기반 접근제어의 표준인 NIST-RBAC 모델은 객체에 특별한 행동을 수행하도록 하나의 조건으로써의 허가를 승인한다. 따라서 다른 역할 멤버들에 의해서 실행되는 하나의 허가의 실행의 결과는 항상 같게 된다.

그림 1에서 보여지는 바와 같이 본 모델은 다른 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 위임시 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 발생시 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. 예를들어 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 역할에 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.

2.3.3 제안 모델의 구성요소

● 사용자 집합(U), 역할 집합(R), 일반적인 역할 집합(RR), 고정적으로 위임할 수 있는 역할 집합(FDBR), 임시적으로 위임 할 수 있는 역할 집합(TDBR), 위임 역할 집합(DTR), 허가 집합(P), 일반적인 역할 허가 집합(PAR), 고정적으로 위임 할 수 있는 역할 허가 집합(PAFB), 임시적으로 위임 할

수 있는 역할 허가 집합(PATB), 위임 역할 허가 집합(PAD), 일반적인 역할을 사용자에게 할당하는 집합(UAR), 고정적으로 위임 할 수 있는 역할을 사용자에게 할당하는 집합(UAFB), 임시적으로 위임할 수 있는 역할을 사용자에게 할당하는 집합(UATB), 위임 역할을 사용자에게 할당하는 집합(UAD), 위임 역할을 역할에 할당하는 집합(RAD), 객체 집합(Ob), 자원 집합(Rs), 서비스 집합(S), 오퍼레이션 집합(Op), 목적 집합(Pu), 의무사항들의 집합(O), 조건 언어 LC0로 표현되는 조건의 집합(C)

- 객체 허가들은 ObP={(op,ob) | op ∈ Op, ob ∈ Ob}
- 프라이버시와 관련 객체 허가들의 집합 PObP= {(obp, pu, c, o) | obp ∈ ObP, pu ∈ Pu, LC0로 표현된 c, o ∈ P(O)}. P(O)는 O의 멱집합
- 프라이버시 관련 객체 허가 할당 PObPA ⊆ R × PObP, 다대다의 사상으로 프라이버시 관련 객체 접근 허가를 역할에 부여하는 관계
- 허가 P ⊆ C×Op×□ (Ob)×□ (Pu)×□ (O)
  - 허가 할당 PA ⊆ R × P, 역할에 허가를 부여하는 다대다 사상 할당 관계
  - 사용자 할당 UA ⊆ U × R, 사용자에게 역할을 부여하는 다대다 사상 할당 관계
- RRH ⊆ RR × RR: 일반적인 역할 계층
- FDBRH ⊆ FDBR × FDDBR: 고정적으로 위임할 수 있는 역할 계층
- DTRHr ⊆ DTR × DTR: 한 역할이 소유한 위임 역할 계층
- DBR = FDBR ∪ TDBR: 위임 할 수 있는 역할들
- R = RR ∪ DBR ∪ DTR
- RR ∩ DBR = ∅
- RR ∩ DTR = ∅
- DBR ∩ DTR = ∅
- FDBR ∩ TDBR = ∅
- UAR ⊆ U × RR
- UAFB ⊆ U × FDBR
- UATB ⊆ U × TDBR
- UA = UAR ∪ UAFB ∪ UATB
- PAR ⊆ P × RR
- PAFB ⊆ P × FDBR
- PAD ⊆ P × DTR
- PA = PAR ∪ PAFB ∪ PAD
- RAD = TDBR × DTR

2.3.4 제안 모델의 조건(condition) 표현

제안한 모델은 조건 표현을 위해서 문맥 변수를 사용하여 표현한다. 변수들은 프라이버시와 관련된 정보를 기록한다. 비록 LC0 조건 언어가 멱집합의 표현으로 한계를 갖지만 프라이버시 허가 할당에서 일반적으로 발견되는 몇 개의 조건들에 대해서는 모델을 만들 수 있고 그 조건들은 LC0에 의해서 표현될 수 있다.

