韓國 컴퓨터情報學會 論文誌
第10卷 第3號, 2005. 7.

2005-10-3-1-12

모바일 환경에 적합한 헬스 케어 정보 시스템에서의 역할기반 접근제어

이 유 리*, 박 동 규**

Role based access control of healthcare information system for Mobile environments

You-Ri Lee*, Dong-Gue Park**

요 약

헬스 케어 정보 시스템의 데이터는 병원 업무에 필요한 많은 정보들을 포함하고 있다. 이러한 정보들은 전자 분산 환경을 통하여 네트워크 상에서 분산되어 있으며 많은 의료 관계자들은 쉽게 환자들의 정보에 접근할 수가 있다. 또한 모바일 환경의 발달로 모바일 폰을 사용하는 사용자가 급격히 증가하였고 이에 따라서 환자와 의사가 자유롭게 이동하면서 의료서비스를 주고받는 모바일 헬스 케어가 나타나게 되었다. 또한 이는 원래 목적을 위해 사용되지 않을 뿐 아니라 환자 개인의 프라이버시를 침해 할 위험을 가져 올 수 있다. 본 논문에서는 모바일 헬스 케어 정보 시스템에서의 데이터 누출 및 수정 등에 의하여 환자의 생명과 직접적인 관련이 있는 정보들을 안전하게 보호하기 위하여 사용자의 접근을 제어하는 방법을 제시하고 이를 모델링함으로써 환자 개인의 정보 및 시스템 안전을 가져올 수 있는 효과적인 접근제어 방법을 제시한다.

Abstract

The health care system revolutionized by the use of information and communication technologies. Computer information processing and electronic communication technologies play an increasingly important role in the area of health care. We propose a new role based access control model for pervasive health care systems, which changed location, time, environment information. Also our model can be solved the occurrence of an reduction authority problem to pervasive health care system at emergency environment. We propose a new role based access control model for pervasive health care systems, which combines role-to-role delegations, negative permission, context concept and dynamic context aware access control. With out approach we aim to preserver the advantages of RBAC and offer great flexibility and fine-grained access control in pervasive healthcare information systems.

▸ Keyword : RBAC, Access Control, Context, Healthcare

• 제1저자 : 이유리
• 접수일 : 2005.06.01, 심사완료일 : 2005.07.03
* 순천향대학교 정보통신공학과 박사과정, ** 순천향대학교 정보기술공학부 교수
※ 이 논문은 2004년도 한국학술진흥재단의 지원에 의하여 연구되었음.(KRF-2004-002-D00391)

Ⅰ. 서 론

최근 의료 환경은 의학의 발전, 정보통신의 발전과 더불어 병원 중심의 환경에서 환자 편의 중심의 진료 방식으로 바뀌어 가고 있다. 이에 따라서 나타난 것이 모바일 헬스 케어이다. 모바일 헬스 케어란 환자와 의사가 공간적으로 구속을 받지 않고 자유롭게 이동하면서 의료 서비스를 주고 받는 것으로 무선 통신 인프라를 통하여 이동형 무선 통신 및 컴퓨팅 장치를 사용하는 헬스 케어를 의미한다. 현재 언제 어디서나 건강상태를 점검하고 검사 자료를 곧바로 병원이나 의료 검진 센터에 전송 할 수 있는 휴대폰이 출시되고 있다. 이를 통하여 환자와 의사가 시간과 공간의 제약을 받지 않고 원하는 서비스를 제공 받을 수 있다. 그러나 사용자가 언제 어디서나 헬스 케어 데이터에 접근 할 수 있다는 것은 헬스 케어 데이터의 대한 보안을 위협한다. 이는 언제 어디서나 인증되지 않은 사용자가 헬스 케어 정보에 접근할 수 있으며 이 정보는 원래의 목적에 의하여 사용되어 지지 않으며 또한 환자의 프라이버시를 침해 할 수 있다. 따라서 환자의 생명을 다루는 헬스 케어 정보 시스템에서의 효과적인 접근제어 방법은 중요하다 할 수 있다.

본 논문에서는 모바일 기기를 통해 의사 및 환자가 헬스 케어 정보에 접근하려고 할 때 사용자의 상황(context)을 인식하여 상황에 적합한 서비스를 제공하기 위하여 상황 기반 접근제어를 고려한다. 상황을 인식하는 것이란 의사가 진료를 위하여 모바일 기기를 통해 환자 진료 데이터에 접근하려고 할 때 그 의사가 위치하고 있는 장소 또는 의사가 접속한 시간 그리고 정보 수집기에 의한 시스템의 과부하 여부를 확인하는 것을 말한다. 이는 모바일 환경에서의 접근제어의 가장 큰 특징으로 볼 수 있다. 또한 헬스 케어 정보 시스템에서의 중요한 요구사항으로 환자의 프라이버시 문제를 들 수 있다. 본 논문에서는 환자의 프라이버시의 문제 해결을 위하여 환자가 원치 않은 정보에 대해서는 공개하지 않는 방식을 고려하였으며, 또한 사용자가 자신의 역할에 할당된 권한을 모두 위임 할 수 있음과 동시에 권한을 위임 받는 사용자에게 불필요한 권한이 할당되는 것을 막기 위해 부분적인 위임을 고려 하였으며 이에 발생되는 충돌을 줄이고자 대칭 역할 기반 접근제어를 고려하여 모바일 환경의 헬스케어 정보 시스템을 위한 새로운 역할기반 접근제어 모델을 제안한다.

본 논문 구성은 다음과 같다. 2장에서는 기존의 역할기반 접근제어와 상황기반 접근제어 및 대칭 역할기반 접근제어와 같은 기존 관련 연구들을 살펴보고, 3장에서는 모바일 헬스 케어 정보 시스템을 위한 새로운 역할기반 접근제어 모델을 제시하며 4장에서는 새로 제안한 모델을 모바일 헬스 케어 정보 시스템에 적용 시켜본다. 마지막으로 5장에서는 결론 및 추후 연구를 기술한다.

Ⅱ. 관련연구

접근제어는 컴퓨터내의 자원 및 통신자원, 정보자원 등에 대하여 사용, 변경, 조회 등의 작업을 할 수 있는 능력을 가능하게 하거나 제한할 수 있는 수단으로 식별 및 인증된 사용자만이 허가된 자원에만 접근을 허용하는 기술적 방법이다.[16,17] 이는 임의적 접근 통제(DAC : Discretionary Access Control)[1], 강제적 접근 통제(MAC : Mandatory Access Control) 역할 기반 접근 통제(RBAC : Role Based Access Control)[2,3]를 중심으로 연구되어 왔다.

임의적 접근제어는 주체나 또는 그들이 속해 있는 그룹의 신분에 근거하여 객체에 대한 접근을 제한하는 방법으로 정보 보호보다는 정보의 공동 활용이 더 중요시되는 환경에 적합하며, '최소 권한(least privilege)'과 '의무분리(separation of duty)'와 같은 무결성 규칙과 관련된 보안 서비스의 제공이 어렵고 또한 정보의 유출 가능성 등으로 인해 환자의 생명을 다루는 헬스 케어 정보 시스템에는 적합하지가 않다.

강제적 접근제어는 주체들과 객체들의 보안 등급에 근거하여 주체의 객체에 대한 접근을 통제하는 방법으로 헬스 케어 정보 시스템에서 다수의 객체들에 보안 등급을 부여하는 것이 어려움으로 인해 헬스 케어 정보 시스템에서의 접근제어 방법으로는 적합하지가 않다.

