논문 2009-5-32

상황제한 RBAC 모델을 이용한 U-헬스케어 접근권한 제어모델 설계

Design of U-Healthcare Access Authority Control Model Using Context Constrain RBAC Model

김창복*, 김남일*, 박승환**

Chang-Bok Kim, Nam-Il Kim, Seong-Hwan Park

요 약 의료정보는 환자의 프라이버시 침해 뿐 아니라 환자의 생명에도 직결되기 때문에, 견고하고 유연한 보안모델에 대한 지속적인 연구가 필요하다. 특히, u-헬스케어 환경은 사용자 상황변화가 다양하기 때문에, 보다 더 유연하고 세밀한 접근 권한제어가 필요하다.

본 논문은 u-헬스케어 영역에서 상황타입(Context Type)과 상황제한(Context Constraint)을 정의하고, 의료정보의 비밀등급, 사용자의 권한등급, 사용자의 역할, 사용자 상황에 따른 권한 변경 등을 정의하였다. 또한, 사용자 역할을 기반하여 상황정보 변화에 적용할 수 있는 상황기반 접근제어 모델을 설계하였다. 상황기반 접근제어 모델은 K2BASE를 이용하여 자원과 권한의 관계성과 접근 포인트로 부터 도달 가능한 모든 자원에 대한 권한을 분석하였다. 상황기반 접근제어 모델은 u-헬스케어 영역에서 상황을 기반으로 권한변경과 역할을 유연하게 변경할 수 있고, 권한이 부여된 자원에 의미적으로 연결된 자원을 획득할 수 있어, 상황변화가 다양한 u-헬스케어 영역에서 유연하고 적응적인 접근제어 모델로서 적용 가능할 것이다.

Abstract The security of medical information need continued research about steady and flexible security model because of privacy of patient's as well as directly relation in the patient's life. In particular, u-healthcare environment is need flexible and detailed access control by variety changes of context. Control model analyzed relation of resource and authority, and analyzed authority about all accessible resource from access point using K2BASE. The context-based access control model can change flexibly authority change and role, and can obtain resource of authority granted and meaningly connected resource. As a result, this thesis can apply flexible and adaptive access control model at u-healthcare domain which context change various.

Key Words : u-Healthcare, Role based Access Control, Context-Based Role Model, Access Point

I. 서 론

유비쿼터스(ubiquitous) 환경은 분산 정보처리, 다양한 이기종 단말기, 불규칙한 접근, 사용자 상황변화 등으로 정보처리 및 서비스 환경이 동적으로 변하기 때문에, 정보의 기밀성, 무결성 등 정보보안에 다양한 문제를 초래할 수 있다. 따라서 유연한 정보접근과 보안이라는 상반되는 요구사항을 만족시킬 수 있는 적합한 보안모델이 필요하다.[1][2]

유비쿼터스는 의료환경 패러다임의 변화로 이어져 u-헬스케어(u-Healthcare)라는 새로운 의료서비스 환경으로 변화되고 있다. u-헬스케어에 의해 모든 의료장비는 필요한 정보를 독립적으로 실시간에 제공할 수 있는 환

*정회원, 가천의과학대학교 IT학과
**정회원, 을지대학교 의료공학과
접수일자 2009.9.5, 수정일자 2009.10.6

경, 모든 의료진과 환자는 온라인 환경에서 의료정보를 제공받을 수 있는 환경, 환자의 모든 의료정보를 의료기관 간에 공유할 수 있는 환경으로의 변화가 이루어지고 있다. 즉, u-헬스케어를 통하여 의료 환경은 병원 중심의 진료라는 공간적 제약을 넘어, 생활과 진료공간을 자연스럽게 결합시켜 일상 속에서 보편적으로 자리를 잡을 것이다.[3] u-헬스케어에서 의료정보는 환자의 프라이버시 침해와 같은 윤리적 문제뿐아니라 환자의 생명에도 직결되기 때문에, u-헬스케어 패러다임에서 정보 보안은 매우 중요한 과제이다. 최근 생체인식 기반 사용자 인증과 PKI기반의 전자서명 기법은 수년간의 연구개발로 많은 발전이 이루어지고 있으나, u-헬스케어 환경에 적합한 의료정보 서비스를 위해서는 사용자와 환자의 환경과 상황(Context)에 따른 접근 권한제어가 필요하다.

본 논문은 u-헬스케어 환경에 적합한 최적의 보안모델을 설계고자 하였다. 이를 위해 본 논문은 u-헬스케어 영역에서 상황타입(Context Type)을 정의하고, 발생할 수 있는 모든 상황을 상황제한(Context Constraint)으로 정의하였으며, 의료정보에 대한 비밀등급, 사용자의 권한등급, 사용자의 역할, 사용자 상황에 따른 접근포인트의 변경 등을 정의하였다. 또한, 사용자 역할을 기반하여 상황정보 변화에 적용할 수 있는 상황기반 접근제어 모델(Context-Based Access Control Model)을 설계하였다. 최종적으로 K2BASE를 이용하여 접근제어 모델 내에서 자원과 권한 간 관계성을 검사하고, 접근 포인트로 부터 도달 가능한 모든 자원에 대한 권한 탐색하여 본 논문에서 제안한 접근제어 모델의 타당성을 입증하였다.

