情報保護學會論文誌
第 23 卷 第 2 號, 2013. 4

SG-RBAC : 스마트그리드 환경에 적합한 역할기반접근제어 모델*

이 우 묘,† 이 건 희, 김 신 규,‡ 서 정 택
ETRI 부설연구소

SG-RBAC : Role Based Access Control Model for Smart Grid Environment*

Woomyo Lee,† Gunhee Lee, Sinkyu Kim,‡ Jungtaek Seo
The Attached Institute of ETRI

요 약

스마트그리드는 다양한 도메인의 다양한 기기가 상호 운용되고 상황에 따라 다른 접근권한을 가질 수 있다. 따라서 스마트그리드 기기 및 시스템 내부에 접근 가능한 권한들을 효율적으로 관리하여, 접근권한 관련 설정 오류를 최소화하고 권한이 없는 사용자의 접근을 차단하기 위한 '스마트그리드 환경에 적합한 접근제어 기술'이 요구된다. 본 논문에서는 스마트그리드 환경을 분석하여 접근제어 시 요구사항들을 정리하고 이를 만족하는 SG-RBAC 모델을 제안하였다. SG-RBAC 모델은 사용자 특성, 역할 특성, 시스템 특성에 따라 권한 활성화 제약이 가능하며, 권한위임과 권한 상속 시에 시간, 위치정보, 위기 상황 발생여부에 따라 제약을 가할 수 있다.

ABSTRACT

Smart grid is composed of variable domains including different systems, and different types of the access control are needed in the multiple domain. Therefore, the access control model suitable for the smart grid environment is required to minimize access control error and deny the unauthorized access. This paper introduce the access control requirements in the smart grid environment and propose the access control model, SG-RBAC, satisfied with the requirements. SG-RBAC model imposes constraints on the access right activation according to the user property, the role property, and the system property. It also imposes constraints on the delegation and the inheritance of access right according to temporal/spatial information and a crisis occurrence.

Keywords: Smart grid, Role based access control, RBAC

I. 서 론

스마트그리드(Smart Grid)는 '발전-송배전-판매'의 세 단계로 이뤄지던 기존의 단방향 전력망에 IT 정보기술을 접목하여 전력 공급자와 소비자 사이에 실시간으로 전력정보를 교환하는 양방향 전력망을 일컫는다. 우리나라는 2010년 1월 스마트그리드 추진을 위한 국가 로드맵을 발표하고 2030년까지 세계최초 국가단위 스마트그리드 구축을 목표로 현재 스마트그리드 사업을 추진하고 있다.

스마트그리드는 다양한 도메인의 다양한 기기가 상호 운용되고 상황에 따라 다른 접근권한을 가질 수 있다. 따라서 스마트그리드 기기 및 시스템 내부에 접근

접수일(2013년 2월 20일), 수정일(2013년 4월 8일), 게재확정일(2013년 4월 8일)
* 본 연구는 2012년도 지식경제부의 재원으로 한국에너지기술평가원(KETEP)의 지원을 받아 수행한 연구 과제입니다. (2012101050004A)
† 주저자, wmlee@postech.ac.kr
‡ 교신저자, skkim@ensec.re.kr

가능한 권한들을 효율적으로 관리하여, 접근권한 관련 설정 오류를 최소화하고 권한이 없는 사용자의 접근을 차단하기 위한 '스마트그리드 환경에 적합한 접근제어 기술'이 요구된다.

접근제어 시스템은 크게 강제적 접근제어(Mandatory Access Control, MAC[1,2,3]), 임의적 접근제어(Discretionary Access Control, DAC[4,5,6]), 역할기반 접근제어 (Role Based Access Control, RBAC[7,8,9,10]) 등으로 구분할 수 있다. 최근에는 기존 접근제어 방법에 다양한 특성이 추가된 접근제어 방법들이 제안되고 있다. GTRBAC(Generalized Temporal Role Based Access Control[11,12,13])은 시간과 주기에 따른 권한 활성화 제약 특성을 가지고, dRBAC(distributed Role Based Access Control[14,15,16])은 다중 도메인 간에 권한 위임 특성을 가지며, PRBAC(Privacy Role Based Access Control[17,18])은 객체 접근시 프라이버시 정책을 반영하는 특성을 가진다. 하지만 스마트그리드 환경에서는 여러 가지 특성을 동시에 가지고 있어야 하므로 기존의 접근제어 방법을 그대로 적용할 수 없다.