문맥 변수의 집합(CV)이라 할때, x ∈ CV의 각 변수는 유한한 영역의 가능한 값들을 갖으며 DX라고 표현한다. 모든 영역은 대응 연산자의 쌍 =, ≠을 갖는다. ⊤(true), ⊥(false)는 불변하는 조건(constant condition)이다. x ∈ CV, v ∈ DX , opr ∈ {=, ≠} 일때, CV에 대한 원자 조건은 ac는 (x opr v)의 형태로 표현되고 LC0의 조건은 아래와 같이 정의한다.

- 불변하는 조건은 LC0의 조건이다.
- 원자 조건은 LC0의 조건이다.
- Ci와 Cj가 LC0의 조건이라면, Ci ∧ Cj도 LC0의 조건이다.

원격 의료 시스템에서의 문맥 변수 사용 예

− OwnerConsent, domain = {yes, no}

개인 의료 데이터 정보를 수집하거나 사용을 위해서 소유자의 동의가 필요할 때 사용되는 문맥 변수

− ParentalConsent, domain = {yes, no}

부모의 동의가 필요한 아이들의 정보 데이터를 수집하거나 사용을 위해서 부모의 동의가 필요할 때 사용되는 문맥 변수

− OwnerAge, domain = {under13, teenage, adult}

소유자의 나이에 대한 조건을 나타날 때 사용되는 문맥 변수

− CurrentTime, domain = {9AM-5AM, 5PM-11PM, 11PM-9AM}

현재 시간에 대한 조건을 나타날 때 사용되는 문맥 변수

2.3.5 제안 모델의 의무사항(Obligation) 표현

의무사항은 액션이 일어나기 이전의 의무사항(pre-obligation)과 이후의 의무사항(post-obligation)으로 나뉜다. 또한 의무사항들은 보통 특별한 임시 제약 조건(temporal constraint)을 가진다. 임시 제약 조건은 시간 도메인의 개념을 기반으로 하며 다음과 같이 정의 한다.

임시 제약 조건 tc 의 튜플은 (ts, te, cnt)로 ts은

시작 시간(starting time), te는 끝나는 시간(ending time)으로 다음과 같이 정의한다.

• 이후 의무사항 일때 (te ≥ ts ≥ 0)

[ts, te], [te+1, 2te-ts+1], ... , [ts+(cnt-1)(te-ts+1), te+(cnt-1)(te-ts+1)]

• 이전 의무사항 일때 (0 ≥ te ≥ ts)

[ts-(cnt-1)(te-ts+1), te-(cnt - 1)(te-ts+1)], ... , [2ts-te+1,ts-1], [ts,te]

원격 의료 시스템에서의 임시 제약 조건 예

• (-6,0,1) : 0 ≥ te ≥ ts 이 조건에 만족함으로 이전 의무 사항으로 액션이 실행되기 이전에 -6부터 0까지 7일 안에 의무사항이 이행되어야 한다.

• (-6,0,2) : 0 ≥ te ≥ ts 이 조건에 만족함으로 이전 의무 사항으로 위의 정의에서 보여지는 바와 같이 계산하면 [-6-(2-1)(0--6+1), 0-(2+1)(0--6+1)]= [-13,-7] 즉 액션이 실행되기 이전 -13일부터 -7까지 7일 안에 한 번의 의무사항이 이행되어야 하며, -6일부터 0일까지 7일 안에 또 한 번의 의무사항이 이행되어야 한다.

• (0,181,1) : te ≥ ts ≥ 0 조건에 만족함으로 이후 의무 사항으로 액션이 실행된 후 0일부터 181일까지 즉 반년안에 한 번의 의무사항이 이행되어야 한다.

• (0,181,∞) : te ≥ ts ≥ 0 조건에 만족함으로 이후 의무 사항으로 액션이 실행된 후 0일부터 181일까지 한번의 의무 사항이 끊임없이 이행되어야 한다. 즉 매해 반년마다 의무 사항이 이행되어야 한다.

의무사항의 튜플은 다음과 같이 정의된다.