II. 관련연구

2.1 역할기반 접근제어

역할기반 접근제어(RBAC : Role Based Access Control)는 사용자의 조직 내 역할을 이용한 접근제어 방식으로, 임의적 접근제어와 강제적 접근제어에 비하여 높은 정교함과 유연성을 제공한다. RBAC는 시스템 자원에 대한 권한부여를 사용자 ID나 정의된 규칙에 의해 판단하지 않고, 사용자가 소속된 조직 내에서의 역할에 의해 결정하는 특징을 가지고 있다. 따라서 역할과 객체간의 관계로 접근권한을 관리함으로써, 사용자와 객체의 수가 대단히 많은 분산기업 환경에 적합한 특성을 제공한다.[4] RBAC는 다음과 같이 네 가지 모델로 구분된다.[5-7]

① RBAC0 : 사용자, 역할, 접근권한, 세션 등으로 구성된 가장 기본적인 모델이다.

② RBAC1 : RBAC0에 역할계층(Role Hierarchy) 개념을 포함한 모델로서, 권한과 책임을 수반하는 계층적인 역할구조를 정의한다. 상위역할은 자신의 접근권한 이외에 하위역할의 접근권한을 상속하며, 하위계층에서 상위계층에 상속의 범위를 제한할 수 있다.

③ RBAC2 : RBAC0에 제약(Constraint)조건을 이용하여, 역할의 범위를 축소한다. 기본적인 역할접근제어에 다양한 상황과 환경에 따른 접근제어를 가능하게 한다.

④ RBAC3 : 계층구조 기반의 RBAC1과 제한상황을 포함한 RBAC2를 병합한 형태의 역할기반 접근제어이다.

RBAC모델에서 사용자(User)는 정보를 사용하는 주체이다. 역할(Role)은 주체에 대한 조직 내의 역할을 나타내며, 고유의 권한과 의무를 갖는다. 한 사용자는 다수의 역할이 주어진다. 또한, 하나의 역할은 다수의 사용자와 관계가 있다. 접근권한(Permission)은 접근권한은 접근하고자 하는 객체에 대해 수행 가능한 접근모드들의 집합으로 구성된다. 세션(Session)은 시스템의 로그인을 통해 사용자가 수행하는 작업에 대한 역할의 활성화 상태이다. 이때 각 세션은 하나의 사용자와 여러 개의 권한을 매칭한다. 사용자-역할(UA)관계는 사용자가 여러 역할을 가질 수 있고 동일 역할에 다수의 사용자가 할당될 수 있는 관계이며, 역할-접근권한(PA)관계에서 역할은 다수의 접근권한이 부여될 수 있고, 동일 접근권한에 여러 역할이 할당될 수 있는 관계이다.

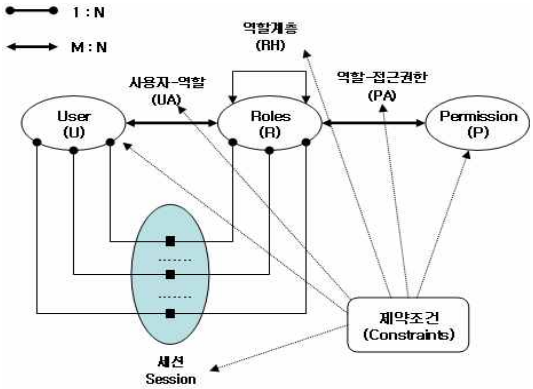

그림 1. 역할기반 접근제어
Fig 1. Role Based Access Control

2.2 상황인식 접근제어 모델

유비쿼터스는 위치와 시간의 제약을 받지 않고 원하는 정보 서비스를 제공 받을 수 있지만, 이것은 정보의 기밀성, 무결성 등 정보보안에 다양한 문제를 초래할 수 있다. 따라서 유연한 정보접근과 보안이라는 상반되는 요구사항을 만족할 수 있는 보안모델이 필요하다. 유비쿼터스 환경은 정보처리 및 서비스 환경이 동적으로 변하기 때문에, 동일한 사용자 또는 역할이라 할지라도 접근권한이 변경될 수 있다. 즉, 접근권한이 없는 역할도 상황에 따라 접근권한이 부여될 수 있으며, 접근권한이 있는 역할도 접근권한이 제한될 수 있다. 따라서 기존의 RBAC 권한모델 뿐 아니라 사용자의 상황에 따라 필요로 하는 정보에 대한 권한제어가 필요하다.[6-8] 전통적인 RBAC모델에 상황의 개념을 포함한 모델은 일반화 역할기반 접근제어모델과 상황제한 역할기반 접근제어 모델이 있다.

일반화 역할기반 접근제어(GRBAC : Generalize RBAC) 모델은 기본적인 RBAC모델에 상황정보를 추가한 방법으로, 접근권한을 위해서 주체(Subject), 객체(Object), 환경(Environment), 연산(Operation), 부호(Sign) 등 5-튜플(tuple)로 표현함으로써, 접근제어 정책 기술의 단순함과 융통성을 제공한다.[8,9] 여기서 주체는 사용자, 객체는 접근하고자 하는 자원, 환경은 주체의 상황, 연산은 자원에 대한 접근모드를 나타낸다. 예를 들어 전공의 역할을 할당 받은 사용자는 주말에 처방전을 읽을 수 없음에 대한 표현은 다음과 같다.

