공간 인식 서비스를 위한 Temporal constraints GEO-RBAC

신 동 욱,[1†] 황 유 동[2‡], 박 동 규[3‡]
[1]순천향대학교

Temporal constraints GEO-RBAC for Context Awareness Service

Dong-wook Shin,[1†] Yu-Dong Hwang[2‡], Dong-Gue Park[3‡]
[1]SoonChunHyang University

요 약

상황 인식 서비스가 발전하고 있는 요즘, 공간 인식 접근 제어 시스템에 높은 보안을 요구하고 있다. 이에 공간 역할의 사용자 할당, 권한의 할당, 역할 스키마와 역할 인스턴스, 공간 역할 계층, 그리고 공간 제약을 제공하는 GEO-RBAC은 공간 인식 서비스에 적합한 접근 제어 모델이다. 하지만 GEO-RBAC은 공간 인식 환경에 필요한 시간 제약을 고려하지 않는 단점이 있다. 따라서 본 논문에서는 시간 제약의 개념을 사용하여 효과적인 접근제어 모델을 제시한 GTRBAC의 시간과 기간 제약 개념을 고려하여 GEO-RBAC의 유연성을 높이고 다양한 경우에도 효과적인 접근제어를 할 수 있도록 시간 제약을 고려한 GEO-RBAC 모델을 제안한다.

Abstract

Developing context awareness service In these day, It demands high security in context awareness service. So GEO-RBAC that provide user assignment of spatial role, assignment of permission, role schema, role instance and spatial role hierarchy to context awareness service is access control model to perfect in context awareness service. But GEO-RBAC is not considering temporal constraints that have to need context awareness environment. Consequently this paper improves the flexibleness of GEO-RBAC to consider time and period constraints notion and the time of GTRBAC that presents effective access control model. also we propose GEO-RBAC to consider temporal constraints for effective access control despite a various case.

I. 서론

유비쿼터스 시대가 점점 실생활로 다가오면서, 공간인식 서비스(Context awareness service)에 대한 관심이 높아지고 있다. 널리 개발된 공간 기반 서비스, 모바일 어플리케이션뿐만 아니라 그에 따른 관리, 그리고 지형정보의 공유에 대한 관심이 높아지고 있어 환경 보호와 홈 시큐리티가 가능한 공간 인식 접근 제어 시스템에 높은 보안을 요구하고 있다.[12]

정보 보호의 서비스 중 하나인 접근제어는 컴퓨터 내의 데이터, 통신 자원 및 기타 여러 가지 데이터 등에 대하여 사용, 변경, 조회 등의 작업을 할 수 있는 능력을 가능하게 하거나 제한할 수 있는 방법으로 인증절차를 거친 사용자만이 허가된 범위 내에서 시스템 내부의 데이터에 대한 접근을 허용하는 기술적인 방법이다.

접근제어를 위해 개발된 보안 정책으로는 임의의 접근제어(DAC : Discretionary Access Control)[1], 강제적 접근 제어(MAC : Mandatory Access Control)[1], 역할 기반 접근 제어(RBAC : Role Based Access Control)[2, 3] 모델 등이 있다.

그러나 이들 모델들은 공간 인식에 따른 자원의 사용에 적합하지 않고, 공간 인식 서비스에서 빈번히 일어날 수 있는 사용자의 위치에 따른 자원에 대한 접근을 제어

할 수 없다는 단점이 있다. 공간 인식 환경에서는 동일한 사용자라 할지라도 사용자가 자원에 접근하고자 하는 위치에 따라 접근 권한을 부여할 수 있어야 한다. 예를 들면 사무실 내부에서 업무 중에는 외부에 유출되어서는 안돼는 자원에 접근 가능하지만, 정보보호 시스템으로 보호되지 않는 사무실 외부에서 손쉽게 자원에 접근 할 수 있다면 자원이 외부로 유출 또는 보안 위협의 대상이 될 수 있는 가능성이 커지기 때문이다.

이러한 문제점들을 해결하기 위하여 공간에 따른 사용자의 권한과 자원의 사용을 제한할 수 있는 GEO-RBAC(Geometry-Role Based Access Control) 모델[12]에 시간(기간과 주기) 제약(temporal constraints)을 적용하여 공간과 시간에 따른 권한 할당을 효율적으로 제어할 수 있는 Temporal Constraints을 고려한 GEO-RBAC 모델을 제안한다. 본 논문에서는 2장에서 기존에 연구되어 왔던 접근제어 모델들을 분석하고, 3장에서는 제안 모델의 특징을 서술하고 4장에서는 제안 모델과 기존 모델을 비교 분석하며, 5장에서 결론을 유도한다.

II. 기존 접근제어 모델의 분석

이 장에서는 접근제어와 관련이 있는 기존 연구들을 재검토하고 그들이 공간 인식 서비스 환경에 적용될 때 제한 사항들을 분석한다.