(c,s,op,ob,tc) : c ∈ C, s ∈ U ∪ CV, op ∈ Op, ob ∈ □ (Ob), tc ∈ T

따라서 조건, 목적, 의무사항을 모두 포함한 유비쿼터스 환경에서의 원격 의료를 위한 접근제어 모델의 허가는 다음과 같은 예와 같이 나타날 수 있다.

PA : (Doctor, ParentalConsent=yes, collect, Children information service, checkup, {(ParentalConsent= na, self, obtain, ParentalConsent,(-3,0,1))})

의사에게 검진을 목적으로 부모의 승인이 있는 아이의 정보서비스를 수집하는 역할을 부여 이을 의무 사항으로 전에 승인이 요구되어진 적이 없는 환자는 검사가 있기 3일 전부터 검사역할안에 부모의 승인을 받아야 된다.

Ⅳ. 유비쿼터스 환경에서의 원격 의료 시스템에 적합한 RBAC 모델 예

유비쿼터스 환경에서의 자원과 서비스들을 사용하기 위해서 사용자는 허가가 필요하며 이는 상황정보 제약 조건이 존재할 때 상황 정보 관리 레이어에 의해서 조건에 대한 검사를 통해서 추상객체가 된다. 제안한 모델에서의 객체는 공유와 개인으로 나누어지며 이는 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 오퍼레이션을 할당됨으로 인해서 허가가 정의된다. 위의 표는 본 논문에서 제안한 RBAC 기반의 접근제어 모델에서 역할에 허가를 할당하기 위한 허가의 예이다. N or P는 제안한 모델에서의 부정적인 허가와 긍정적인 허가를 나타내는 부분이다. 허가 1,2,3의 경우 P이기 때문에 긍정적인 허가로 역할에 긍정적인 허가를 할당하지만 허가 4의 경우 사용자의 프라이버시를 보호하기 위해서 허가 4를 할당받은 역할을 가진 사용자는 암병동에서 보험정보에 대한 수정할 수 없게 된다.

본 논문에서 제안하고 있는 접근제어 모델은 서비스와 추상 객체 사이에 상황기반 바인딩 제약 조건을 두어서 상황관리 레이어에 있는 센서로부터 상황정보에 대한 데이터 수집을 통하여 객체에 대한 오퍼레이션을 할당하게 된다. 따라서 Context에서 P(place)는 장소 T(time)는 시간을 의미한다. 예를

표 1. 제안한 RBAC 기반의 접근제어 모델에서 역할에 허가를 할당하기 위한 허가의 예

	허가 1	허가 2	허가 3	허가 4
permission	P1	P2	P3	P4
N or P	P	P	P	N
Operation	RW	RWM	W	M
Context	P	P	T	P
	진료실	응급실	09:00~11:30	암병동
Object	S	P	S	P
Service	의료관리정보	진단정보	진단처리정보	보험정보
Purpose	Promotion	Promotion	Offer	Rebate
Condition	Yes	No	No	No
Obligation	Yes	No	No	No

표 2. 기존 모델과의 비교표

Model	negative permission	user-to-user delegation	context based	partial delegation	role-to-role delegation	temporal delegation	Privacy
CA-RBAC[6]	x	o	o	x	x	x	x
A flexible Delegation Model in RBAC[7]	x	o	x	o	o	o	x
P-RBAC[8]	x	x	x	x	x	x	o
An Obligation Model[9]	x	x	x	x	x	x	o
proposed model	o	o	o	o	o	o	o

들어 허가 2의 경우는 허가 2를 할당받은 역할을 가진 사용자라 할지라도 응급실이 아닌 다른 진료실에서는 허가 받은 역할이라 할지라도 역할을 사용할 수 없게 된다.