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

그러나 최근 무선 환경이 발달함에 따라서 무선 환경에서의 접근제어 방식에 대한 연구가 이루어지고 있고 이는 접근 권한이 있는 사용자라 할지라도 사용자의 상황에 따라 접근 가능한 정보가 제한되어야 한다는 특징을 지니고 있다. 즉, 최근 무선 환경에서 연구되는 접근제어 방식은 전통적인 역할기반 접근제어 기법과는 달리 때때로 사용자들이 최근 하고 있던 일이나, 장소, 시간과 같은 상황에 의해 허가들이 할당되는 방식이다. [4,5,13]

대표적인 상황기반 접근제어로는 GRBAC[6]과 xoRBAC[7]을 들 수 있다.

GRBAC은 접근제어 결정에 사용자 역할(subject role), 객체 역할(object role), 환경 역할(environment role)을 사용하여 전통적인 역할기반 접근제어를 확장하여 시간에 따른 접근제어와 같은 상황 기반 접근제어를 제공한다.

xoRBAC은 역할기반 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.

이러한 방식은 사용자에게 역할을 부여함으로써 권한을 부여하게 된다. 즉, 권한을 부여 받기 위하여 역할에 할당되어야 한다는 것이다. 그러나 실제적으로 사용자에게 필요한 것은 권한이다. 따라서 대칭 RBAC[8]과 같이 사용자-역할 관계에 필적하는 수행을 갖는 허가-역할 관계를 지원 할 필요성이 있다. 대칭 RBAC 모델은 임무분리와 역할의 계층구조를 고려한 권한 할당 제약조건을 제시함으로써 역할의 이해관계 충돌과 권한의 공유와 통합을 권한 할당에 반영하는 모델이다.

위 모델들은 최근 연구되고 있는 접근제어 방식들이다. 그러나 이 모델들은 헬스 케어 환경에서의 사용자의 프라이버시와 관련되어 사용자의 헬스 케어 정보를 특정 역할들이나 사용자에게 사용하지 못하도록 할 수 없으며, 또한 의료 상황에 따른 역할 위임과 부분적인 위임을 고려하지 못한다는 단점이 있다.

따라서 본 논문에서는 모바일 환경에서 사용자의 위치나 장소에 따라서 헬스 케어 환경에 부여된 사용자의 직무나 직위에 따라 접근을 통제하는 방법인 상황기반의 접근제어에 대칭 역할기반 접근제어의 개념을 통합하고 의료 상황에 따른 부분적인 위임과 환자의 프라이버시 보호를 위한 부정적인 허가의 개념을 동시에 고려하여 모바일 환경에 적합한 헬스 케어 정보 시스템의 접근제어 모델을 제안한다.

III. 새로운 역할기반 접근제어 모델

위의 내용으로 알 수 있듯이 모바일 환경에서의 헬스 케어 정보 시스템 접근제어를 위해서는 다음과 같은 조건을 만족할 수 있는 접근제어 모델이어야 한다.

- 모바일 환경에서의 접근제어를 위한 시간과 장소와 같은 상황정보 접근제어가 가능해야 한다.
- 헬스 케어 환경에서의 좀 더 세밀한 접근제어를 위한 허가 역할 제약을 고려 할 수 있어야 한다.
- 역할 계층에서 역할 위임시에 동적이고 부분적인 위임을 할 수 있어야 한다.
- 사용자의 프라이버시와 관련하여 환자가 공개하길 원치 않는 정보는 접근이 부인되어야 한다.

본 논문에서는 모바일 헬스 케어 환경에 적합한 접근제어를 적용하기 위하여 위의 조건을 만족하는 새로운 역할기반 접근제어 모델을 제안한다.

제안된 모델은 다음 (그림 1)과 같이 표현 할 수 있다. 시간제약과 장소의 제약 및 허가 역할 제약 등은 (그림 1)의 constraint로 표현하고 부분적인 위임과 관련하여 하나의 역할을 여러 개의 부역할로 나누었으며 부정적인 허가를 위하여 허가를 두 가지로 나누었음을 알 수 있다.

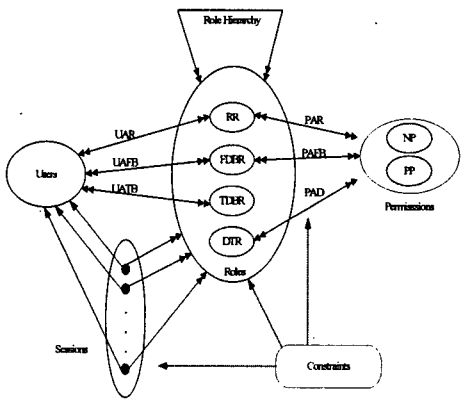


그림 1 모바일 헬스 케어 시스템을 위한 새로운 역할기반 접근제어 모델

Fig 1. New Role based access control model for mobile healthcare system

3.1 역할 계층

역할은 역할의 구성원에게 부여된 책임, 권한과 관련하여 연관된 의미를 가진 모바일 헬스 케어 시스템 내의 직무 기능이나 명칭을 말하며 각 역할의 계층에는 부역할 계층이 존재한다. 부역할은 부분 위임과 관련하여 일반적인 역할(Regular roles : RR), 고정적인 위임 역할(Fixed delegatable roles : FDBR), 임시적 위임 역할(Temporal delegatable roles : TDBR) 그리고 위임 역할(Delegation role :DTR)로 분류된다.[9] 일반적인 역할은 위임이 불가능한 역할 고유의 부역할이며, 고정적 위임 역할과 임시적 위임 역할은 위임이 가능한 역할들이다. 또한 위임 역할은 사용자가 아닌 역할에 위임을 할 수 있는 부역할로 역할 대 역할의 위임이 가능하다.

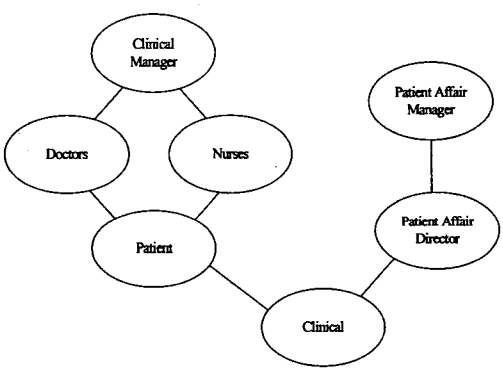


그림 2 모바일 헬스 케어 정보 시스템을 위한 역할 계층의 예
Fig 2. Role hierarchy for mobile healthcare system

표 1 허가 역할 할당
Table 1. Permission role assignment

role	permission
CM(Clinical Manager)	BPD_RWM, DD_RWM, PHD_RWM, ID_RWM, P_RWM
D(Doctor)	BPD_R, DD_RWM, PHD_RWM, ID_R, P_RWM
N(Nurse)	BPD_R, DD_R, PHD_RWM, ID_R, P_R
P(Patient)	BPD_R, DD_R, PHD_R, ID_R, P_R

BPD: Basic Patient Data(기초 환자 정보)
DD: Diagnosis Data(진단정보)
PHD: Patient Health Data(환자 건강 정보)
ID: Insurance Data(보험정보)
P: Prescription(처방전)
R: read(읽기) W: write(쓰기)
M: modify(수정) D: deny(부인)

표 2 허가-역할 할당의 예
Table 2. For example permission-role assignment

PAR (Permission regular role assignment)

RR	Permissions
CM	BPD_RWM
D	DD_RWM, PHD_RWM
N	PHD_RWM
P	BPD_R,DD_R, PHD_R

PAFB (Permission fixed delegatable role assignment)

FDBR	Permissions
CM′	ID_RWM
D′	P_RWM
N′	
P′	ID_R,P_R

PATB (Permission temporal delegatable role assigement)

TDBR	Permissions
CM″	
D″	
N″	
P″	D1

PAD (Permission delegation role assignment)

DTR	Permissions
D1	P_RWM
	ID_RWM

〈표 1〉과 〈표 2〉는 허가-역할 할당의 예를 보여준다. 이는 권한의 부분적인 위임을 위하여 사용된다. 즉, 사용자는 자신의 모든 권한을 위임하여 줄 수도 있으나 좀 더 세밀한 접근제어를 위해서는 모든 권한 뿐 아니라 부분적인 권한의 위임이 필요하다.