본 논문에서는 스마트그리드 환경을 분석하여 접근제어 요구사항들을 정리하였다. 또한 제안한 요구사항들을 모두 만족하는 SG-RBAC 모델을 통해 사용자 특성, 역할 특성, 시스템 특성에 따른 권한 제약방식과 시간, 위치정보, 위기 상황 발생여부에 따라 제약이 가능한 권한 위임 및 상속 방식을 제안하였다. 제안하는 SG-RBAC모델은 GTRBAC [11,12,13]의 시간에 따른 권한활성화 제약 특성과 PRBAC[17,18]의 조건·의무 개념을 포함하고 있으며, 다양한 권한 활성화 제약 방식과 권한 위임 방식을 가진다.

Ⅱ장에서는 스마트그리드 환경에서의 접근제어 요구사항을 정리한다. Ⅲ장에서는 요구사항을 모두 만족하는 스마트그리드 환경에 적합한 접근제어 모델을 제안하며 Ⅳ장에서 결론을 맺는다.

Ⅱ. 스마트그리드 환경에서의 접근제어 요구사항

스마트그리드 환경에서는 전력회사, 전력거래소, 이동통신사 등 다수의 기업이 참여하여 서로 다른 시스템으로 구성된 다양한 도메인을 구성한다. 각 지역에 분산된 시스템들은 서로 협력하여 유기적으로 동작하므로 다중 도메인 상에서 다양한 종류의 객체 접근이 필요하게 된다. 따라서 스마트그리드 기기 및 시스템 내부에 접근 가능한 권한들을 효율적으로 관리하여, 접근권한 관련 설정 오류를 최소화하고 권한이 없는 사용자의 접근을 차단해야 한다. 또한 국가 기반시설인 전력망에 전력수급상 위기 상황이 발생할 경우 각 상황을 예외적으로 처리하여 불필요한 권한들을 비활성화하고, 필요에 따라 권한 위임을 활성화하여 필수 기능을 항상 수행할 수 있어야 한다. 이러한 스마트그리드 환경의 특성에 따라 다양한 접근제어 요구사항이 발생하며, 이를 [표 1]로 정리하였다.

[표 1] 스마트그리드 환경에서 접근제어 요구사항

	요구사항	
1	다중도메인 지원	
2	사용자 권한 활성화 제약	권한 사용 시간
		사용자의 위치정보
		권한 유효기간
		위기 시 권한 (비)활성화
3	권한 위임	사용자간 위임
		역할간 위임
		다중 위임
4	권한 위임 제약	위임된 권한 사용 시간
		사용자의 위치정보
		타 역할계층 사용자간 권한 위임
		위임된 권한 유효기간
		위기 시 임의 위임 가능
5	권한 상속 제한	역할계층 레벨
		유효기간
6	직무분할(SoD) 지원	

A 전력회사의 전력운영센터와 B 이동통신사가 구축한 통신 시스템 사이에 접근제어가 발생한 경우를 예를 들어 설명할 수 있다. B 통신회사의 특정 기기가 A 전력회사 운영시스템의 데이터베이스에 접근하고자 할 때, 접근하려는 주체(B 통신회사 기기)의 위치에 따라 접근을 허가하고, 정해진 시간 외에는 권한을 가진 주체라도 해당 권한을 사용할 수 없도록 조치할 수 있어야 한다. 또한 A 전력회사 운영시스템은 B 통신회사의 기기에 권한을 부여할 때 유효기간을 설정하여 일정시간 이후에 재인증이 이뤄지도록 해야 한다.