(<전공의, 처방전, 주말, 읽기>, −)

GRBAC모델은 부호에 따라 "positive, negative, mixed" 권한 등을 사용한다. positive 권한은 허용권한만이 정책에 기술되며, negative 권한은 거부권한만이 정책에 기술되고, mixed 권한은 두 가지를 혼합하여 정책을 기술하는 모델이다.

상황제한 역할기반 접근제어(xoRBAC)모델은 기존의 RBAC에 상황정보를 접근제어 결정에 이용하기 위하여 상황제한을 사용하는 방법이다. 상황제한은 실시간 상황정보의 실제 값과 접근제어 정책의 상황을 비교하여, 사용자 및 역할에 대한 접근제어를 위해 사용된다. 상황제한은 상황타입, 함수, 조건 값 등 3-튜플을 갖는다. 상황타입은 시간, 요일, 위치, 혈압 등과 같은 동적속성과 역할, 소유관계, 생일, 국적과 같이 정적속성이 있다. 일반적으로 정적속성은 사용자 인터페이스로 입력하여 데이터베이스에 저장된 내용을 참조하며, 동적속성은 위치, 생체, 조도센서 등 다양한 센서를 통해 센싱된다.

상황제한 역할기반 접근제어 모델은 각 객체의 접근권한에 대해서 접근제어 정책을 상황제한으로 기술하여, 사용자의 접근요청시 제한조건이 모두 참 값을 가질 때 허용 또는 거부된다.[10] 따라서 각 객체의 권한에 대하여 상황제한이 기술되므로 사용자의 상황에 따른 접근제어를 수행하고자 할 때 최악의 경우 제한상황은 다음과 같은 경우의 수가 필요할 수 있다.

$$\text{상황제한} = \text{역할수} * 2^{\text{상황수}}$$

이것은 사용자의 접근요청이 발생하였을 때 권한을 부여하기 위하여 상황 정보제약의 탐색과 평가시간을 길게 하는 문제를 발생시킨다.

2.3 상황인식 접근제어 모델

(1) ISO/IEC 10181-3 접근제어 모델

전통적인 접근제어 프레임웍은 ISO/IEC 10181-3에 의해 제공되며, 파일, 데이터베이스, 프로그램, 기업자원 등의 접근제어에서 적용되고 있다. ISO/IEC 프레임웍은 정보요구자(Initiator), 타겟(Target), AEF(Access Control Enforcement Function), ADF(Access Control Decision Function) 등의 컴포넌트로 구성되어 있다. 그림 2.14에 ISO/IEC 10181-3 접근제어 프레임웍에 대해서 나타냈다.[11] 정보요구자는 사용자 또는 역할로서 정보를 요구하는 주체이다. 타겟은 정보요구자가 접근을 시도하는 객체이며, 파일, 데이터베이스, 프로그램 또는 다양한 기업자원일 수 있다. AEF는 사용자의 접근요구에 대한 접근권한 결정을 ADF에 요구하며, ADF에 의해 접근권한 결정을 응답받아 타겟에 대해 접근권한을 실행하는 컴포넌트이다. ADF는 사용자의 자원 접근요구에 대해 정책결정 정보를 통해 정책을 결정하는 컴포넌트이다.

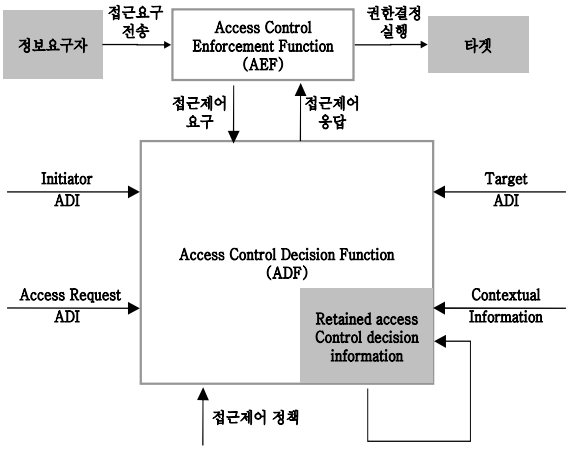

그림 2. ISO/IEC 10181-3 접근제어 프레임웍
Fig 2. ISO/IEC 10181-3 Access Control Framework

ISO/IEC 10181-3 접근제어 프레임웍의 접근제어 방법은 다음과 같다.

단계 1 : 정보요구자는 AEF에게 타겟 자원에 대한 접근 권한을 요청
단계 2 : AEF는 ADF에 접근권한 결정을 요청
단계 3 : ADF는 접근권한 요구메시지를 기준으로 정책결정에 필요한 속성 및 상황정보를 부가하여 접근 제어 메시지를 결정한다.
단계 4 : ADF는 접근제어 메시지와 접근제어 정책이 저장되어 있는 저장소를 비교하여 자원에 대한 접근 권한을 결정한다.
단계 5 : ADF는 접근권한 결정을 AEF에 전송한다.
단계 6 : AEF는 정책결과를 타겟에 실행

정보요구자 속성에 대한 속성정보는 Initiator ADI를 통해 추출할 수 있으며, 접근제어 ID, 그룹 ID, 역할 ID 등이다. 타겟에 대한 속성정보는 Target ADI를 통해 추출되며, 타겟 ID, 타겟 위치 등이다. 타겟에 대한 접근모드는 Access Request ADI를 통해 추출되며, 자원에 대한 읽기, 쓰기 등과 무결성 레벨, 데이터 타입 등이다. 또한, 그림 2에서 ISO/IEC 10181-3 접근제어 프레임웍은 자원에 대한 접근제어에 있어 상황 정보의 개념을 사용하였음을 알 수 있다.