접근제어를 위한 보안 정책으로는 역할 기반 접근제어(Role Based Access Control : RBAC) 시간(기간과 주기)에 따른 제약과 역할의 활성화/비활성화, 이벤트, 트리거를 이용하여 자원의 사용을 제한하여 최소 권한 원칙을 이행할 수 있는 GTRBAC (Generalized Temporal Role Based Access Control)[8] 모델, OGIS(Open GIS Consortium)[11]을 기반으로 사용자의 위치를 인식해 정의되어진 공간 역할에 사용자 할당, 권한 할당, 공간 역할계층, 공간 제약을 제공하여 위치에 따른 자원의 사용을 제한하는 GEO-RBAC(Geometry Role Based Access Control)모델 등이 있다.

역할 기반 접근 제어(RBAC)는 사용자와 자원 관리를 경감시키기 위해 사용된다. 역할기반 접근제어에서 접근 권한은 역할과 관련이 있으며 사용자는 적절한 역할에 할당된다. 역할 기반 접근제어는 접근제어 요구 사항을 지정하는 첫 번째 수단으로서 역할 추상화를 사용한다. 역할을 관리 하는 동안에, 허가들은 역할들에 할당되고, 사용자들은 역할에 할당된다. 허가는 정보에 특정한 오퍼레이션을 수행할 능력을 승인하는 것이다. 현실 세계에서, 하나의 역할은 조직 내에서 하나의 직무 기능으로 정의할 수 있으며, 그 역할에 할당된 사용자에 부여된 권한과 책임을 의미한다. 하나의 역할 계층(role hierarchy)은 일반적으로 조직의 관리 구조에 따라서 역할사이의 권한 상속관계를 나타낸다. 역할 계층은 허가 권한 시스템과 유사하기 때문에 기업 조직 구조의 모델링에 적합하다. 그러나 역할기반 접근제어는 접근 권한의 동적 활성화와 응용 레벨 제약의 명세를 필요로 하는 워크플로우(workflow)를 고려하지 않고 있다.

GTRBAC 모델(Generalized Temporal Role Based Access Control)은 TRBAC 모델(Temporal Role Based Access Control)[7]을 확장한 모델로, 역할의 사용과, 역할 - 권한 할당, 역할 활성화를 포함한 주기적이고 지속적인 시간의 제약 집합을 위한 명세를 포함한다. GTRBAC 모델의 특징을 정리하면 다음과 같다.

- Temporal constraints on role enabling/disabling : 이 제약은 지연시간 또는 일정 기간 동안 사용자 - 역할 또는 역할 - 권한에 할당된 역할이 가능하도록 한다.
- Temporal constraints on user-role and role-permission assignments : 지정된 지연시간 또는 기간 동안 사용자와 권한을 역할에 할당한다.
- Activation constraints : 이 제약은 사용자들이 역할을 활성화 할 때 제한을 한다. 명세된 가간동안 역할의 활성화를 제한하거나 세션 상에서 역할의 활성화 수를 제한한다.
- Run-time events : 런타임 이벤트 들은 관리자가 GTRBAC 이벤트들을 동적으로 시작하거나, 역할 활성화 제약들 또는 기간을 가능하도록 한다.
- Constraint enabling expressions : GTRBAC 모델은 가능 또는 불가능하게 하는 기간 제약들과 역할 활성화 제약들을 포함한다. 기간 제약들은 사용자 - 역할 할당관계와 역할 - 권한 할당관계들에 의해 역할이 가능하게 한다.
- Triggers : 트리거 들은 다양한 임시 이벤트들 사이의 종속성을 표현하기 위하여 트리거 프레임 웍을 제공하여 시스템에 의해 동적으로 변화하는 접근제어 요구사항에 적절히 대응할 수 있다.

위의 내용으로 알 수 있듯이 GTRBAC 모델은 역할 활성화/비활성화와 이벤트 제약, 트리거를 이용하여 기존 모델에서는 불가능했던 접근 권한의 동적 활성화와 응용 레벨 제약의 명세를 필요로 하는 워크플로우(workflow)를 고려할 수 있게 되었고, 시간(기간과 주기)에 따른 제약으로 자원의 사용을 제한할 수 있게 되었다. 그러나 GTRBAC의 역할 계층 또한 기존 모델과 마찬가지로 I 역할 계층에서는 권한이 상위 역할로 무조건 상속되고, A 역할 계층에서는 상위 역할이 하위역할을 활성화 할 수 있으므로 하위 역할의 권한을 모두 획득할 수 있게 되어 권한의 남용을 방지 할 수 없고, 최소권한 원칙을 위배하게 되는 단점이 있다. 또한 이러한 부분 역할 계층이 하나의 역할 계층에 다양하게 혼합되어 존재 한다면 세션 상에서 사용자가 역할을 활성화 하였을 때 활성화 된 역할에게 역할 계층에 의해서 어떤 권한들이 허가되는지를 결정하는 복잡한 계산을 해야 한다.