A전력회사의 운영시스템에는 전력제어 관리자, 전력거래 운영자, 실시간관제업무 수행자와 같은 관리자들이 각각 업무에 필요한 다양한 역할들을 부여받는다고 가정할 수 있다. 전력제어 관리자가 자리를 비울 경우 상황에 맞게 권한의 일부를 동료에게 위임할 수 있어야 한다. 또한 특정 시스템이 공격을 받아 일부

프로세스가 동작하지 않을 경우, 위기상황을 감지하여 다른 프로세스에 권한을 위임함으로써 전력공급이 중단되는 상황을 피할 수 있어야 한다. 하지만 무분별한 권한위임은 보안상 심각한 위협으로 작용될 수 있으므로 사용자가 위임된 역할을 사용하는 시간이나 사용자의 위치정보에 따라 권한위임에 제한을 가할 수 있어야 한다. 또한 위임된 권한이 남용되지 않도록 권한 위임 시 유효기간을 설정하고, 전력수급상 위기 상황이 발생할 경우 각 상황을 예외적으로 처리하여 해당 담당자가 없더라도 위임된 권한이 활성화되어 필요한 기능을 수행할 수 있어야 한다.

스마트미터와 같은 특정 기기들은 설치된 위치를 벗어날 경우 동작하지 않고, 스마트기기를 관리하는 점검원들은 정해진 장소와 시간에만 점검 업무를 수행할 수 있어야 한다. 이 때 점검원들에게 주어진 점검 권한은 일정기간동안만 유효성을 가지도록 제한할 수 있어야 한다.

역할기반 접근제어에서 역할계층을 사용하면 상위 계층 역할이 하위 계층 역할의 퍼미션을 상속받게 된다. 이때 모든 역할의 퍼미션이 역할계층의 레벨에 따라 상속될 경우 상위 계층 역할을 부여받은 사용자에게 필요이상의 객체접근이 허용될 수 있으므로 역할계층의 레벨과 상속 유효기간에 따라 상속된 역할에 제한을 가할 수 있어야 한다.

일반적인 접근제어 시스템에서 요구되는 직무분할(Separation of Duty, SoD)은 업무와 관련된 권한들을 다양한 역할에 배분하여 한 사용자가 너무 많은 권한을 획득하는 것을 막아주는 개념이다. 스마트그리드는 다수의 역할과 권한이 사용되므로 제약(constraint)을 통해 불필요한 권한 활성화, 권한 위임, 권한 상속이 발생하지 않도록 하여 최소 특권의 원리(principle of least privilege)를 적용함으로써 직무분할을 실현해야 한다.

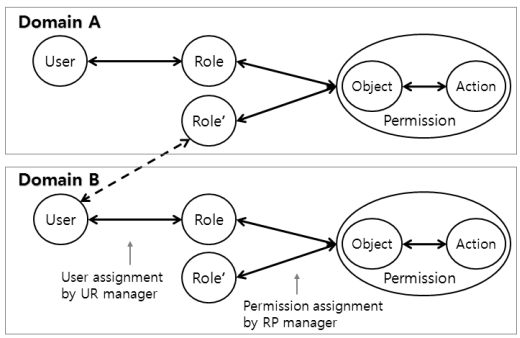
III. SG-RBAC 모델

본 논문에서는 대규모 시스템에서 정책 관리 편의성이 가장 높은 것으로 알려진 역할기반 접근제어 방식을 기반으로 앞서 정리한 접근제어 요구사항들을 모두 만족하는 SG-RBAC 모델을 제안한다. SG-RBAC 모델은 GTRBAC[11,12,13]의 시간에 따른 권한활성화 제약 특성과 PRBAC[17,18]의 조건·의무 개념을 적용하였으며, 본 논문에서는 SG-RBAC모델을 통해 사용자 특성, 역할 특성, 시스템 특성에 따른 권한 제약방식과 시간, 위치정보, 위기 상황 발생여부에 따라 제약이 가능한 권한 위임 및 상속 방식을 제안한다.

3.1 SG-RBAC 모델 구성

SG-RBAC 모델에서 각 도메인은 [그림 1]과 같이 사용자(user), 역할(role), 타도메인접근역할(role′), 퍼미션(permission)으로 구성된다. 사용자, 역할, 퍼미션은 기존의 RBAC 모델과 동일하며 타도메인접근역할 개념이 추가되었다.