또한 본 논문에서 제안한 허가들은 조건, 의무 목적과 같은 프라이버시 보호를 위한 요소들을 추가하여 개인화된 허가들을 제공 한다. 목적의 경우 사용자의 승진이나 환불과 같은 목적에 대한 제약조건이 필요할 때 위의 표와 같이 사용 할 수 있으며 제약의 경우 만약에 사용자가 환자이고 어린 아이라면 아이의 데이터를 사용하는데 있어서 부모의 승인이 필요한 경우 승인조건을 환자의 상태 정보를 알기 원하는 부모에게 환자의 동의가 있었을때 진료 후나 아니면 진료 전 환자 상태에 대해서 알려주어야 하는 경우 의무 사항을 Yes하여 제약 조건들을 모두 표현 할 수 있다.

Ⅴ. 기존 모델과의 비교

본 논문에서 제안한 유비쿼터스 환경에서의 원격 의료 서비스 제공을 위한 접근제어 모델이 기존의 접근제어 모델과 다른 특징은 위의 표 2와 같다.

Ⅵ. 결 론

본 논문에서는 유비쿼터스 환경에서의 원격 의료 서비스의 사용자 접근제어를 위하여 유비쿼터스 환경과 의료 서비스라는 특성을 고려하여 접근제어 모델의 요구사항을 분석하였고 그 특성인 상황(context), 부정적인 허가(negative permission), 사용자 프라이버시를 위한 목적(purpose), 제약(condition), 의무(obligation)의 개념을 포함하는 접근제어 모델을 제안하였다. 따라서 본 논문에서 제안한 유비쿼터스 환경에서의 원격 의료 시스템에 적합한 RBAC 모델을 적용하면 유비쿼터스 환경에서의 원격 의료 시스템을 사용하는 사용자의 프라이버시 보호 및 유동성 있고 세밀한 접근제어가 가능하게 된다.

참 고 문 헌

〔1〕 Ravi Sandhu., "Role-based access control." In Advances in Computers, Vol. 46. Academic Press, pp. 237-286, 1998.

〔2〕 R.S.Sandhu, E.J.Coyne, H.L.Feinstein, C.E.Youman., "Role-Based Access control Models", IEEE Computer, vol. 29, 1996.

〔3〕 David F. Ferraiolo, Janet A. Cugini, D. Richard Kuhn., "Role-based Access Control (RBAC) : Features and motivations", Proc. of 11th Annual Computer Security Application Conference, 1995.

〔4〕 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.

〔5〕 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

〔6〕 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
〔7〕 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
〔8〕 Qun Ni, Alberti Trombetta, "Privacy-aware Role Based Access Control", Symposium on Access Control Models and Technologies (SACMAT 2007), pp. 41-50, June, 2007
〔9〕 Qun Ni, Elisa Bertino, Jorge Lobo, "An Obligation Model Bridging Access Control Policicess CoPrivacy Policice", Symposium on Access Control Models and Technologies (SACMAT 2008), pp. 133-142, June, 2008

이 유 리 (You-ri Lee) 정회원

2004년 2월 순천향대학교 정보통신공학과 공학석사
2009년 2월 순천향대학교 정보통신공학과 공학박사
2009년~현재 한국전자통신연구원 보안관제기술연구팀
<관심분야> 접근제어, 유비쿼터스 컴퓨팅 보안

박 동 규 (Dong-Gue Park) 정회원

1992년 한양대학교 대학원 전자공학과 공학박사
1999~2003년 순천향대학교 정보기술공학부 부교수
2004년~현재 순천향대학교 정보통신공학과 교수
<관심분야> 네트워크 보안, 유비쿼터스 컴퓨팅 보안

황 유 동 (Yu-dong Hwang) 정회원

1998년 2월 순천향대학교 제어계측 공학과 공학사
2000년 8월 순천향대학교 전기전자공학과 석사
2003년~현재 순천향대학교 전기전자공학과 정보보호전공 박사과정
<관심분야> 네트워크 보안, 시스템 보안, 접근제어

유 승 엽 (Seung-Yeop Yoo) 정회원

2008년 9월 순천향대학교 정보통신공학과 학사
2008년 9월~현재 순천향대학교 정보통신공학과 석사과정
<관심분야> 네트워크 보안, 시스템 보안