(2) CAAC 상황인식 접근제어 모델

CAAC(Context-Aware Access Control) 상황인식 접근제어 모델은 사용자의 역할과 상황정보를 이용하여 접근권한을 결정하는 시스템이다.[11] CAAC시스템에서 상황형태(CT : Context Type)는 상황정보를 정의하기 위해 상황제한의 요소로 사용한다. CAAC는 기본적으로 정의된 CT를 CTp라 정의하며, 5개의 CTp= {Time, Location, ID, ObjID, Trust}가 정의된다. 여기서 Time은 접근요구 시간, Location은 접근요구 장소, ID는 접근요구 사용자, ObjID는 접근 요구 객체, Trust는 인증레벨 등급으로 정의한다.

상황제한(CC : Context Constraint)은 CT를 이용하여 상황정보를 규칙적인 형식으로 정의한 것이다. 상황제한은 다음과 같이 서술된다.

$$CC := CL1 \cup CL2 \cup \cdots \cup CLi$$
$$CL := CN1 \cap CN2 \cdots \cap CNi$$
$$CN := \langle CT \rangle \langle OP \rangle \langle VALUE \rangle$$

CC는 상황제한이며, CL은 상황정보 요소이다. 또한, CN은 상황타입에 대한 현재 상황조건의 표현이다. 여기서, CT는 상황타입이며, OP는 논리연산자로서 추가 확장할 수 있으며, VALUE는 CT의 값이다.

권한정책(AP : Authorization Policy)은 사용자 또는 역할에 대해서 특정 자원에 대한 사용권한을 제공하는 정책이다. 권한정책은 3-튜플로 나뉜다.

$$AP = (S, P, C)$$

S(Subject)는 정책의 주체로서 사용자 또는 역할이며, P(Permission)는 <M, O>로 표현되며, 접근모드와 접근객체를 나타낸다. M(Mode)은 접근모드이며 O(Object)는 접근하고자 하는 객체를 의미한다. C는 상황제한이며, 모든 조건이 "True"일 경우에 접근이 허용된다. 만약 상황제한이 없다면, 기본적인 RBAC 모델이 된다.

데이터 접근(DA : Data Access)은 사용자가 상황정보를 제공하여, 특정 정보를 접근하려는 시도이며, 다음과 같이 정의한다.

$$Data\ Access = (U, P, RC)$$

U(User)는 데이터 접근을 요구하는 사용자이며, P는 권한정책과 동일하다. RC(Runtime Context)는 CT의 실

제 값으로, 다음과 같이 표현된다.

RC={v1 of CT1, v2 of CT2,… vn of CTn}

위 식에 의해서 현재 상황에 대한 권한정책이 참이며, 사용자의 역할에 대해 접근하고 하는 객체에 접근권한이 부여된다. 그림 3에 CAAC 접근권한에 대해서 나타냈다. CAAC 권한모델은 인증엔진, 권한엔진 및 사용자-역할저장소, 정책 저장소, 상황저장소, 상황서비스 등으로 구분된다.

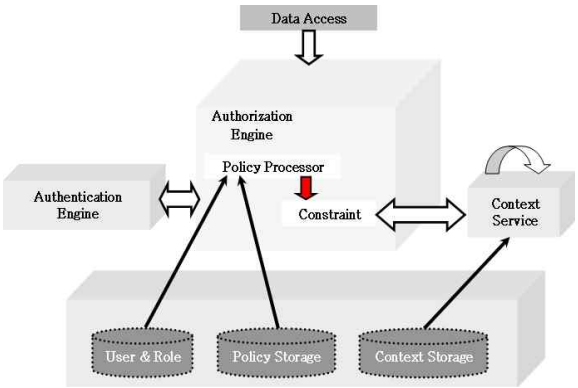

그림 3. CAAC 권한모델
Fig 3. CAAC Authority Model

III. U-헬스케어 상황기반 접근제어 모델 설계

3.1 U-헬스케어 상황인식

u-헬스케어 장비는 환자의 심장 박동수, 혈압, 산소포화도 등 헬스케어정보를 센싱하여, 환자의 헬스정보를 전송한다. 만일 환자의 응급 상황에서 주치의가 없거나 심지어 환자가 병원 내에 없을 경우에는 환자의 생명에 심각한 위협을 초래한다. 이와 같은 응급상황에서는 주치의가 없더라도 의사역할을 보유한 사람에게 환자의 의료정보에 대한 접근권한을 제공해야 할 것이다. 즉, u-헬스케어에서 환자의 상태, 사용자역할, 사용자와 환자와의 거리 등 상황정보 인식하여, 상황에 따라 접근권한을 변경해야 한다. 본 논문은 상황정보를 표현하기 위해, 다음과 같이 기본적인 상황타입을 정의하였다.