- 사용자 : 사용자는 도메인에서 특정역할을 가지며 특정 객체에 접근권한을 가지는 주체를 뜻한다. 도메인의 사용자-역할 맵핑관리자(UR 관리자)는 사용자를 인증하여 정당한 사용자에게 적절한 역할을 부여하며 사용자-역할 맵핑을 관리한다.
- 역할 : 도메인 내에서만 사용되는 역할로서 UR 관리자가 사용자에게 부여하며 역할마다 특정 객체들에 대한 접근권한을 가지고 있다. 도메인의 역할-퍼미션 맵핑관리자(RP 관리자)는 역할마다 접근 가능한 객체와 접근 방법을 퍼미션을 통해 부여하며 역할-퍼미션 맵핑을 관리한다.
- 타도메인접근역할 : 타 도메인의 사용자가 객체 접근시 사용되는 역할로서, 사용자가 자신이 속하지 않은 타 도메인의 객체에 접근할 경우 인증기관으로부터 인증서를 부여받아야 한다.
- 퍼미션 : 접근대상이 되는 객체(object)와 접근방법(action)으로 구성된다.



[그림 1] SG-RBAC 모델 구성도

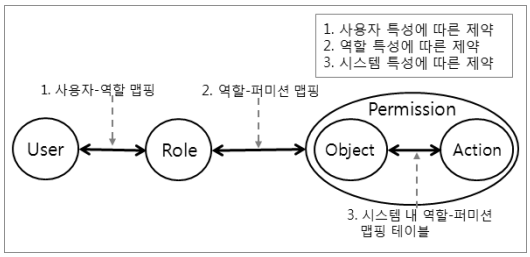
3.1.1 SG-RBAC 모델 구성 요소

SG-RBAC 모델은 사용자, 역할, 객체, 퍼미션, 역할 계층, 사용자 속성값, 위임 속성값, 크래덴셜, 사용자-역할 맵핑, 역할-사용자 맵핑 등 다양한 구성 요소를 가진다. 각 구성요소는 다음과 같이 표현될 수 있다.

-사용자집합:USER={$user_1$,$user_2$,…,$user_{n1}$}
-역할집합:ROLE={$role_1$, $role_2$,…,$role_{n2}$}
-위임가능한 역할집합:ROLE*={$role_x$|$role_x$∈ROLE}
ROLE*⊆ROLE
-위임된 역할집합:D_ROLE={$Drole_1$,…, $Drole\_dn$}
D_ROLE⊆ROLE*⊆ROLE, dn≤n2
-상속가능 역할집합:I_ROLE={$Irole_1$,…, $Irole\_in$}
I_ROLE⊆ROLE
-사용자A역할집합:
ROLE_A={$role_x$,〔$Irole_y$||condition_I〕|$role_x$, $role_y$∈ROLE}, ROLE_A ⊆ ROLE
-객체집합:OBJECT={$object_1$,… $object_{l1}$}
-접근방식집합:ACTION={$action_1$,… $action_{l2}$}
-퍼미션집합:PERM⊆OBJECT×ACTION
PERM={$perm_1$,$perm_2$,…,$perm_{n3}$}
perm_i=〈$object_x$,$action_y$〉,
where 1≤i≤n3,1≤x≤l1, 1≤y≤l2
-역할 계층:RH⊆ROLE×ROLE
-사용자속성값 집합:ATT={att_1,att_2,…,att_{n1}}
-위임속성값 집합:D_ATT={D_att_1,D_att_2,…}
-크레덴셜 집합:CREDENTIAL={{credential_role}∨{credential_Drole}|role∈ROLE,Drole∈D_ROLE}
F_{CRE}(role, $condition_{CRE}$) → credential_role
F_{CRE}(Drole, $condition_D$) → credential_Drole
-사용자-역할 맵핑:UA⊆USER×ROLE
UA={∪〈$user_x$,$role_y$,($condition_{CRE}$)〉| $user_x$∈USER, $role_y$∈ROLE}
-역할-퍼미션 맵핑:PA⊆ROLE×PERM
PA={∪〈$role_x$, $perm_y$, condition_P〉|role∈ROLE, $perm_y$∈PERM}
-시스템 내 역할-퍼미션 맵핑:PA_S ⊆ PA
-사용자-역할:
Assigned_users(role)→{user}⊆USER
-역할-퍼미션:
Assigned_permessions(role)→{perm}⊆PERM

3.2 권한 활성화 제약(constraint)