GEO-RBAC 모델(Geometry Role Based Access Control)은 OGIS(Open GIS Consortium)를 기반으로 모든 지형을 데이터베이스화 시켜 정밀한 위상적 논리 공간을

만들고, 사용자의 위치를 위치 인식 단말기나 휴대폰으로 인식하여 물리 지형의 위치를 논리공간에 매핑 시키는 방법을 사용한다. 이렇게 만들어진 논리 공간에 정밀한 공간 범위 설정하고, 이 범위에 역할을 할당하여 사용자가 정해진 범위의 공간 안에서 자원의 사용을 제한할 수 있도록 한 모델이다. GEO-RBAC 모델의 특징을 정리하면 다음과 같다.

- 공간 인식 객체 : 지형(feature)에 각각 이름을 두고 그 이름으로 신원이 확인된다. 그 지형은 치수를 가지며, 기하학으로서 표현된다.
- 공간에 역할을 부여할 수 있는 이유는 OGIS의 Feature 기하, 공간참조시스템, 위치적 기하, Feature들간의 관계, 메타데이타, 정확도 및 속성스키마의 관계들 때문이다.
- 공간참조시스템에 의해 실세계의 지점과 임의의 기하좌표를 매핑 시켜 하나의 공간과 범위를 창출해 낸다.
- Feature : 지형은 크게 "공간"과 "비공간"으로 나누어지며, 공간은 길, 호수, 도시 등 지형을 나타낸다. 비공간은 자동차, 비행기 등 지형형태로 나타낼 수 없는 것들을 말하고 지형이 어떠한 위치에도 속하지 않았다면 비 공간이다.
- 역할 범위 : 역할 범위는 역할이 사용자가 가정될 수 있는 장소의 경계선을 정의하고. 역할의 범위는 기하학적인 의미상의 성격묘사를 갖는 것으로 가정한다.
- 논리 지형 : 공간 지형을 모델링 하여 실제 위치와 접목시키기 위한 개념적인 지형이다.
- 역할 스키마 : 역할 스키마는 유사한 의미를 가지는 공간 인식 조직 기능의 집합으로 공통된 어떤 성질들을 정의한다. 역할 스키마는 공간 역할 집합을 위한 공통된 이름뿐만 아니라 역할이 가능하게 할 수 있는 공간 제약도 정의하고 있다.

R_{schema} = < 역할의 이름, 역할범위, 논리적 위치, 실제위치를 매핑한 위치 >로 표시한다. 또한 모든 역할의 실례를 드는 역할 스키마는 역할 범위(지형)이름에 의해 완전히 신원 파악이 된다.

- 역할 인스턴스 : 공간 역할이라고도 하며, 스키마 레벨에서 제약 정의를 이행하는 역할이다. $R_{instance}$ = <공간 역할 이름, 역할 범위>로 표시한다.
- 권한 : Operations와 Objects 두 가지로 이루어져 있다. PRMS = <Ops, Obs>로 표시한다.
- Session : 기본적으로 Session은 EnableSession과 DisableSession으로 나누어진다.
- EnableSession : 사용자가 역할범위 공간에서 논리적 위치이면 EnableSession이다.
- DisableSession : 사용자가 역할 범위 공간에서 논리적 위치에서 벗어나면 DisableSession이다.

GEO-RBAC 모델은 OGIS를 이용하여 정밀한 지형을 표현할 수 있으며, 역할을 역할 스키마와 역할 인스턴스로 분류하여, 역할 관리의 용이함과 역할 명세의 단순화를 추구하였고 사용자의 위치 조건에 따라서 enabling/activation 상태를 두어 역할의 가능/불가능/활성화 상태로의 변환을 용이하게 한다. 그리고 권한 상속을 위해 역할 스키마계층과 역할 인스턴스 계층을 두어 권한 상속을 용이하게 하며, 정적/동적 의무 분리 제약을 두어 충돌이 일어날 수 있는 배타관계를 고려하였다. 또한 제약 클래스의 상위계층 일반화를 통해 제약의 증가를 막고 관리를 용이하게 한다. 그림 1은 GEO-RBAC 모델이다. GEO-RBAC 모델은 위의 설명과 그림에서 알 수 있듯이 공간 인식 서비스를 위한 접근제어 모델이다. GEO-RBAC 모델의 중심은 공간이고, 공간에 관한 정적의무 분리 동적 의무 분리 제약을 지원하지만, 시간에 관한 제약은 제공되지 않고 있다. 이는 시간 제약을 필요로 하는 경우 그에 맞는 서비스를 할 수 없음을 이야기한다. 따라서 GEO-RBAC 모델에 GTRBAC 모델의 temporal constraints의 개념을 적용한 GEO-RBAC 모델을 제안한다.