PAD에 D1이라는 위임 역할을 생성하고 이는 Doctor의 위임할 수 있는 허가(보험 정보 읽고 쓰고 수정하기(PHD_RWM) 권한)와 의료 관리자의 위임할 수 있는 허가(처방전 정보 읽고 쓰고 수정하기(P_RWM) 권한)을 할당받아서 이를 환자의 임시 위임 역할(P″)에 할당한다. 위임 역할 D1을 새로 생성하여 TDBR에 위임할 권한을 부여함으로써 권한 기반으로 위임할 수 있으며 또한 D1이라는 역할을 P″에 할당함으로써 동적 위임이 일어남으로써 유동성 있는 접근제어가 가능하게 된다.

3.2 허가

전통적인 역할기반 접근제어의 기본적인 개념은 사용자가 역할에 할당되고, 역할에 허가가 할당되며 사용자는 역할의 멤버가 됨으로써 허가를 얻는다. 그러나 모바일 헬스 케어 정보 시스템을 위한 새로운 RBAC 모델에서의 기본적

인 개념은 사용자가 역할에 할당되고, 역할에 긍정적인 허가가 할당되면 사용자는 역할의 멤버가 됨으로써 허가를 얻지만 역할에 부정적인 허가가 할당되면 사용자는 역할의 멤버가 될 수가 없다. 즉, 허가는 (그림 1)에서 보여 지는 것과 같이 긍정적인 허가(PP: Positive Permission)와 부정적인 허가(NP: Negative Permission)[10][15]로 이루어져 있다. 부정적인 허가는 모바일 헬스 케어 정보 시스템에서 환자의 프라이버시를 위해서 중요한 개념이다. 이는 접근을 부여 하는 것 보다 부인하는 개념으로 환자가 자신의 진료 기록이 공개되어지는 것을 원치 않을 때 환자의 프라이버시를 위하여 사용할 수 있다. 예를 들어 내과에 있는 모든 간호사들은 환자의 진단 정보를 볼 수 있는 권한을 가지고 있다고 가정하자. 그러나 Bob은 암에 걸렸고 이 사실을 가족인 누구에게도 알리지 않고 싶어 하는데, Bob의 가족 중 한명이 이 내과의 간호사라면 Bob의 진단 정보를 확인하여 Bob이 암에 걸린 사실을 알 수가 있다. 이 때 Bob의 프라이버시를 보호하기 위하여 이 간호사에게 자신의 진단 정보에 대해서 부정적인 허가를 부여함으로써 Bob은 자신의 프라이버시를 침해 받지 않을 수 있다. 이렇듯 헬스 케어 정보 시스템에서 환자의 프라이버시를 지켜주기 위해서 부정적인 허가는 필수적인 요소라고 할 수 있다.

위 (그림 2)와 같은 역할 계층이 존재할 때 PM(Patient Affair Manger)의 허가 역할 할당은 다음 〈표 3〉과 같고 D의 위임 할 수 있는 역할 P_RWM과 PM의 위임할 수 있는 역할 DD_D를 위임 역할 D2에 동적 할당하고 이를 CM에 할당한다면 동적 위임이 일어남과 동시에 CM은 DD_RWM의 긍정적인 허가와 DD_D의 부정적인 허가가 부여됨으로써 DD의 허가에 대한 충돌이 발생하게 된다. 이렇듯 긍정적인 허가와 부정적인 허가는 역할의 상속과 위임에 의하여 권한의 충돌을 가져올 수 있다. 이와 같은 권한의 충돌은 모바일 헬스 케어 정보 시스템의 특성상 응급 상황을 위하여 헬스 케어 정보를 공개 할 것인지 또는 사용자의 프라이버시를 위하여 헬스 케어 정보를 비공개 할 것인지의 두 가지 특성을 고려해야 하며, 이 두 가지의 우선순위는 권한 정책 수립을 통하여 해결 할 수 있다.

표 3 PM의 허가 역할 할당
Table 3. permission role assignment of PM

role	negative permission
PM	BPD_RWM, DD_D, PHD_D

PAR		PAFB	
RR	Permissions	FDBR	Permissions
PM	BPD_RWM	PM'	DD_D, PHD_D
PATB		PAD	
TDBR	Permissions	DTR	Permissions
PM''		D2	P_RWM
			DD_D

3.3 제약 조건

모바일 환경에서의 헬스 케어 정보 시스템 접근제어를 위해서 상황정보 제약조건, 사용자-역할 할당 제약조건 그리고 권한-역할 할당 제약조건을 고려해야 한다.

3.3.1 상황정보 제약 조건

모바일 헬스 케어 정보 시스템에서의 접근제어는 여러 가지 보안과 관련된 상황정보를 포함한다. 즉, 접근 권한이 있는 사용자라 할지라도 사용자의 상황에 따라서 접근 가능한 정보가 제한되어야 한다. 따라서 모바일 헬스 케어 정보 시스템을 위한 상황정보 제약조건에는 시간, 장소, 자원 시스템 정보가 있다. 즉, 장소, 시간, 시스템 정보(네트워크 밴드위스, CPU의 사용, 메모리의 사용)에 의하여 모바일을 이용하여 헬스 케어 정보 시스템에 접근하고자 할 때 사용자의 권한은 변화 할 수 있다.

예를 들어 스마트 병원이라고 가정할 때, 상황 정보 수집기가 존재하여 모바일 사용자가 어느 곳에 위치하며 몇 시인지 CPU와 메모리 사용이 어떠한지를 종합하여 사용자의 권한을 활성화 시킨다.[11]

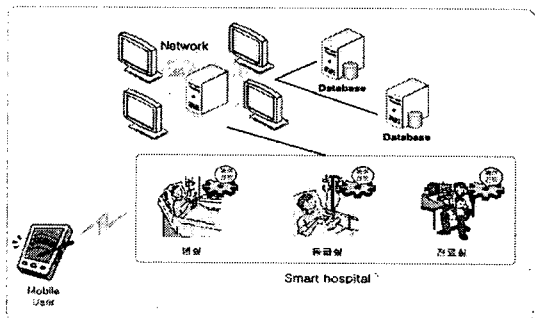


그림 3 모바일 헬스 케어 정보 시스템
Fig 3. Mobile healthcare information system

위치하는 곳에서의 사용자가 사용하려고 하는 자원의 CPU와 메모리 사용이 많다면 사용자의 권한은 축소 될 수 있다. 그러나 모바일 헬스 케어 정보 시스템의 특성상 응급 상황의 경우, 급히 환자의 정보에 접근하려고 할 때 환경의 영향 때문에 의사의 권한이 축소된다면 환자의 생명이 위험할 수 있다. 따라서 모바일 헬스 케어 정보 시스템에서는 상황에 따른 동적 접근제어와 함께 환경에 따라서 역할이 변화 되어서는 안 되는 역할도 함께 정의 되어야 한다. 위와 같은 상황정보 제약 조건을 통하여 모바일 헬스 케어 정보 시스템에서의 사용자의 동적인 역할의 할당이 가능하다. 이러한 상황정보 제약 조건은 권한의 충돌을 가져올 수 있다. 이런 경우에는 두 룰 사이의 명백한 우선순위를 할당함으로써 해결 할 수 있다.[12][14]

다음 〈표 4〉는 주체 상황 정보 할당의 예를 나타낸 표이다. 각 주체들에게 다음 〈표 4〉에서 보여 주는 것처럼 상황정보 제약을 할당 하였다면, 주체들은 자신들이 권한을 가지고 있다고 하여서 그 권한을 활성화 시킬 수 없다. 예를 들어 day_doctor는 기초 환자 정보를 읽을 수 있고 환자의 진단 정보를 읽고 쓰고 수정 할 수 있는 권한을 가지고 있다.