CS = {Role, Location, Time, Distance, Status, Device}

여기서 Role은 사용자 역할, Location은 사용자 위치, Time은 의료정보 접근시간, Distance는 환자와의 거리, Status는 환자의 상태, Device사용자 단말기 형태이다. 이러한 상황타입은 상황에 따라 추가 변경될 수 있다. u-헬스케어의 상황은 상황제한을 이용하여 표현할 수 있다. 다음은 환자의 정상상태와 응급상태에서 환자의 의료정보를 읽을 수 있는 두 가지 상황에 대한 상황제한에 대해서 나타냈다.

- CC1 := "Role >= Physician" ∩ "Distance <= 500m" ∩ "Status = Emergency"
- CC2 := ("Role = Healthcare Staff" ∩ "Time>=8:00 ∩ Time<=17:00" ∩ "Location = Hospital" ∩ "Status = Normal") ∪ ("Role = Attending Physician" ∩ "Status = Normal")

CC1은 의사 역할을 가진 사용자가 환자와 500m이내의 인접거리에 있으며, 환자가 응급상태에 있다는 것을 표현한다. 또한, 상황제한 CC2는 헬스케어 의료진 역할을 가진 사용자가 근무시간 내 그리고 병원 내에 있고 환자가 정상상태 또는 사용자의 역할이 주치의이며 환자가 정상상태인 경우를 표현한다.

3.2 U-헬스케어 접근제어 모델 설계

U-헬스케어에서 발생할 수 있는 환자정보를 중요도에 따라 비밀등급(security level)을 4단계로 나누었으며, 필요에 따라 좀 더 많은 등급으로 분류할 수 있다. 권한등급은 사용자의 역할에 따라 분류하며, 권한등급에 따라 접근할 수 있는 비밀등급이 다르다.

환자의 Top Secret는 기존 또는 현재의 병력 중 환자의 민감한 프라이버시 정보로서, 정보가 노출되었을 때 심각한 프라이버시 침해가 가능한 환자정보이며, 심지어 생명에도 위협 받을 수 있는 극히 개인적인 정보이다. Secret는 주치의 뿐 아니라 일반적인 의사 역할을 가진 사용자가 접근할 수 있는 정보이다. 이 또한 정보가 노출되었을 때 프라이버시 침해가 가능한 정보이다. Confidential은 환자의 진료 및 치료에 있어, 필요한 처방

에 관련된 정보들로서, 간호사 역할, 약사 역할, 방사선 및 CT촬영과 같은 역할을 가진 사용자가 접근할 수 있는 정보이다. Unclassified는 환자의 일반적인 정보로서 병원 내에서는 누구나 접근할 수 있는 환자의 공개된 대외비 정보이다. 표 1에 나타난 환자정보에 대한 권한등급 및 역할의 일반적인 예는 각 역할의 중요도에 따라 상향 또는 하향 조정될 수 있다.

표 1. 의료정보에 대한 권한등급 및 역할
Table 1. Authority and Role of Medical Information

권한등급	비밀등급	역 할
등급 1	Top Secret	주치의
등급 2	Secret	전임의, 전공의, 타 진료과 전임의
등급 3	Confidential	간호사, 약사, 보건직
등급 4	Unclassified	간호조무사, 의료보조원, 간병인

u-헬스케어 상황기반 접근제어 모델(Access Control Model)은 크립키(Kripke) 구조의 계층적 모델 정의방법으로, 역할 및 업무절차 뿐 아니라, 상황에 따라 역할과 권한을 변경할 수 있으며, 접근된 환자정보와 의미적으로 연결된 모든 환자정보를 접근할 수 있도록 설계한 접근제어 모델이다. 특히, 상황기반 접근제어 모델의 구조는 상위 역할의 권한을 가진 사용자라 할지라도, 하위 역할의 모든 자원을 사용할 수 없으며, 하위 역할의 사용자라 할지라도 상위 역할의 자원을 사용할 수 있도록 설계하였다. 그림 4에 본 논문에서 정의한 상황기반 접근제어 모델에 대해서 나타냈다. 그림에서 사용자의 접근권한은 p0~p18로 표현하였으며, 자원은 T(Top Secret), S(Secret), C(Confidential) 등 비밀등급에 대한 이니셜을 이용하여 표현하였다. 화살표는 자원의 관계를 나타내며, 화살표로 연결된 모든 자원은 접근이 가능한 자원임을 나타낸다. 또한, 점선으로 나타낸 자원간의 관계는 동일한 자원임을 나타낸다.

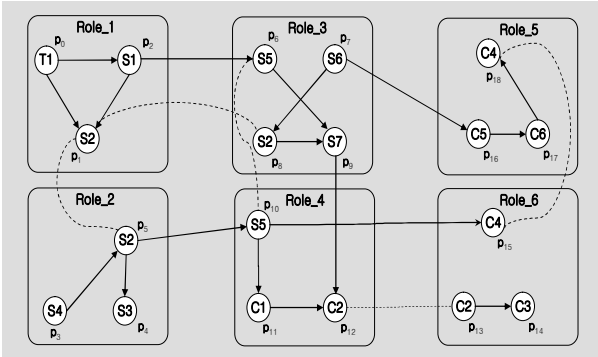

그림 4. 상황기반 접근제어 모델
Fig 4. Context-Based Access Control Model

p0~p18은 사용자의 권한으로서, 동일한 역할 그룹 내에서 상황에 따라 다양한 권한에 매핑 할 수 있다. 상황기반 접근제어 모델은 권한 등급이 높은 역할이 권한 등급이 낮은 자원을 접근할 수 없는 경우도 발생하며, 권한 등급이 낮은 역할이 상황에 따라 상위등급의 자원을 접근할 수 있다. 즉 권한매핑에 대한 문제는 사용자들의 상황정보에 따라 변경되기 때문에, 모든 환자 정보의 접근 권한은 상황에 따라 매핑 할 수 있는 가능성은 충분히 제공되고 있다.