SG-RBAC 모델은 사용자 특성과 역할 특성에 따라 사용자의 위치정보, 시간, 주기 등을 고려하여 접근권환 활성화에 제약을 가할 수 있으며 크게 세 가지 제약으로 구분할 수 있다〔그림 2〕. 본 장에서는 사용자-역할 맵핑에 적용되는 사용자 특성에 따른 제약방식, 역할-퍼미션 맵핑에 적용되는 역할 특성에 따른 제약방식, 시스템 관리자에 의해 관리되는 시스템 특성에 따른 제약방식을 제안한다. 또한 각각의 제약방식이 적용 가능한 시나리오를 제시한다.



〔그림 2〕 SG-RBAC 권한 활성화 제약

3.2.1 주기, 시간, 위치 정보의 표현

SG-RBAC 모델은 접근권환 활성화 제약 시 사용자의 주기, 시간, 위치정보를 고려한다. 사용자의 주기, 시간, 위치정보를 제약에 사용되는 조건으로 만들기 위해 수식적으로 표현 할 수 있어야 한다.

□ 주기 표현
〔19〕에서 제안된 방식을 단순화하여 사용하며, 주기는 다음과 같이 표현할 수 있다.

$$P = O_i \cdot C_i, \quad C_i \subseteq C_{i-1} \qquad (1)$$

C_i는 년, 월, 주를 표현하며 Y, M, W로 표시한다.
· C_i = {Y, M, W}
O_i는 C_i와 함께 사용되며 아래와 같이 특정 기간을 나타낼 수 있다.
· O_1 = all,
· C_i = Y 일 때, O_i = n (현재 년도부터 +n 년도 까지)
· C_i = M 일 때, 1≤O_i≤12, (O_i=1, 1월)
· C_i = W 일 때, 1≤O_i≤7, (O_i=1, 월요일)

예를 들어 주기가 P = 3·Y + All·M + {1,2,3,4,5}·W 일 경우, 현재 시점인 13년도부터 16년도 12월까지 매월 평일이 해당 주기가 된다.

□ 시간 표현

t_begin은 시작시간, t_end는 종료시간, P는 주기를 나타내며 시간구간은 다음과 같이 표현한다.

$$T = \langle [t\_begin, t\_end], P \rangle \quad (2)$$

예를 들어, 시간이 T = 〈[09:00, 18:00], [3·Y + All·M + {1,2,3,4,5}·W]〉 일 경우 현재 시점인 13년도부터 16년도 12월까지 평일 09:00부터 18:00까지 가 해당 시간이 된다.

□ 위치 정보 표현

위치정보는 다음과 같이 표현된다.

$$L = \sum_{i=1}^{n} P_i \cdot S_i \quad (3)$$

P_i는 명칭을 나타내며 S_i는 시, 구, 동, 번지 등의 단위를 나타낸다.

S_i={시, 구, 동, 번지, … }

예를 들어, L={대전·시+유성·구+전민·동+123·번지} 일 경우 대전시 유성구 전민동 123번지를 의미한다.

3.2.2 사용자 특성에 따른 권한 제약

UR 관리자는 사용자를 식별 및 인증하고, [정의 1]의 방식으로 크래덴셜을 발급하여 정당한 사용자에게 적절한 역할을 부여한다. 특정 시스템의 객체에 접근하려는 주체는 유효한 크래덴셜을 시스템 관리자에게 제시하여 주체가 객체 접근에 대한 퍼미션이 부여된 역할을 수행하고 있음을 증명해야 한다.

정의 1. 크래덴셜(credential) 사용

UR관리자는 사용자를 인증한 뒤 사용자의 속성에 맡는 역할을 확인하고 크랜덴셜을 생성하여 사용자에게 부여한다. UR 관리자는 (role, $condition_{CRE}$) 또는 (Drole, $condition_D$)를 반영하여 크래덴셜을 생성한다.

F_{CRE}(role,$condition_{CRE}$)→credential_role

F_{CRE}(Drole,$condition_D$)→credential_Drole □

UR 관리자는 사용자에게 역할을 부여할 때 사용자의 특성에 따라 크래덴셜 유효조건을 설정하여 객체 접근에 다양한 제약을 가할 수 있다. 크랜덴셜 유효조건은 사용자가 역할을 사용하는 시간이나 사용자의 위치정보에 따라 크래덴셜 활성화를 제한하며 [정의 2]와 같이 표현된다.