표 4 주체 상황정보 할당의 예
Table 4. For example subject context information assignment

Subject	Place	Time	User	Priority
day_doctor	병원	(9,19)		
night_doctor	병원	(19,9)		
day_nurse	처치실	(9,19)		High
night_nurse	처치실	(19,9)		High
Tom	암병동	(9,19)	암환자	

그러나 위에 상황정보가 할당 되어 있으므로 day_doctor는 병원에서 9시에서 오후 7시 사이에만 자신이 가지고 있는 권한, 즉 기초 환자 정보를 읽고 환자의 진단 정보를 읽고 쓰고 수정 하는 등의 일을 할 수 있다. 주체가 간호사의 역할을 부여 받았다면, 간호사의 역할에 할당되어있는 허가들에 대해서 권한을 부여 받게 된다. 만약에 Tom이 day_nurse라고 한다면 처치실에서 9시부터 19시 사이에 간호사 역할에 할당되어 있는 권한을 사용 할 수 있을 것이다. 그러나 〈표 4〉에서 보여 지는 바와 같이 상황정보가 할당 되어 있어 있기 때문에 상황정보 접근 제어 정책에 따라서 새로운 것이 우선함으로써 자신이 가지고 있는 day_nurse의 역할은 오버라이딩 되어 Tom은 암병동에서 9시부터 19시까지 암환자의 기본정보, 진단정보, 건강정보에 대해서만 읽기 권한을 가질 수 있다.[4]

이처럼 문맥 정보를 통하여 사용자의 권한을 활성화 시켜 줌으로써 의료 정보 시스템에서의 사용자의 좀 더 세밀한 접근제어가 가능하다.

3.3.2 사용자-역할 할당 제약 조건

사용자 역할 할당 제약 조건은 정적 의무분리(SSD: Static Separation of Duty)와 동적 의무분리(DSD: Dynamic Separation of Duty)로 나뉜다. 정적 의무분리에 속한 역할은 두 개의 역할이 상호 배타적 이어야 한다는 필수조건이 있기 때문에 한 사용자에게 두 개 이상의 역할에 할당될 수 없다. 동적 의무분리에 속한 역할은 사용자가 독립적으로 행동할 때는 이해의 상충을 생성하지 않으므로 두 가지 이상의 역할에 할당되는 것은 허용이 되나, 두 역할이 활성화 되는 것은 금지 한다. 따라서 두 개 이상의 역할에 할당될 수 있으나 한 세션상에서 동시에 활성화 될 수 없다.

3.3.3 권한-역할 할당 제약 조건

권한 할당 제약조건은 확장된 대칭형 접근제어 모델을 따른다.[8] 이는 기존 사용자-역할 관계에 적용했던 제약조건을 권한-역할 관계에도 대칭적으로 적용하며 적용과정에서 역할의 계층구조, 임무분리, 동적인 권한특성, 공유제한 등의 개념을 추가로 고려한 모델로 단순히 사용자 할당 제약 조건을 권한 할당 제약조건으로 적용할 경우 발생할 수 있는 문제들을 해결하고 권한 할당의 오류를 줄일 수 있는 모델이다. 권한 할당 제약 조건은 다음 〈표 5〉와 같다.

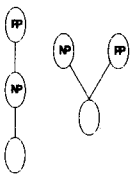
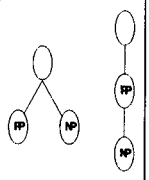
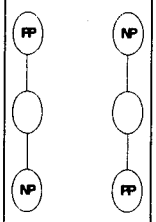
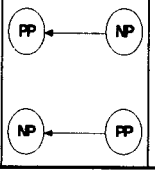
표 5 권한 할당 제약 조건
Table 5. permission assignment constraint

제약조건	설명
DP (Disjoint permissions)	- 분리 권한 제약 조건 - 동일한 권한은 정적인 임무 분리가 선언된 두 개 이상의 역할에 할당되지 못한다. - dp에 속한 권한은 ssd에 속한 두 개 이상의 역할에 할당될 수 없다.
CP (Conflicting permissions)	- 충돌 권한 제약 조건 - 충돌 권한들은 동일 역할에 할당될 수 없다. - 두 권한 사이의 이해 관계의 충돌과 임무분리를 동시에 고려하여 충돌권한에 의해 발생 할 수 있는 권한 할당의 오류를 줄인다. - cp에 속한 권한은 동일한 역할에 둘 이상 할당 될 수 없다.

PP (Prerequisite permission)	- 선행 권한 제약 조건 - AND 관계시 선행 역할을 필요로 하는 권한을 역할에 할당하기 위하여 선행 권한의 집합의 모든 권한이 할당되어야 한다. - OR 관계시 선행 역할을 필요로 하는 권한을 역할에 할당하기 위하여 선행 권한의 집합의 권한 중에 하나 이상의 권한이 할당되어야 한다.
PASR (Permission assigned to single role)	- 단일 역할에만 권한 할당 - 역할과 권한이 강한 연관 관계를 가지는 경우 권한의 공유를 제한하는데 유용 - 업무 특성상 또는 보안 관리상의 이유로 특정 권한을 한 역할에만 할당하는 경우 사용됨

그러나 모바일 헬스 케어 시스템을 위한 새로운 역할기반 접근제어 모델에서 위의 권한 할당 제약 조건만 가지고서는 부정적인 허가와 긍정적인 허가의 충돌을 방지할 수 없다. 따라서 허가의 상속 및 위임을 위하여 〈표 6〉과 같은 제약조건이 필요하다. D_CP는 자식 역할이 부정적인 허가를 가지고 있을 때 부모 역할이 자식에게 자신의 긍정적인 허가를 위임함으로 인하여 충돌 권한에 의해 발생 할 수 있는 권한 할당의 오류를 줄이기 위한 것이다. 예를 들어 자식 역할인 환자 역할은 진료 데이터 읽기에 대한 부정적인 허가를 가지고 있는데 간호사가 이 환자에게 진료 데이터 읽기 권한을 위임 했을 때 발생 할 수 있는 충돌이다. I_CP는 역할 계층상에서 부모 역할은 긍정적인 허가를 가지고 있을 때 자식의 역할이 부정적인 허가를 상속함으로 인하여 충돌 권한에 의해 발생 할 수 있는 권한 할당의 오류를 줄이기 위한 것이다. 예를 들어 부모 역할인 간호사는 환자의 진료 데이터 읽기 권한을 가지고 있을 때 자식 역할인 환자는 환자의 진료 데이터 읽기에 대한 부정적인 권한을 가지고 있다면 환자의 이 권한의 상속이 이루어질 때 발생 할 수 있는 충돌이다. DI_CP는 D_CP와 I_CP 두 가지 모두에 의하여 발 생 할 수 있는 충돌을 말한다. DTR_CP는 역할 대 역할 위임으로 인하여 자신이 가지고 있는 권한과 위임된 역할의 충돌이 이루어 졌을 때 발생 할 수 있다.