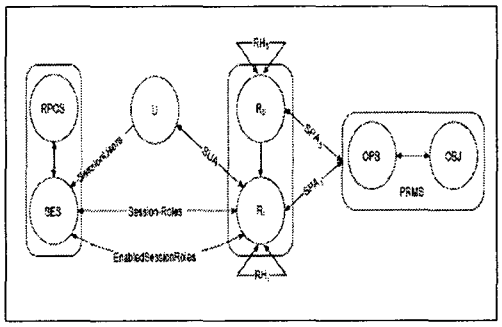

그림 1. GEO-RBAC 모델

III. Temporal constraints를 고려한 GEO-RBAC(Geometry Role Based Access Control)

3절에서는 기존의 GEO-RBAC 제약의 특징을 분석하고 temporal constraints를 적용한 GEO-RBAC 모델을 설명한다.

3.1 GEO-RBAC(Geometry Role Based Access Contorl) 모델의 제약특성

1. Granularity (schema/instance level) : 제약은 역할 스키마와 역할 인스턴스의 두 개 레벨 모두에서 정의할 수 있다.
2. Dimension (spatial/non-spatial) : 제약은 공간 수치를 가질 수도 있고 없을 수도 있다. 비공간 제약은 역할의 공간 치수를 고려하지 않기 때문에 표준 RBAC 제약과 흡

사해진다. 제약은 주어진 공간 관계를 이행하는 역할 인스턴스를 적용할 때 공간이다.

3. Verification time (static/dynamic at activation time/dynamic at enabling time) : 제약은 정지 상태 이거나 역할이 수행되고 있을 때 평가되어질 수 있다. 이 경우에서 역할 activation time에 제약을 둘 것인지 enabling time에 제약을 둘 것인지를 생각한다.

GEO-RBAC 모델의 제약에서 위의 3가지 특성의 결합으로 그림 2, 3과 같은 클래스를 표현할 수 있다. 그림 2는 Static/Dynamic 상태, Instance/Shema based 상태, activation/enabling 상태, Spatial/Non-Spatial 상태를 구분하여, 다음을 정의한다.

1) 만약 집합이 역할 인스턴스의 집합이면 인스턴스 기반 제약이다.

2) 만약 집합이 역할 스키마 집합이면 스키마 기반 제약이다.

3) 만약 type = ⊥ 이면 정적 제약이다.

4) 만약 type = a(type = e)이면 활성화(가능) 상태에서 동적 제약이다.

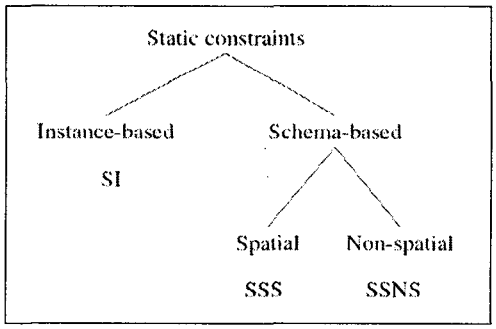

그림 2. GEO-RBAC의 정적 의무 분리 분류

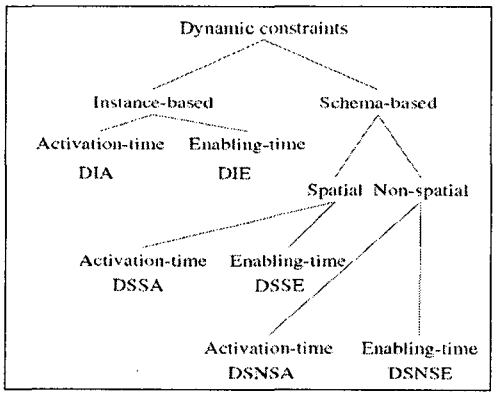

그림 3. GEO-RBAC의 동적 의무 분리 분류

3.2 GEO-RBAC의 정적 제약

정적 제약은 그림 2에서 볼 수 있듯이 세 가지로 분류 할 수 있다.

① SI(Static Instance-based) 제약 : 인스턴스 레벨에서 정의되며(role_instance_set, n)⊥으로 표시한다. 의미는 role_instance_set에 명세된 것 중에서 n개의 역할 또는 더

표 1 GEO-RBAC 모델의 정적 제약 명세표

class	SI
form	(RoleSet, n)⊥
formal specification	$\forall h \subseteq RoleSet, \lvert h\rvert \geq n \Rightarrow \bigcap_{r \in h} SR\_AssignedUser(r) = \varnothing$
class	SSNS
form1	(ShemaSet, n)⊥ |SchemaSet|>1
form2	({r, s}, n)⊥
formal specification 1	$\forall s = \{rsi, \cdots rsj\}, s \subseteq SchemaSet, \lvert s\rvert \geq n \Rightarrow \bigcap_{i \leq k \leq j} \bigcup_{r \in Ext(rs_k)} SR\_AssignedUser(r) = \emptyset$
formal specification 2	$\forall h \subseteq Ext(rs), \lvert h\rvert \geq n \Rightarrow \bigcap_{r \in h} SR\_AssignedUser(r) = \varnothing$
class	SSS
form	(rs1, rs2, rel)⊥
formal specification	$\forall x \subseteq Ext(rs1), \forall y \subseteq Ext(rs2), x\ rel\ y \Rightarrow SR\_AssignedUser(x) \cap SR\_AssignedUser(y) = \varnothing$

많은 역할 인스턴스가 실행되는 것을 금지한다.