정의 2. 사용자특성에 따른 제약($condition_{CRE}$) 표현

사용자-역할 맵핑은 UR 관리자에 의해 관리되며 다음과 같은 형식을 가진다.

사용자-역할 맵핑 : UA ⊆ USER × ROLE

UA={∪〈$user_x$,$role_y$,$condition_{CRE}$〉|$user_x$∈USER,$role_y$∈ROLE }

UR 관리자는 사용자-역할 맵핑에 크래덴셜 유효조건($condition_{CRE}$)을 추가하여 사용자의 특성에 따라 크래덴셜의 활성화를 제한한다. 사용자가 역할을 사용하는 시간(T)이나 사용자의 위치정보(L)에 따라 크래덴셜 활성화를 제한하고 크래덴셜 유효기간(Expiration Time, ET)을 설정하여 발급된 크래덴셜의 사용 기한을 설정한다.

$condition_{CRE}$ = 〈T, L, ET〉,

T = 〈[t_begin, t_end], P〉

$$L = \sum_{i=1}^{n} P_i \cdot S_i \ , \ ET = \langle t\_begin, t\_end \rangle$$

ua = 〈$user_x$, $role_y$, $condition_{CRE\_y}$〉

ua∈UA, 1≤x≤n1, 1≤y≤n2 □

시나리오 1. 지역A에 스마트미터를 설치한 사업자(UA 관리자)는 $user_1$에게 스마트미터 점검원($role_1$)의 역할을 부여하고 오전 근무시간에 지역A에 설치된 스마트미터에 접근을 허가하는 크래덴셜을 부여한다고 가정하자. SG-RBAC 모델에서는 다음의 과정을 통해 제약이 이루어진다.

1. UA 관리자가 사용자($user_1$)가 정당한 사용자인지 확인한다.
2. UA 관리자는 사용자-역할 맵핑테이블에서 $user_1$이 포함된 행을 [표 2]와 같이 수정한다.

[표 2] 사용자-역할 맵핑 테이블

User	Role	크래덴셜 유효조건 ($condition_{CRE}$)		
		T	L	ET
$user_1$	$role_1$	9:00,18:00	지역A	1일
$user_2$	$role_2$	-	지역B	2달
$user_3$	$role_3$	-	지역C	1일

3. UA 관리자는 사용자에게 점검자 역할($role_1$)을 부여하고, F_{CRE} 함수를 통해 역할과 크래덴셜유효조건에 대한 크래덴셜($credential_{role\_1}$)을 발급한다.

3.2.3 역할 특성에 따른 권한 제약

RP 관리자는 역할에 퍼미션을 부여할 때 역할의 특성에 따라 역할유효조건을 설정하여 객체 접근에 다양한 제약을 가할 수 있다. 역할의 특성에 따라 특정 객체에 접근시 정해진 시간 안에 또는 특정 위치 안에서만 접근권한이 필요할 수 있다. 이러한 경우에는 역할유효조건에 해당 시간 또는 위치를 적용하여 역할이 특정시간과 위치에서만 퍼미션이 활성화되어 접근권한을 사용할 수 있도록 한다. 즉 사용자는 UR 관리자로부터 부여받은 역할을 통해 특정 퍼미션을 가지게 되지만 퍼미션 유효조건에 적합한 상황에서만 퍼미션이 활성화되어 특정 객체에 접근이 허용된다. 퍼미션 유효조건은 퍼미션 사용자가 퍼미션을 사용하는 시간이나 사용자의 위치정보에 따라 퍼미션의 활성화를 제한하고 위기상황이 발생하면 퍼미션을 비활성화시키도록 하는 이벤트 항목을 추가할 수 있으며 〔정의 3〕과 같이 표현된다.

정의 3. 역할 특성에 따른 제약($condition_P$) 표현

역할-퍼미션 맵핑은 RP 관리자에 의해 관리되며 다음과 같은 형식을 가진다.