표 6 권한 할당 제약 조건 추가
Table 6. permission assignment constraint additions

D_CP (Delegation_Conflicting permissions)		- 위임으로 인해 발생할 수 있는 충돌 - 같은 허가에 대해서 부모 역할이 긍정적인 허가와 부정적인 허가를 모두 지니고 있어서 두 가지 모두를 위임받게 되었을 때 생기는 충돌 - 헬스 케어의 특성상 환자의 프라이버시를 위하여 부정적인 허가를 우선
I_CP (Inheritance_Conflicting permissions)		- 상속에 의해 발생할 수 있는 충돌 - 같은 허가에 대하서 자식 역할이 긍정적인 허가와 부정적인 허가를 모두 지니고 있어서 두 가지 모두를 상속받게 되었을 때 생기는 충돌 - 헬스 케어의 특성상 환자의 프라이버시를 위하여 부정적인 허가를 우선
DI_CP (Delegation_Inheritance_Conflicting permissions)		- 위임과 상속으로 인해 발생할 수 있는 충돌 - 부모의 긍정적인 허가의 위임과 자식의 부정적인 허가의 상속 또는 부모의 부정적인 허가의 위임과 자식의 긍정적인 허가의 상속으로 인하여 생기는 충돌 - 헬스 케어의 특성상 환자의 프라이버시를 위하여 부정적인 허가를 우선
DTR_CP (Delegation_role_Conflicting permissions)		- 역할 대 역할 위임에 의하여 생기는 충돌

3.4 제안 모델의 정형적 명세

제안 모델을 정형적으로 표현하면 다음과 같다.

3.4.1 제안모델의 주요 함수

U(사용자 집합), S(세션 집합), P(허가 집합), R(역할 집합), RR(일반적인 역할 집합), FDBR(고정적으로 위임할 수 있는 역할 집합), TDBR(임시적으로 위임할 수 있는 역할 집합), DTR(위임 역할 집합), PAR(일반적인 역할 허가 집합), PAFB(고정적으로 위임할 수 있는 역할 허가 집합), PATB(임시적으로 위임할 수 있는 역할 허가 집합), PAD(위임 역할 허가 집합), UAR(일반적인 역할을 사용자

에게 할당하는 집합), UAFB(고정적으로 위임할 수 있는 역할을 사용자에게 할당하는 집합), UATB(임시적으로 위임할 수 있는 역할을 사용자에게 할당하는 집합), UAD(위임 역할을 사용자에게 할당하는 집합), RAD(위임 역할을 역할에 할당하는 집합)

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
user_r(r) : RR → 2U: 사용자들에게 일반적인 역할을 매핑하는 함수
user_fb(r) : FDBR → 2U: 사용자들에게 고정적으로 위임할 수 있는 역할을 매핑하는 함수
user_tb(r) : TDBR → 2U: 사용자들에게 임시적으로 위임할 수 있는 역할을 매핑하는 함수
own_fb(r) : FDBR → RR: 일반적인 역할에 고정적으로 위임할 수 있는 역할을 매핑하는 함수
own_tb(r) : TDBR → FDBR: 고정적으로 위임할 수 있는 역할에 임시적으로 위임할 수 있는 역할을 매핑하는 함수
∀rr ∈ RR , ∃u : U, fdbr : FDBR, tdbr : TDBR • (u, rr) ∈ URA∧rr = own_ fb(fdbr)∧fdbr = own_tb(tdbr) ⇒ user_r(rr) = user_fb(fdbr) ∧ user_fb(fdbr) = user_tb(tdbr): 모든 사용자들은 일반적인 역할, 고정적으로 위임할 수 있는 역할, 임시적으로 위임할 수 있는 역할을 할당받는다.
own_d(r) : FDBR → 2DTR and ∄(fdbr1 fdbr2 ∈ FDBR, dtr ∈ DTR) • (fdbr1 ≠ fdbr2) ∧(dtr ∈ own_d(fdbr1) ∧ dtr ∈ own_d(fdbr2)): 위임 역할들의 집합(DTR)에 고정적으로 위임할 수 있는 역할 (FDBR)을 매핑하는 함수
rad(r) : TDBR → 2DTR: 위임 역할들의 집합(DTR)에 임시적으로 위임할 수 있는 한 역할(TDBR)을 매핑하는 함수
permissions_r(r) : RR → 2P, 허가들의 집합에 일반적인 역할들을 매핑시키는 함수
permission_fb(r) : FDBR → 2P, 허가들의 집합에 고정적으로 위임할 수 있는 역할들을 매핑시키는 함수
permissions_d(r) : DTR → 2P, 허가들의 집합에 위임 역할들을 매핑시키는 함수
permissions_t*(r) : TDBR → 2P: RAD로부터 상속받은 허가들의 집합에 임시적으로 위임할 수 있는 역할들을 매핑시키는 함수
permissions_f*(r) : FDBR → 2P: PAFB와 RAD와 함께 위임할 수 있는 허가들의 집합에 고정적으로 위임할 수 있는 역할들을 매핑시키는 함수(멀티 스텝 위임일 때 가능)
permissions_r(r) = {p : P |∃r′ ≤ r • (r′, p) ∈ PAR}
permissions_fb(r) = {p : P |∃r′ ≤ r • (r′, p) ∈ PAFB}
permissions_d(r) = {p : P | ∃r′ ≤r • (r′, p) ∈ PAD}
permission_t*(r) = {p : P |∃r′ ∈ DTR • (r′, p) ∈ PAD∧r′ ∈ rad(r′)}
permissions_f*(r) = {p : P | (r, p) ∈ PAFB} ∪ {p : P | ∃r′ ∈ TDBR • p ∈ permissions_t*(r′) ∧r = own_tb(r′)}
∀dtr ∈ DTR, ∃fdbr ∈ FDBR • (dtr∈ own_d(fdbr) ∧ (p e r m i s s i o n s _ d (d t r) ⊆ permission_f*(fdbr)): 멀티 스텝 위임이 가능할 때 FDBR에 의해 위임될 수 있는 DTR에 위임될 수 있는 권한은 PAFB와 RAD에 의해서 이 역할에 할당된 권한들이다.

Authorization Token(인증토큰 : 역할이 가지고 있는 허가 중에서 가능한 허가만을 선택한다.)

Authorization Token은 7개의 튜플로 이루어져 있다.

표 7 접근제어 모델 비교
Table 7. access control model compare

Model	negative permission	user-to-user delegation	context based	partial delegation	role-to-role delegation	temporal delegation	permission-role constraint
A novel use of RBAC(6)	o	o	x	x	x	x	x
A context-related access control(1)	x	o	o	x	x	x	x
An authorization model for e-Consent(2)	o	o	o	x	x	x	x
A flexible Delegation Model in RBAC(3)	x	o	x	o	o	o	x
Symmetric RBAC(8)	x	o	x	x	x	x	o
proposed model	o	o	o	o	o	o	o