표 2. 상황에 따른 접근 포인트
Table 2. Access Point about Context

사용자	위치	시간	환자상태	거리	장비	접근포인트
주치의	Public	≠WT	Stability	FAR	Mobile	p1
간호사	Public	X	Emerg3	Near	X	p0
관련의사	Public	X	Emerg2	near	X	p0
의사	Hospital	WT	Emerg2	Near	X	p2
간호사	Hospital	WT	X	Near	X	p13
간호사	Hospital	WT	X	X	PC	p14
간호사	X	≠WT	Stability	X	X	p16

표 2에 사용자 역할과 상황에 따른 접근포인트의 변경에 대해서 정의하였다. 이러한 u-헬스케어에 대한 상황타입과 상황정보는 더욱 확장할 수 있다.

IV. 모델분석 및 평가

4.1 시뮬레이션

본 논문의 u-헬스케어 상황기반 접근제어 모델은 환

자의 상태에 따라 유연하게 환자정보의 접근권한을 제어할 수 있도록 설계하였다. 즉, 크립키(Kripke) 구조의 계층적 모델 정의방법으로, 역할 및 업무절차 뿐 아니라, 상황에 따른 역할과 권한을 변경할 수 있으며, 접근된 환자정보와 연결된 모든 환자정보를 접근할 수 있도록 설계하였다. 또한, 도달성 분석 도구인 K2BASE를 이용하여, 모델을 평탄화하여 자원의 도달성과 권한분석을 하였다.

자원에 대한 권한범위를 정형적으로 명세하기 위해, 분기시제 논리인 계산트리논리(CTL)가 이용됐다. CTL 식의 구문은 다음과 같이 정의된다.[12,13]

$$\Phi ::= true \mid x \mid \neg\Phi \mid \Phi 1 \vee \Phi 2 \mid AG\ \Phi \mid A(\Phi 1\ W\ \Phi 2)$$

CTL로 주어진 범위에서, 함수 pre(P)는 역방향 도달성 분석으로 자원들의 집합을 찾는 것에 이용된다.

$$pre\forall(P) = \{x \in X \mid \forall x' \cdot if\ (x,x') \in R\ then\ x' \in P\}$$

이 함수는 상태들의 부분 집합 P를 얻어 P로 전이시키기 위한 상태들의 부분 집합을 반환한다. 즉, P 에서 상태들에 선임자(predecessors)의 집합이다. 어떤 CTL식 에 대해, 가 참인 상태들의 집합을 ||[]||으로 나타낸다. CTL로 주어진 범위에서, 함수 post(P)는 전방향 도달성 분석으로 자원들의 집합을 찾을 수 있다.

$$post\exists(P) = \{x' \in X \mid \exists x \cdot\ x \in P \wedge (x,x') \in R\}$$

K2BASE에 역할그룹 정의, 역할 그룹의 권한 정의, 권한에 대한 자원 정의, 역할 그룹간의 전이 정의, 권한간의 전이 정의 등에 대한 코드를 작성하여 시뮬레이션 하였다. 이 중에서 역할그룹 정의 및 역할 그룹의 권한 정의에 대한 XML 코드는 다음과 같다.

```
<Service name="CBRM" place="s0">
    <Topic name="CBRM" />
    <InnerProcess place="R1" />
    <InnerProcess place="R2" />
    <InnerProcess place="R3" />
    <InnerProcess place="R4" />
    <InnerProcess place="R5" />
      <InnerProcess place="R6" />
</Service>
```

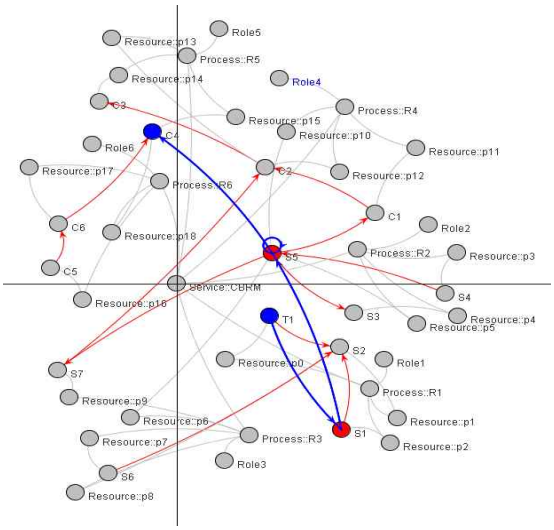

그림 5. K2BASE 시뮬레이션
Fig 5. K2BASE Simulation

그림 5는 상황기반 접근제어 모델을 K2BASE를 이용하여, 자원의 연결성을 검토한 결과이다. 그림 5에서 Process:R1~Process:R5는 사용자의 역할이며, Resource:P0~Resource:P18은 각 역할에 대한 권한이다. 또한, 권한에 연결된 자원들은 자원의 비밀 등급에 따라 T, S, C로 표현하였다.