역할-퍼미션 맵핑:$PA \subseteq ROLE \times PERM$

$PA = \{ \cup\langle role_x, perm_y, condition_P\rangle \mid role_x \in ROLE, perm_y \in PERM \}$

RP 관리자는 역할-퍼미션 맵핑에 $condition_P$을 추가하여 사용자 특성에 상관없이 역할의 특성에 따라 퍼미션 사용을 제한한다. 즉 특정 역할이 퍼미션을 사용하는 시간이나 위치정보, 위기상황이 발생여부에 따라 역할이 가진 퍼미션의 활성화를 제한하고 다음과 같이 표현된다.

$condition_P = \langle T, L, event\rangle$

$T = \langle [t\_begin, t\_end], P\rangle$, $L = \sum_{i=1}^{n} P_i \cdot S_i$, $EVENT = \bigcirc$ or $\times$

$pa = \langle role_y, perm_z, condition_{Py}\rangle$,

$pa \in PA,\ 1 \le y \le n_2,\ 1 \le z \le n_3$ □

시스템은 객체에 접근하려는 사용자가 객체에 대한 접근권한(퍼미션)이 있는 역할을 수행하고 있는지 여부를 확인하여야 한다. 하나의 도메인 내에 다수의 시스템이 존재할 수 있으며 각 시스템 관리자들은 시스템 내 객체들에 대한 역할-퍼미션 맵핑 테이블을 관리하고 RP관리자로부터 실시간으로 테이블을 업데이트 할 수 있어야 한다. (역할-퍼미션 맵핑에 수정이 발생할 경우, RP 관리자가 해당 시스템 관리자에게 실시간으로 알려주어 시스템에 반영하는 방법과 시스템들이 각자 주기적으로 RP관리자에게 쿼리메시지를 보내어 맵핑테이블을 업데이트하는 방법이 있다.) 사용자가 특정 시스템의 객체에 접근할 경우, 시스템은 사용자의 역할 크래덴셜의 유효여부를 확인하고 현재 퍼미션 유효조건을 만족하는지 확인하게 된다.

시나리오 2. RP 관리자는 전력위기상황에서 전력제어 및 복구와 관련된 역할들이 원활히 수행될 수 있도록 부가서비스와 관련된 역할들은 비활성화되도록 설정한다고 가정하자. SG-RBAC 모델에서는 〔표 3〕과 같이 역할-퍼미션 맵핑테이블에 퍼미션 유효조건을 추가하여 제약이 가능하다.

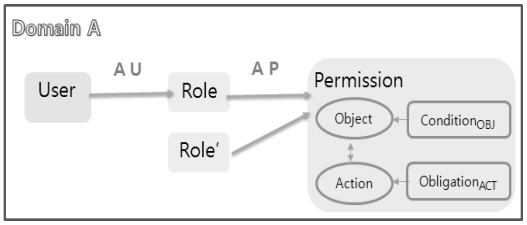
〔표 3〕 역할-퍼미션 맵핑 테이블

역할 role	퍼미션유효조건 ($condition_P$)			퍼미션 (객체-접근방법)
	T	L	EVENT	
부가서비스 관련 역할	9:00, 18:00	지역 A	위기상황 발생시 disable	object1-action1
제어 관련 역할	12:00, 14:00	지역 B	-	object2-action2

3.2.4 시스템 특성에 따른 권한 제약

일반적으로 접근권한 제약은 UR 관리자가 사용자-역할 맵핑에서 적용하는 크래덴셜 유효조건과 RP 관리자가 역할-퍼미션 맵핑에 적용하는 퍼미션 유효조건을 통해 발생된다. 하지만 스마트그리드에 적용되는 다양한 시스템들은 서로 다른 시스템 환경과 특성을 가지므로 각 시스템 관리자들이 시스템 특성에 따라 사용자의 객체접근에 추가적인 제한을 가할 수 있어야 한다. 따라서 각 시스템마다 객체접근조건($condition_{OBJ}$)과 의무사항($obligation_{ACT}$)〔18〕을 이용하여 시스템 관리자들로 하여금 객체접근에 대한 추가적인 제한을 가할 수 있도록 한다〔그림 3〕.