〈p,obj, r, t_inst, usage_count, denied_users, executors〉
p는 허가
obj는 객체
r은 역할
t_inst는 작업 인스턴스
usage_count는 시간의 숫자
denied_user는 가능한 허가를 받지 않은 사용자의 이름
executors는 가능한 허가를 사용하려고 하는 사용자
Auth_Tokens(인증토큰의 집합)
AToken(t_inst) : T_INST → 2Auth_Toekns : 작업 인스턴스(t_inst)에서 가능한 허가들을 생성해주는 인증토큰의 집합
PAuth_Token(at) : Auth_Tokens → P, 인증토큰(at)에서 가능한 허가들을 매핑시키는 함수
RAuth_Token(at) : Auth_Tokens → R, 가능한 허가들을 위한 역할들을 매핑시키는 함수
OAuth_Token(at) : Autho_Token → Obj, 활동이 인증된 객체들을 매핑시키는 함수
CountAuth_Token(at) : Auth_Tokens → N, 인증토큰(at)에서 사용하고 있는 최근값을 매핑시키는 함수
Executors(at) : Auth_Tokens → 2U, 사용자들이 마지막으로 사용할 가능한 허가들을 매핑시키는 함수
Enabled_PR(r,obj) : R × Obj → 2P, 객체를 사용하는 역할의 가능한 허가들을 매핑시키는 함수
Denied_Users(at) : Auth_Tokens → 2U, PAuth_Token(at)의 사용이 부인된 사용자들을 매핑시키는 함수
Enabled_permission_user(r) : 가능한 허가 사용자
$\forall at \in Auth\_Tokens, \forall u \in Executors(at)$
$u \in user\_r(RAuth\_Token(at)) \vee$
$\exists r \in R : (RAuth\_Token(at) \rightarrow r) \wedge u \in user\_r(r)$
Enabled_permission_role(r) : 역할들에 가능한 허가
$\forall r \in R, \forall p \in PR(r), \forall obj \in ObP(p)$
$p \in Enabled\_PR(r, obj) \Rightarrow$
$\exists t \in T, \exists at \in AToken(t\_inst) :$
$p \in PAuth\_Token(at) \wedge r \in RAuth\_Token(at) \wedge$
$obj \in OAuth\_Token(at) \wedge$
$CountAuth\_Token(at) \neq 0$

3.4.2 상황 정보 제약조건의 정형적 명세

〈Subject, Object, Authorization type, Operation, Place, Time, Patient, System information, priority 〉

Subject - 사용자를 말하며 환자나 의사와 같이 자원을 사용할 주체
Object - 사용자가 사용할 자원을 의미
Authorization type - Type={-, +}, -는 부정적인 허가를 나타내며 +는 긍정적인 허가를 나타냄

Place - 사용자가 어느 장소에서 자원에 대해 접근할 수 있는지에 대한 장소 상황 정보

Time - 사용자가 어느 시간에 자원에 접근 할 수 있는지에 대한 시간 상황정보로 (begin, end) 형태를 지님, (-∞,∞) 다음과 같이 나타났을 때 항상 권한이 가능함을 나타냄

Patient - 주체가 특별히 관리해야 하거나 관리하고 있는 사용자(환자) 상황을 말함

System information - 사용자가 자원에 접속할 상황에 대한 네트워크 밴드위스, CPU와 메모리 사용과 같은 시스템 정보 상황을 말함

priority - 우선순위 상황정보를 제공함으로써 사용자 권한의 충돌을 방지 할 수 있음

예를 들어

〈진료의사, 환자 진료 기록, +, 읽기/쓰기, 진료실, (-∞, ∞), 암환자〉

다음과 같은 형태를 지니고 있는 권한이 있다면, 진료의사는 암환자의 환자 진료 기록에 대해서 진료실에서 읽기 쓰기 권한을 활성화 시킬 수 있다. 즉, 이 진료의사가 진료실을 빠져나가 검사실에서 환자의 진료 기록을 보고자 한다면 이 진료의사는 환자 진료 기록의 읽기 쓰기 권한을 가지고 있다고 하더라도 그 권한을 활성화 하지 못한다. 또한 진료의사가 접속했을 때 네트워크 밴드위스와 CPU의 사용이 많다면 진료의사는 읽기 쓰기 기능을 다 가지고 있다고 하여도 읽기 기능만을 활성화 시키며 쓰기 기능을 할 수 없다. 그러나 모바일 헬스 케어 정보 시스템은 사람의 생명을 다루기 때문에 응급 상황과 같은 위급한 상황 시 권한이 축소되었을 때

문제가 발생할 수 있다. 따라서 응급상황에 대한 우선순위를 높게 두어서 사용자 권한의 충돌이 발생 하였을 때 응급상황에 대한 대처를 먼저 할 수 있도록 할 수 있다.

3.4.3 권한 할당 제약조건의 정형적 명세

DP 제약조건

$$\forall ssd \left(\bigcap_{d=1}^{q} perms(srd) \cap dp \right) = \varnothing$$

CP 제약조건

$$\forall (r, cp)\ (counts(perms(r) \cap cp) \leq 1)$$

PP 제약조건

(i) $\forall r \forall pp(((tp \in perms(r)) \wedge (ao='AND')) \ pps \subseteq perms(r))$

(ii) $\forall r \forall pp(((tp \in perms(r)) \wedge (ao='OR')) \ pps\_pi \subseteq perms(r))\ (1 \leq i \leq w)$

PASR 제약조건

$\forall pasr\ ((pasr\_ps \subseteq perms(pasr\_r)) \wedge (pasr\_ps \cap \cup perms(cp\_rk)) = \varnothing$

3.5 이전 연구와 모바일 환경에서의 헬스 케어 시스템의 접근제어 모델의 비교

〈표 7〉은 모바일 헬스 케어 정보 시스템을 위한 접근제어 모델의 특성을 요약하고 관련 연구들과 비교 한 것이다. 모바일 헬스 케어 정보 시스템을 위한 접근제어 모델은 이전 헬스 케어 정보 시스템에 부정적인 허가의 개념과 사용자 대 사용자 위임, 역할 대 역할 위임, 부분적인 위임이 가능한 통합적인 모델이다. 또한 모바일 환경의 특성을 고려하여 상황정보 제약과 사용자 역할 할당 제약 그리고 허가 역할 할당 제약을 고려하여 좀 더 세밀하고 유동성 있는 접근제어를 할 수 있다.

Ⅳ. 모바일 헬스 케어 시스템 접근제어의 예

모바일 헬스 케어 시스템의 접근제어를 위한 그림 역할 계층을 아래 (그림 4)와 같이 볼 수 있다.

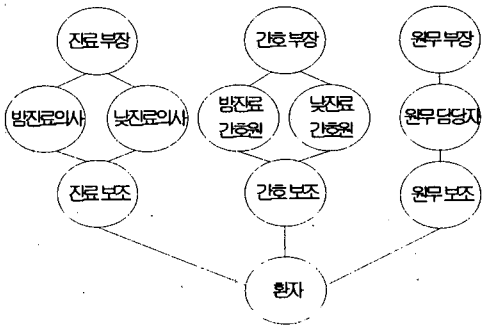


그림 4 모바일 헬스 케어 정보 시스템 접근제어 역할계층의 예
Fig 4. For example role hierarchy of role based access control for mobile healthcare information system

〈표 8〉은 모바일 헬스 케어 정보 시스템에서의 사용자와 역할 그리고 허가의 예이다. 사용자는 허가를 할당받은 역할을 할당 받음으로써 권한을 부여 받게 된다. 이를 제안된 부역할로 나타내보면 다음 〈표 9〉와 같다. 각 역할은 다음과 같이 위임에 따라서 부역할로 나뉘며 D1이라는 위임 역할을 R12''에 임시 역할로 할당함으로써 R12의 역할을 지닌 사용자는 〈표 8〉에서 보는 바와 같이 User12로 P12와 P13의 권한을 할당 받았으므로 기초 환자 정보를 읽고 쓰고 수정할 수 있는 권한과 진단정보 부인 그리고 진단처리 정보 읽기 권한을 사용 할 수 있다.