예) RoleSet = {Doctor(Hosp1), Doctor(Hosp2)}를 가정하면, 제약 (RoleSet, 2)⊥ ∈ SI의 의미는 사용자가 Hosp1과 Hosp2 두 곳에서 의사가 될 수 없다. 그리고 역할은 같은 스키마 이거나 다른 스키마의 인스턴스가 될 수 있다.

② SSNS(Static Schema based Non-spatial) 제약 : 스키마 레벨에서 정의되며(role_schema_set,n)⊥, n≥2로 표시한다. 의미는 role_schema_set에서 n개의 스키마로부터 n개의 역할 인스턴스가 실행될 수 없도록 한다.

예) 역할 스키마 Do = <Doctor, Hospital, Sector, mSector>를 가정하면, 제약 (Do, 2)⊥ ∈ SSNS 제약의 의미는 사용자가 여러 개의 병원에서 의사가 될 수 있다는 의미이다.

③ SSS(Static Schema based spatial) 제약 : 역시 스키마 레벨에서 정의된다,
예) 역할 Doctor와 Manager에 반응하는 Do와 Ma스키마를 가정한다. 제약 (Do, Ma, Equal)ㅗ의 의미는 개인 사용자는 같은 병원에서 Doctor와 Manager가 동시에 될 수 없다는 의미이다. 표 1은 정적 제약 클래스의 명세표를 보여준다.

표 2 GEO-RBAC 모델의 동적 제약 명세표

class	DIA
form	(RoleSet, n)$_a$
formal specification	$\forall t \in SES, \forall h \subseteq RoleSet, h \subseteq SessionRoles(t) \Rightarrow |h|<n$
class	DIE
form	(RoleSet, n)a
formal specification	$\forall t \in SES, \forall h \subseteq RoleSet, \forall pos \in RPOS, h \subseteq EnabledSessionRoles(t, pos) \Rightarrow |h|<n$
class	DSNSA
form1	(ScheamSet, n)a |SchemaSet|>1
form2	({r, s}, n)$_a$
formal specification 1	$\forall t \in SES, \forall s=\{rsi, \cdots, rsj\}, s \subseteq SchemaSet, \forall h=\{ri(ei), \cdots, rj(ej)\}, rk \in Ext(rs_k), i \le j \le k, h \subseteq SessionRoles(t) \Rightarrow |h|<n$
formal specification 2	$\forall t \in SES, \forall h \subseteq Ext(rs), h \subseteq SessionRoles(t) \Rightarrow |h|<n$
class	DSNSE
form1	(SchemaSet, n)e |SchemaSet|>1
form2	({rs}, n)e
formal specification 1	$\forall t \in SES, \forall s=\{rsi, \cdots, rsj\}, s \subseteq SchemaSet, \forall pos \in RPOS, \forall h=\{ri(ei), \cdots, rj(ej)\}, rk \in Ext(rs_k), i \le j \le k, h \subseteq EnabledSessionRoles(t, pos) \Rightarrow |h|<n$
formal specification 2	$\forall t \in SES, \forall pos \in RPOS, \forall h \subseteq Ext(rs), h \subseteq EnabledSessionRoles(t, pos) \Rightarrow |h|<n$
class	DSSA
form	(rs1, rs2, rel)a
formal specification	$\forall x \in Ext(rs1), \forall y \in Ext(rs2), \forall t \in SES, x \; Rel \; y \Rightarrow \{x, y\} \not\subseteq SessionRoles(t)$
class	DSSE
form	(rs1, rs2, rel)e
formal specification	$\forall x \in Ext(rs1), \forall y \in Ext(rs2), \forall t \in SES, \forall pos \in RPOS,, x \; Rel \; y \Rightarrow \{x, y\} \not\subseteq EnabledSessionRoles(t,pos)$

3.3 GEO-RBAC의 동적 제약

동적 제약에서는 activation time과 enabling time을 구분하여 결정하고 6개로 분류할 수 있다.

① DIA(Dynamic Instance-based Activation) 제약과 DIE(Dynamic Instance-based Enabling) 제약 : 인스턴스 레벨에서 정의되며, (role_instance_set, n)f, f ∈{a, e}로 표시한다.
- f = a인 경우 : activation time
- f = e인 경우 : enabling time

role_instance_set에 명세 되어진 것 중에 n개의 역할 또는 더 많은 역할 인스턴스의 실행을 금지한다.
예)인스턴스 RoleSet={Nurse(Dep1), Nurse(Dep2)}
제약 (RoleSet, 2)a 의 의미는 Nurse가 근무하는 동안 병동 Dep1과 Dep2 에서 활성화 되어 질 수 없다.