환자정보인 자원들은 접근할 수 있는 권한을 가진 역할들과 개별적으로 연결되어 있으며, 접근권한이 부여된 자원과 연결된 모든 자원을 접근할 수 있는 권한이 부여된다. 또한, 상황에 따라 접근 포인트의 변경에 따라 권한이 변경되었을 경우 필요한 권한과 접근할 수 있는 자원들을 탐색할 수 있으며, 개별적인 자원에 대해 중복되는 자원 접근을 유연하게 탐색할 수 있다. 예를 들어, 주치의의 권한을 가진 R1은 프라이버시가 가장 높은 환자정보(T1)에 대한 접근 권한을 가지며, 화살표로 연결된 하위 정보들에 대한 권한을 갖고 있다. 또한, 환자정보 S5가 과다한 권한부여 현황을 탐색할 수 있다.

4.2 모델평가

상황기반 접근제어 모델에서 환자의 상황에 따라 권한의 변경되면 접근 포인트가 결정된다. 상황에 따른 접근포인트의 변경은 역할변경으로 간주할 수 있다. 예를 들어, 환자와 관련 없는 의사역할을 가진 사용자가 환자의 응급상황에서 주치의의 권한을 가진 환자의 의료정보

를 접근할 수 있는 권한을 추가적으로 받아야할 것이다. 이를 전제로 본 접근제어 모델은 기존의 사용자에 대한 접근 포인트로 부터 상황변경에 따라 변경된 접근 포인트의 정보자원까지의 도달성을 검사하면 추가로 할당되어야할 권한이 무엇이지를 검색 및 분성을 통해 도출할 수 있다. 이를 통해 정보관리자는 정보에 대한 권한할당을 동적으로 제어할 수 있다.

전통적인 접근제어모델은 하나의 정보에 대해서 권한을 부여하여, 상황에 따른 정책변경을 개별적으로 제어함으로써 많은 정책의 생성과 로딩으로 인한 정책평가에 많은 시간이 소요되었으며, 사용자가 자원의 개별적 접근으로 인한 접근하고자 하는 자원과 연관된 정보들이 무엇인지를 사용자가 직접 인지하여 접근해야하는 어려움이 있었다. 그러나 본 논문의 상황기반 접근제어 모델은 사용자가 접근을 시도하는 특정자원에 대해서 접근권한이 허용된 경우, 접근자원과 의미있는 모든 자원을 접근할 수 있는 방법을 제시한다.

그림 5에서 특정 정보자원에 대한 과다하게 권한이 부여되었음을 알 수 있다. 이를 통해 상황기반 접근제어 모델의 평가 및 정제 방법에 활용될 수 있다. 즉, 특정 권한에 대해 필요 없는 권한 부여 또는 권한을 부여해서는 안되는 역할 등에 대해서 보안 관리자를 통해 권한모델을 정제할 수 있는 방법을 제시한다.

본 시뮬레이션을 통해 상황기반 접근제어 모델에서 자원에 대한 권한부여, 자원과 의미적 연결성, 자원 보호 및 공유 등 다양한 보안정책을 위한 역할모델 정제방법을 제시하였다. 본 논문에서 제안한 상황기반 접근제어 모델에 대한 평가는 다음과 같다.

① u-헬스케어 정보시스템에서 환자의의 응급 상황에 대해서 유연하게 대처할 수 있는 접근제어가 가능하다.
② 접근자원과 의미적으로 관련된 자원들의 접근성을 이용하여 자원접근의 효율성 및 신속성
③ 환자와 사용자의 상황과 역할에 적합한 권한과 자원할당을 위한 유연한 접근제어모델
④ 환자의 상황에 따라 접근 포인트 변경으로 발생되는 역할 및 권한변경 등 상황기반 접근제어가 용이
⑤ 자원에 대한 권한부여, 자원과 자원간의 의미적 연결성, 자원의 보호 및 공유등 동적인 보안정책 가능

V. 결 론

u-헬스케어에서 의료정보는 환자의 프라이버시 침해와 같은 윤리적 문제뿐아니라 환자의 생명에도 직결되기 때문에, u-헬스케어 패러다임에서 정보 보안은 매우 중요한 과제이다.

본 논문은 u-헬스케어 환경에 적합한 최적의 보안모델을 설계하고자 하였다. 이를 위해 본 논문은 u-헬스케어 영역에서 상황타입(Context Type)과 상황제한(Context Constraint)을 정의하고, 의료정보에 대한 비밀등급, 사용자의 권한등급, 사용자의 역할, 사용자 상황에 따른 권한의 변경 등을 정의하였다. 또한, u-헬스케어에서 발생할 수 있는 모든 상황정보를 고려한 권한모델인 상황기반 접근제어 모델을 정의하고, 도달성 분석 도구인 K2BASE에 입력하여, 각 역할에 대한 자원 및 권한간의 관계와 도달경로에 따른 권한 범위 검사를 수행하고, 권한이 부여된 자원 뿐 아니라 사용자 이벤트에 관련된 모든 자원에 대한 접근을 제어하고자 하였다.