표 8 모바일 헬스 케어 정보 시스템에서의 허가-역할 할당과 사용자-역할 할당의 예
Table 8. For example permission-role assignment and user-role assignment for mobile healthcare information system

User	Role		Permission		
				Object	Operation
User1	R1	진료부장	P1	의료관리정보	RWM
User2	R2	간호부장	P2	간호관리정보	RWM
User3	R3	원무부장	P3	원무관리정보	RWM
User4	R4	밤진료의사	P4	진단정보	RWM
			P5	처방전	RWM
			P6	환자건강정보	RWM
			P7	응급진료정보	RWM
User5	R5	낮진료의사	P4	진단정보	RWM
			P5	처방전	RWM
			P6	환자건강정보	RWM
User6	R6	밤진료간호원	P8	진단처리정보	RWM
			P9	응급진료정보	R
User7	R7	낮진료간호원	P8	진단처리정보	RWM
User8	R8	원무담당자	P10	보험정보	RWM
User9	R9	진료보조	P12	기초환자정보	RWM
User10	R10	간호보조	P13	진단처리정보	R
			P12	기초환자정보	RWM
			P14	접수등록정보	RWM
			P21	수납정보	RWM
User11	R11	원무보조	P15	환자건강정보	D
			P20	진단정보	D
User12	R12	환자	P16	기초환자정보	R
			P17	진단정보	R
			P11	환자건강정보	R
			P18	보험정보	R
			P19	처방전	R

(R : 읽기 W : 쓰기 M : 수정)

표 9 모바일 헬스 케어 시스템의 부역할 예
Table 9. For example sub role of mobile healthcare system

PAR (Permission regular role assignment)		PAFB (Permission fixed delegatable role assignment)	
RR	Permissions	FDBR	Permissions
R1	P1	R1′	
R2	P2	R2′	
R3	P3	R3′	
R4	P4,P5,P7	R4′	P6
R5	P4,P5	R5′	P6
R6	P8	R6′	
R7	P8	R7′	
R8	P10	R8′	
R9	P12	R9′	
R10	P12,P14	R10′	P13,P21
R11	P15	R11′	P20
R12	P16,P17	R12′	P11,P18,P19

PATB (Permission temporal delegatable role assigement)		PAD (Permission delegation role assignment)	
TDBR	Permissions	DTR	Permissions
R1″		D1	P12
R2″			P13
R3″			P20
R4″			
R5″			
R6″	P9		
R7″			
R8″			
R9″			
R10″			
R11″			
R12″	D1		

위에서 보여준 〈표 7과 8〉을 통하여 User1부터 User12까지의 사용자는 권한을 할당 받았다. 그러나 사용자는 권한을 할당 받았다고 하여 모두 사용할 수 있는 것이 아니다. (그림 1)에서 보여주는 바와 같이 제약 조건을 만족하여야만 권한이 활성화되어 사용 할 수 있다.

본 논문에서 제안한 사용자 역할 할당 제약 조건과 권한 역할 할당 제약 조건의 예는 〈표 10〉, 〈표 11〉과 같다.

표 10 모바일 헬스 케어 시스템의 사용자 역할 할당 제약 조건의 예
Table 10. For example user role assignment constraint of mobile healthcare system

	역할	
정적의무분리(SSD)	밤 진료의사	낮 진료의사
동적의무분리(DSD)	밤 진료간호원	낮 진료간호원

표 11 모바일 헬스 케어 시스템의 권한 역할 할당 제약 조건의 예
Table 11. For example permission role assignment constraint of mobile healthcare system

DP	접수등록 RWM	수납정보 RWM	
D_CP	환자건강정보 R	환자건강정보 D	
I_CP	진단정보 R	진단정보 D	
DI_CP	진단정보 R	진단정보 D	진단정보 R
DTR_CP	진단정보 R	진단정보 D	
PP	환자건강정보 RWM, AND, 기초 환자정보 RWM	처방전 RWM, OR, 진단정보 R, 환자건강정보 R	
PASR	응급진료정보 RWM	응급진료정보 R	

〈표 10〉은 모바일 헬스 케어 시스템의 사용자 역할 할당 제약 조건의 예로 밤 진료의사와 낮 진료 의사는 서로 정적 의무분리의 제약 조건을 가지고 있다. 이는 밤 진료의사의 역할과 낮 진료의사의 역할은 한 사용자에게 할당 될 수 없음을 보여준다. 또한 밤 진료 간호원과 낮 진료 간호원은 서로 동적 의무분리의 제약 조건을 가지고 있다. 이는 밤 진료 간호원의 역할과 낮 진료 간호원의 역할은 한 사용자에게 할당 될 수 있으나 한 세션 상에서 동시에 사용될 수는 없음을 보여준다.

〈표 11〉은 모바일 헬스 케어 시스템의 권한 역할 할당 제약 조건의 예를 보여준다. 접수등록 읽기 쓰기 수정하기 허가와 수납정보 읽기 쓰기 수정하기 허가는 DP 제약조건을 가지므로 한 역할에 할당 되지 못한다.

D_CP 제약조건의 예로 원무 담당자의 허가인 환자 건강정보 읽기를 이는 원무 보조 역할에게 위임 된다. 이때 원무 보조 역할은 환자 건강정보 부인의 허가를 가지고 있으므로 이는 위임으로 인한 충돌이 발생하게 된다. 이러한 권한 할당의 오류를 줄이고자 권한 정책에 의한 우선순위를 살펴보게 되며 헬스케어의 특성상 사용자의 프라이버시 보호를 위하여 긍정적인 허가보다는 부정적인 허가가 우선하게 된다. 따라서 원무 보조 역할을 가진 사용자는 환자 건강 정보에 대한 부인 권한을 할당 받게 된다.

I_CP 제약조건의 예로 환자는 진단정보에 대한 읽기 허가를 가지고 있다. 이 허가는 역할 계층상 원무 보조 역할에게 상속이 이루어지며 이때 원무 보조 역할은 진단정보에 대한 부인 허가를 가지고 있으므로 상속에 의한 충돌이 발생하게 되며 D_CP와 같이 우선순위를 살펴서 권한을 부여받게 된다. DI_CP 제약 조건의 예로 원무 보조는 원무 담당자로부터 진단정보 읽기 허가를 위임받게 되고 환자로부터 진단정보 읽기 부인 허가를 상속받게 된다. 이는 역할 계층상에서 위임과 상속으로 인한 충돌을 발생하게 되며 이러한 권한 할당의 오류를 줄이고자 우선순위를 살펴서 권한을 부여 받게 된다.

DTR_CP 제약 조건의 예로는 〈표 9〉에서 설명한 봐와 같이 역할 D1을 환자의 임시 역할로 위임함으로써 환자는 자신이 가지고 있던 진단정보 읽기 허가와 D1의 진단정보 부인 허가를 모두 가지게 됨으로써 두 허가는 충돌을 발생시킨다. 위와 같이 권한 할당의 오류를 줄이고자 우선순위를 살펴보아 부정적인 허가를 우선하여 환자는 진단정보에 대한 부인 허가를 지니게 된다.

PP 제약 조건의 AND의 예로 환자 건강정보에 대한 읽기 쓰기 수정하기의 권한을 가진 역할은 기초 환자 정보에 대한 읽기 쓰기 수정하기의 권한을 모두 포함하고 있어야 한며 OR의 예로 처방전에 대한 읽기 쓰기 수정하기 권한을 가진 역할은 진단정보 읽기, 환자 건강정보 읽기 두 가지 권한 중 한 가지 권한을 포함하고 있어야 한다.

PASR 제약조건은 업무 특성상 또는 보안 관리상의 이유로 특정 권한을 한 역할에만 할당해야 함으로 응급 진료정보에 대한 읽기 쓰기 수정하기의 허가는 밤 진료 의사에게만 할당되어야 하며 응급 진료정보에 대한 읽기 허가는 밤 진료 간호원에게만 할당되어야 한다는 제약이다.