②DSNSA(Dynamic Schema-based Non-Spatial Activation) 제약과 DSNSE(Dynamic Schema-based Non-Spatial Enabling) 제약 : 스키마 레벨에서 정의되며, (role_schema_set, n)f, n≥2, f∈{a, e}로 표시한다.
- f = a인 경우 : activation time
- f = e인 경우 : enabling time

의미는 role_schema_set에서 n 스키마로 부터 역할 인스턴스를 구분 짓는 n 세션의 역할 사용을 금지한다.
예) 간호사 역할을 위한 스키마 Nu를 가정한다. activation time 제약({Nu}, 2)a은 간호사가 다른 병동에 할당 될 수 있지만 시스템과 상호 작용하는 세션동안에는 하나 이상의 병동에서 활동할 수 없다.
enabling time 제약 ({Nu}, 2)e은 간호사가 더 많은 병동

에서 활성화 되어 질 수 있는 상태이기 때문에 같은 스키마의 다른 역할을 실행할 수 있다,

③ DSSA(Dynamic Schema-based Spatial Activation) 제약과 DSSE(Dynamic Schema-based Spatial Enabling) 제약 : 스키마 레벨에서 정의되며 (rs1, rs2, rel)f, f∈{a, e}로 표시한다.

- f = a인 경우 : activation time
- f = e인 경우 : enabling time

의미는 그들의 범위가 공간 관계 rel을 만족할 때 rs2 스키마와 rs1으로 부터 역할 인스턴스를 구분 짓는다.

예) 역할 Doctor와 Patient에 반응하는 Do와 Pa스키마를 가정한다. 제약 (Do, Pa, Equal)의 의미는 의사가 같은 병원에서 동시에 환자를 볼 수 없다는 의미이다. 표 2는 동적 제약의 명세표를 보여준다.

3.4 제안 모델의 정적 제약

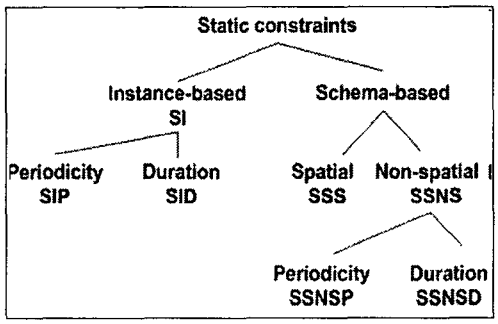

그림 4. 시간 제약 정적 의무 분리 분류

그림 4와 그림 5는 기존의 GEO-RBAC모델에 시간 제약을 추가한 temporal constraints를 고려한 GEO-RBAC 모델이다. 시간 제약의 관념은 GTRBAC의 정의를 따르고 있다. 제안된 모델은 다음과 같은 제약 분류를 나타낼 수 있다.

① SIP(Static Instance-based Periodicity) 제약과 SID(Static Instance-based Duration) 제약 : 인스턴스 레벨에서 정의되며(role_instance_set, n)⊥ & (I, P, SSoD) 또는 (role_instance_set, n)⊥ & ([I, P|D], Dx, SSoD)로 표시한다. 의미는 role_instance_set에 명세된 것 중에서 n개의 역할 또는 더 많은 역할 인스턴스가 주어진 시간 또는 기간 동안 실행되는 것을 금지한다.

예) RoleSet = {Doctor(Hosp1), Doctor(Hosp2)}를 가정하면, 제약 (RoleSet, 2)⊥ & ([1.1.2006, ∞], WorkingDaysOfWeek),({Doctor(Hosp1), Doctor(Hosp2)})) ∈ SIP의 의미는 사용자가 Hosp1과 Hosp2 두 곳에서 2006년 1월 1일부터 ∞까지 의사가 될 수 없다. 그리고 역할은 같은 스키마 이거나 다른 스키마의 인스턴스가 될 수 있다.

② SSNSP(Static Schema-based Non-Spatial Periodicity) 제약과 SSNSD(Static Schema-based Non-Spatial Duration) 제약 : 스키마 레벨에서 정의되며(role_schema_set,n)⊥ & (I, P, SSoD) , n≥2 또는 (role_schema_set,n)⊥ & ([I, P|D], Dx, SSoD) , n≥2로 표시한다. 의미는 role_schema_set에서 n개의 스키마로부터 n개의 역할 인스턴스가 주어진 시간 또는 기간 동안 실행될 수 없도록 한다.