본 논문을 통해 첫째, u-헬스케어 정보시스템에서 환자의의 응급 상황에 대해서 유연하게 대처할 수 있는 접근제어가 가능하고, 둘째, 접근권한이 부여된 자원과 의미적으로 관련된 자원들의 접근성을 이용하여, 한 번의 자원 접근으로 관련있는 모든 자원을 접근할 수 있는 방법을 가능하도록 제안하였다. 세 번째, 도달성 시뮬레이션을 통해 u-헬스케어에의 모든 의료정보를 상황에 따라 권한 할당 및 자원의 권한에 대한 정제가 용이하게 되었다.

본 논문에서 제안한 상황기반 접근제어 모델은 유비쿼터스 환경에 적합한 보안모델로서, 보안체계 강화 및 차세대 보안체계에 대한 기반 구축이 가능할 것으로 기대된다. 특히, 동적인 상황변화가 많은 u-헬스케어 분야에서 상황에 따른 체계적인 보안체계를 구축할 수 있는 기반이 제공될 것이다. 또한, 본 모델은 u-헬스케어 영역뿐 아니라 다양한 영역에 적응할 수 있는 모델로 응용될 수 있다. 추후 연구로서, u-헬스케어에서 발생할 수 있는 다양한 상황제한을 온톨로지로 구축하여, 권한할당 접근포인트를 추론할 수 있는 방법에 대한 연구가 필요하다.

참 고 문 헌

[1] Jason I. Hong and James A. Landay, "Support for

location: An architecture for privacy-sensitive ubiquitous computing", Proceedings of the 2nd international conference on Mobile systems, applications, and services MobiSys'04, Boston, MA, USA, pp. 177-189. 2004.

[2] 강달천, "유비쿼터스 컴퓨팅 환경에서의 개인정보 보호", 한국인터넷법학회, 인터넷법 연구, 제 3권 2호, pp. 29-54, 2004.

[3] 김창복, 이상순, 이병수, "상황인식 기반의 적응형 u-헬스케어 보안체계에 대한 연구", 정보기술학회 논문지, 제 6권 4호, pp. 37-46, 2008.

[4] Ravi Sandhu, Venkata Bhamidipati and Qamar Munawer. "The ARBAC97 Model for Role-Based Administration of Roles.", ACM Transactions on Information and System Security, Vol. 2, Number 1, pp. 105-135, 1999.

[5] Ravi Sandhu, Edward Coyne, Hal Feinstein and Charles Youman, "Role-Based Access Control Models", IEEE Computer, Vol. 29, Number 2, pages 38-47, 1996.

[6] Ravi Sandhu, Venkata Bhamidi and Qamar Munawer. "The ARBAC97 Model for Role-Base Administration of Roles", ACM Transcations on Information and System Security, Vol. 2, Number 1, pp. 105-135, 1999.

[7] Ravi Sandhu, "Role Activation Hierarchies", Proc. Third ACM Workshop in Role-Based Access Control, Fairfax, Virginia, October 22-33, pp. 33-40, 1998.

[8] M. J. Covington, M. J. Moyer and M. Ahamad, "Generalized role-based access control for securing future applications", In 23rd National Information Systems Security Conference, Baltimore, MD, October 2000.

[9] M. J. Moyer and M. Ahamad, "Generalized Role-Based Access Control", In proc of IEEE Int'l Conf. on Distributed Computing Systems(ICDSC2001), Mesa, pp. 391-398, 2001.

[10] Gustaf Neumann and Mark Strembeck, "An Approach to Engineer and Enforce Context Constraints in an RBAC Environment", Proceedings of the Eighth ACM Symposium on Access Control Models and Technologies, Como, Italy, June 2003.

[11] J. Hu and A. C. Weaver, "Dynamic, Context-aware Security Infrastructure for Distributed Healthcare Applications", Proceedings of First Workshop on Pervasive Security, Privacy and Trust (PSPT), August 26, 2004.[3] C. A. Balanis, "Antenna theory: analysis and design", John Wiley & Sons, Inc., 2nd ed. 1997

[12] C. Heitmeyer et al., "Using abstraction and model checking to detect safety violations in requirements specifications", IEEE Transactions on Software Engineering, Vol. 24, No. 11, 1998.

[13] William Chan et al., "Temporal Logic Queries", Proceedings of CAV 2000, LNCS 1855, Springer, 2000.

저자 소개

김 창 복(정회원)

- 1989년 단국대학교 일반대학원 전자공학과 졸업(공학석사)
- 2008년 인천대학교 일반대학원 컴퓨터공학과 졸업(공학박사)
- 2009년 현재 가천의과학대학교 IT학과 교수

<관심분야 >: u-헬스케어 정보처리, 센서 네트워크, 임베디드 시스템

박 승 환(정회원)

- 1984년 인하대학교 전자공학과 졸업 (공학사)
- 1990년 인하대학교 대학원 전자공학과 졸업(공학석사)
- 1996년 인하대학교 대학원 전자공학과 졸업(공학박사)
- 2009년 현재 을지대학교 의료공학과 교수

<관심분야 >: 의료 정보 처리 및 마이크로프로세서 응용시스템,네트워크 보안

김 남 일(정회원)

- 2000년8월 : 건국대학교 전자공학과 박사
- 2009년 현재 : 가천의과학대학교 IT학과 교수

<관심분야>컴퓨터네트워크,트래픽제어, 유비쿼터스,유헬스케어,BcN