위와 같이 사용자 역할 할당 제약 조건과 권한 역할 할당 제약 조건을 통하여 사용자에게 할당된 역할은 모바일 환경의 특성상 상황정보 제약 조건을 적용시켜야 한다. 다음 〈표 12〉는 상황 정보 제약 조건의 예를 보여준다.

표 12 상황정보 제약조건의 예
Table 12. For example context constraint

Subject	Object	Authorization type	Operation	Place	Time	Patient	System Information	Priority
밤진료의사	응급진료 정보	+	RWM	응급실	(-∞, ∞)		High/Low	High
밤진료간호원	응급진료 정보	*	R	응급실	(18, 06)		High/Low	High
환자	진단정보	-	R	암병동		암환자		

예를 들어 밤 진료의사는 응급진료 정보에 대한 읽고 쓰고 수정하는 권한을 가지고 있다. 그러나 모바일 헬스 케어 환경에서 상황 정보 수집기의 시스템 정보가 높을 때 권한은 응급진료 정보에 대한 읽기 권한 만으로 축소 될 수 있다. 응급상황을 경우 헬스 케어는 환자의 생명을 다루는 분야이기 때문에 환자는 심각한 상황에 빠질 수 있다. 따라서 다음과 같은 상황정보 제약 조건을 줌으로써 밤 진료 의사는 응급실에서 24시간 시스템 정보와 상관없이 높은 우선순위를 가짐으로 권한의 축소가 이루어 지지 않는다. 또 다른 예로 밤 진료 간호원은 응급진료 정보에 대한 읽기 권한을 시스템 정보와 상관없이 밤 6시부터 아침 6시까지 다른 사용자에게 위임 할 수 있다.

암환자에게 자신의 진단 정보는 충격을 가져올 수 있다. 따라서 그 충격을 방지하기 위하여 암병동에서 암환자에게만 환자의 진단정보의 읽기 권한을 부인 할 수 있다. 이는 위의 〈표 12〉와 같이 나타낼 수 있으며 이를 통하여 환자의 진단정보 읽기 권한은 부정적인 허가를 갖는다.

위 예제를 통하여 사용자는 역할들을 할당 받을 수 있으며 이를 통해 모바일 헬스 케어 환경에서의 접근제어가 가능하다. 그러나 각 사용자가 할당된 허가들은 상황정보와 동적의무분리 제약에 의하여 활성화가 될 수도 있고 되지 못 할 수도 있다. 즉, 상황정보 수집기에 의하여 수집된 시스템 정보와 사용자가 접속한 시간, 사용자가 접속한 장소 등에 따라서 사용자의 활성화되는 권한이 달라질 수 있다. 이를 통하여 모바일 헬스 케어 시스템에서 사용자는 좀 더 유동성 있는 접근제어 서비스를 제공 받을 수 있으며 부정적인 허가의 개념을 통하여 환자의 사생활 보호와 관련된 윤리적인 문제까지 해결 할 수 있다.

V. 결론

본 논문은 모바일 헬스 케어 정보 시스템을 위한 역할기반 접근제어 모델을 제안하였다. 제안된 모델은 모바일 헬스 케어 정보 시스템의 특징을 고려하기 위하여 전통적인 역할 기반 접근제어에 상황정보 기반의 접근제어를 고려하였다. 또한 환자의 프라이버시를 보호하기 위한 부정적인 허가와 사용자의 유동성 있는 접근을 위한 역할 대 역할 위임, 부분적인 위임의 개념을 통합하여 모델링 하였다. 또한 모바일 헬스 케어 정보 시스템에서 좀 더 유동성 있고 세밀한 접근제어를 가능하게 하기 위하여 사용자 역할 할당 제약 조건과 허가 역할 할당 제약 조건을 제시하였다. 앞으로는 유비쿼터스 환경에서 모바일 사용자에 대한 헬스 케어 정보시스템 접근제어에 대한 연구가 수행되어야 할 것으로 사료된다.

참고문헌

[1] C.P.Pfleeger, Security in Computing, second edition, Prentice-Hall International Inc, 1997.

[2] R.S.Sandhu and E.J.Coyne and H.L.Feinstein and C.E.Youman "Role-Based Access control Method", IEEE Computer, vol. 29, 1996.

[3] D.Ferraiom and J.Cugini and R.Kuhm "Role-based Access Control(RBAC) : Features and motivations", Proc. of 11th Annual Computer Security Application Conference, 1995.

[4] Marc Wilikens, Simone Feriti, Marcelo Masera, A Context-Related Authorization and Access Control Method Based on RBAC, ACM Symposium on Access Control Models an d Technologies(SACMAT 2002), pp.117-124, June, 2002

[5] Michael J. Covington, Wende Long, Srividhya Srinivasan, Securing Context-Aware Applications Using Environment Roles, Symposium on Access Control Models and Technologies (SACMAT 2001), pp.10-20, May, 2001

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

[7] 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

[8] Chang-Joo Moon, Dae-Ha Park, Soung-Jin Park, Doo-Kwon Baik, "Symmetric RBAC model that takes the separation of duty and role hierarchies into consideration", Computer&security, pp.126-136, 2004

[9] Xinwen Zhang, Sejong Oh, and Ravi Sandhu, PBDM: A Flexible Delegation Model in RBAC, Proc. 8th ACM Symposium on Access Control Models and Technologies (SACMAT 2003), pp.149-157, June, 2003.

[10] D.Ferraiolo, R.Sandhu, S.Gavrila, D.Kuhn, R.Chandramouli, Proposed NIST standard for role-based access control. ACM Transactions on information and System Security (TISSEC), 4(3):224-274, 2001.

[11] Guangsen Zhang, Manish Parashar, Context -aware Dynamic Access Control for pervasive applications, IEEE International Conference, Fourth International Workshop on Grid Computing, pp.101-108, November, 2003

[12] Salem BENFERHAT, Rania EL BAIDA, Frederic CUPPENS, A Stratification based approach for handling conflicts in Access Control, Symposium on Access Control Models and Technologies (SACMAT 2003), pp.189-195, June, 2003

[13] Mark Evered, serge Bogeholz, "A case study in access control requirements for a health information system, australian Information security workshop 2004 (AISW 2004), 2004

[14] 이유리, 박동규, "헬스 케어 정보 시스템에서의 동적 문맥 기반 접근제어", 순천향 산업기술 연구소 논문집 2004, 제10권 제2호 ,pp.235-241, 2004

[15] 이유리, 박동규, "헬스 케어 정보 시스템의 특성을 고려한 새로운 역할기반 접근제어 모델", 한국 정보 기술 학회 논문집 2004, 제2권 제 2호, pp.47-54, 2004

[16] 박동규, 황유동, 안현수, "SECOS의 접근제어를 위한 RBAC의 구현", 한국컴퓨터정보학회논문지, 2002,1, 7권 2호, pp.9-18

[17] 김강, 박진섭, "정보시스템 보안을 위한 위험분석 모델", 한국컴퓨터정보학회논문지, 2002,9 7권3호, pp.60-67

저자소개

이 유 리

2002년 2월 : 순천향대학교 정보통신공학과 공학학사

2004년 2월 : 순천향대학교 정보통신공학과 공학석사

2004년~현재 : 순천향대학교 정보통신공학과 박사과정

〈관심분야〉 접근제어, 보안

박 동 규

1992년 한양대학교대학원 전자 공학과 공학박사

1999년~2003년 순천향대학교 정보기술공학부 부교수

2004년~현재 순천향대학교 정보기술공학부 교수

〈관심분야〉 접근제어, 보안