예) 역할 스키마 Do = <Doctor, Hospital, Sector, mSector>를 가정하면, 제약 (Do, 2)⊥ & ([1.1.2006, ∞], WorkingDaysOfWeek),({Do})) ∈ SSNSP 제약의 의미는 사용자가 여러 개의 병원에서 2006년 1월 1일부터 ∞까지 의사가 될 수 있다는 의미이다.

3.5 제안 모델의 동적 제약

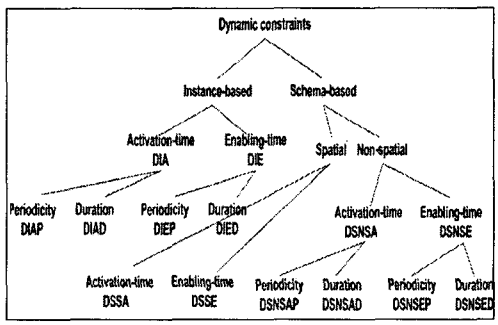

그림 5. 시간 제약 동적 의무 분리 분류

① DIAP/D(Dynamic Instance-based Activation Periodicity/Duration) 제약과 DIEP/D (Dynamic Instance-based Enabling Periodicity/Duration) 제약 제약과 제약 : 인스턴스 레벨에서 정의되며, (role_instance_set, n)f & (I, P, DSoD) f ∈{a, e} 또는 (role_instance_set, n)f & ([I, P|D], Dx, DSoD) f ∈{a, e}로 표시한다.

- f = a인 경우 : activation time
- f = e인 경우 : enabling time

role_instance_set에 명세 되어진 것 중 n개의 역할 또는 더 많은 역할 인스턴스로 부터 일정 시간 또는 일정 기간 동안 실행을 금지한다.

예)인스턴스 RoleSet={Nurse(Dep1), Nurse(Dep2)}를 가정하면, 제약 (RoleSet, 2)a & ([1.1.2006, ∞], WorkingDaysOfWeek), (Nurse(Dep1), Nurse(Dep2)) 의 의미는 Nurse가 근무하는 2006년 1월 1일부터 ∞까지의 시간동안 병동 Dep1과 Dep2 에서 활성화 되어 질 수 없다.

② DSNSAP/D(Dynamic Schema-based Non-Spatial

Activation Periodicity/Duration) 제약과 DSNSEP?/D(Dynamic Schema-based Non-Spatial Enabling Periodicity/Duration) 제약 : 스키마 레벨에서 정의되며, (role_schema_set, n)f & (I, P, DSoD), n ≥2, f∈{a, e} 또는 (role_schema_set, n)f & ([I, P|D], Dx, DSoD), n≥2, f∈{a, e}로 표시한다.
- f = a인 경우 : activation time
- f = e인 경우 : enabling time
의미는 role_schema_set에서 n 스키마로 부터 역할 인스턴스를 구분 짓는 n 세션에 일정 시간 또는 일정 기간 동안 역할 사용을 금지한다.
예) 간호사 역할을 위한 스키마 Nu를 가정한다. activation time 제약({Nu}, 2)a & ([1.1.2006, ∞], WorkingDaysOfWeek), (Nu)은 간호사가 다른 병동에 할당 될 수 있지만 시스템과 상호 작용하는 세션 동안 2006년 1월 1일부터 ∞ 시간까지 하나 이상의 병동에서 활동할 수 없다. enabling time 제약 ({Nu}, 2)e & ([1.1.2006, ∞], WorkingDaysOfWeek), (Nu)은 간호사가 더 많은 병동에서 활성화 되어 질 수 있는 상태이기 때문에 역할 2006년 1월 1일부터 ∞ 시간까지, 같은 스키마의 다른 역할을 실행할 수 있다.

IV. 제안 모델과 기존 모델의 비교

temporal constraints를 고려한 GEO-RBAC 모델의 특징을 기존 모델과 비교하면 표 3과 같다.

- 역할 스키마 레벨에서의 역할 시간, 기간, 주기 제약 고려.
- 역할 스키마 레벨에서의 역할 enable/activation 시의 시간, 기간, 주기 제약 고려.
- 역할 인스턴스 레벨에서의 역할 시간, 기간, 주기 제약 고려.
- 역할 인스턴스 레벨에서의 역할 enable/activation 시의 시간, 기간, 주기 제약 고려.

표 3 기존 모델과 제안 모델의 제약 비교

역할 : 사용자 - 역할 할당	RBAC	GT RBAC	GEO-RBAC	제안모델
사용자 - 역할 할당	o	o	o	o
시간과 기간 제약을 고려한 사용자 - 역할 할당	x	o	x	o
공간 제약을 고려한 사용자 - 역할 할당	x	x	o	o
시간과 공간 제약을 고려한 사용자 - 역할 할당	x	x	x	o

- 역할 스키마 레벨에서의 역할 시간, 기간, 주기 제약 고려.
- 역할 스키마 레벨에서의 역할 enable/activation 시의 시간, 기간, 주기 제약 고려.
- 역할 인스턴스 레벨에서의 역할 시간, 기간, 주기 제약 고려.
- 역할 인스턴스 레벨에서의 역할 enable/activation 시의 시간, 기간, 주기 제약 고려.
기존의 모델에 시간, 기간 주기 제약을 추가함으로써 다음과 같은 이점을 얻을 수 있다. 예를 들어서 PartTimeDoctor, DayTimeDoctor, NightTimeDoctor의 역할을 가정한다. PartTimeDoctor의 역할 가능 시간은 3:00 p.m.~ 6:00 p.m.과 7:00 a.m. ~ 10:00 a.m.이고, DayTimeDoctor는 9:00am ~ 9:00pm, NightTimeDoctor는 9:00pm ~ 9:00am를 갖는 역할이 있을 경우, 시간에 구애받는 역할이기 때문에 시간에 따른 제약이 주어져야 한다.
하지만 위에서 설명한 바와 같이 기존의 GEO-RBAC 모델로는 시간에 관한 제약 모델이 없기 때문에 제약을 둘 수가 없다. 공간 제약과 Enabling/Activation 시에 대한 제약만을 가지고 있기 때문이다. 하지만 제안된 모델은 년, 월, 일 등 시간과 기간, 주기를 설정하고 역할 스키마 레벨, 역할 인스턴스 레벨에서 주기적/지속적 제약을 줄 수 있기 때문에 기존의 모델보다 훨씬 더 유연하고 강력한 제약을 취할 수 있다.

V. 결론

본 모델에서는 기존의 GEO-RBAC 모델(Geometry Role Based Access Control)의 강력한 공간 인식 접근 제어 모델에 temporal constraints를 추가 함 으로써 더 유연한 제약이 가능한 모델을 제안한다.

- 역할 스키마 레벨에서의 역할 시간, 기간, 주기 제약을 고려하고, 역할 enable/activation 시간에서의 시간, 기간, 주기 제약을 고려하였다.
- 역할 인스턴스 레벨에서의 역할 시간, 기간, 주기 제약을 고려하고, 역할 enable/activation 시간에서의 시간, 기간, 주기 제약을 고려하였다.
- 역할에 시간 제약을 둬야하는 경우 유연하게 대처할 수 있다.

제안한 모델은 홈 시큐리티가 가능한 공간 인식 접근 제어 시스템에 높은 보안을 제공할 수 있는 기능을 제공하고 있다.
향후에는 공간 인식 서비스에서 발생할 수 있는 공간 역할 딜레마에 대한 연구가 필요할 것으로 생각되고, 멀티 도메인 환경에서의 공간 인식 서비스에 대한 연구가 필요할 것으로 사료된다.

[참고문헌]

[1] C.P.Pfleeger, Security in Computing, second edition, Prentice-Hall International Inc, pp.290-315 , 1997

[2] R.S.Sandhu and E.J.Coyne and H.L.Feinstein and C.E.Youman "Role-Based Access control Models", IEEE Computer, vol. 29, pp.38-47, 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] Dagstull and G.Coulouris and J.Dollimore "A Security Model for Cooperative work : a model and its system implications" Positions paper for ACM European SIGOPS Workshop, 1994

[5] R.K.Thomas and R.S.Sandhu "Task-based Authorization Controls(TBAC) : A Family of Models for Active and Enterprise-oriented Authorization Management" Proc. of the IFIP WF11.3 Workshop on Database Security, 1997

[6] S. Oh and S. Park "Task-Role Based Access Control (T-RBAC): An Improved Access Control Model for Enterprise Environment", Proceedings of the 11th International Conference on Database and Expert Systems Applications, pp. 264-273, 2000

[7] J. B. D. Joshi and E. Bertino and A. Ghafoor "Temporal Hierarchies and Inheritance Semantics for GTRBAC", Seventh ACM Symposium on Access Control Models and Technologies, pp. 74-83, 2002

[8] J. B. D. Joshi and E. Bertino and A. Ghafoor "Hybrid Role Hierarchy for Generalized Temporal Role Based Access Control Model", Proceedings of the 26 th Annual International Computer Software and Applications Conference, 2002

[9] J. B. D. Joshi and E. Bertino and A. Ghafoor "Temporal Role Hierarchies in GTRBAC", CERIAS, 2002

[10] 진희채, "지형,공간정보의 상호운영성을 보장하는 Open GIS", 1998.3 정보과학회지 제 16권 제 3호

[11] Elisa Bertino, Barbara Catania, Maria Luisa Damiani, Paolo Perlasca, "GEO-RBAC: a spatially aware RBAC", CERIAS Tech Report 2006-05

[12] Michael J. Covington., Matthew J. Moyer, Mustaque Ahamad, "Securing context-aware applications using environment roles", Proceedings of the sixth ACM symposium on Access control models and technologies ,May 2001