- 객체접근조건 ($condition_{OBJ}$): 시스템 관리자는 자신이 관리하는 다양한 자원 즉 객체에 $condition_{OBJ}$를 생성하여 주체가 특정 객체에 접근시 $condition_{OBJ}$을 만족하는지 확인하여 접근허가를 결정할 수 있다.
- 의무사항 ($obligation_{ACT}$): 시스템은 자신이 포함하는 다양한 객체의 접근방법에 의무사항($obligation_{ACT}$)를 추가하여 주체가 특정 객체에 접근 후 수행해야할 의무 행동들을 정할 수 있다.



〔그림 3〕 객체접근조건과 의무사항을 이용한 권한 제약

시나리오 3. 사용자가 개인정보관리시스템의 데이터베이스에 저장된 개인정보에 접근(read)하려고 할 때, 개인정보관리시스템이 사용자의 역할과 크래덴셜을 확인하고 추가적으로 주체의 ID를 요구하는 과정이 필요하다고 가정하자. SG-RBAC 모델에서는 개인정보관리시스템이 데이터베이스에 접근하려는 주체에게 ID를 확인하는 객체접근조건을 생성하고 있다. 사용자가 데이터베이스에 접근(read)이 가능한 역할을 가지고 있고 크래덴셜 유효조건과 퍼미션 유효조건을 만족하고 있을지라도, 추가적으로 주체의 ID와 같은 식별정보를 요구하여 개인정보관리시스템에서 미리 인증된 사용자인지 확인할 수 있다.

3.3 객체 접근제어 방법

스마트그리드 환경에서는 다양한 사업자가 참여하여 서비스 형태에 따라 여러 종류의 시스템들을 사용하며, 타 도메인의 객체에 접근이 필요한 상황이 발생하게 된다. 이에 따라, 본 장에서는 SG-RBAC 모델에서 사용자가 객체에 접근하기 위해 객체를 관리하는 시스템 관리자와 수행하는 일련의 절차를 동일 도메인 내 접근방법과 타 도메인 간 접근방법으로 나누어 기술하였다.

3.3.1 동일 도메인 내 객체 접근방법

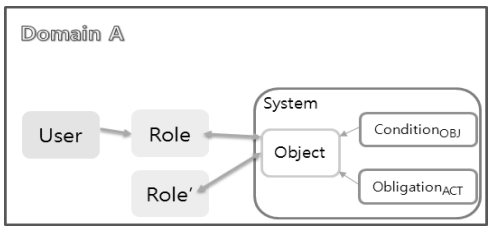
동일 도메인 상에서 사용자가 시스템의 객체에 접근하는 방법은 다음과 같다.

1. 사용자는 동일 도메인 내 시스템의 객체에 접근하기 위해 역할과 크래덴셜($credential_{role}$)을 시스템에 전송
2. 시스템 관리자는
   · 크래덴셜을 검증하여 사용자가 제시한 역할을 수행할 수 있는 정당한 사용자인지 확인
   · 시스템이 관리하는 역할-퍼미션 맵핑 테이블을 통해 사용자가 제시한 역할이 접근하고자 하는 객체에 어떠한 접근방법(퍼미션)이 있는지 확인
   · 크래덴셜 유효조건과 퍼미션 유효조건을 확인하여 현재 사용자 역할의 활성화 여부를 확인
   · 객체에 객체접근조건($condition_{OBJ}$)이 있을 경우에는 시스템 관리자는 사용자에게 조건 항목을 제시하고 응답을 기다림

(3.) 사용자는 조건 항목에 대한 응답을 시스템 관리자에게 전송

4. 시스템 관리자는
   · 사용자에게 객체 접근을 허가
   · 객체에 의무사항($obligation_{ACT}$) 항목이 있을 경우 의무사항을 사용자에게 전달

(5.) 사용자는 의무사항을 수행



〔그림 4〕 동일 도메인 내 객체 접근

3.3.2 타 도메인 간 객체 접근방법

스마트그리드와 같은 다중 도메인 환경에서는 서로 다른 도메인 사이에서 접근제어가 필요하다. 이를 위해 SG-RBAC 모델은 사용자 인증을 위한 별도의 인증기관(CA)을 사용하여 타 도메인 간 객체 접근시에 별도의 인증절차를 추가하고 인증받은 사용자에 한하

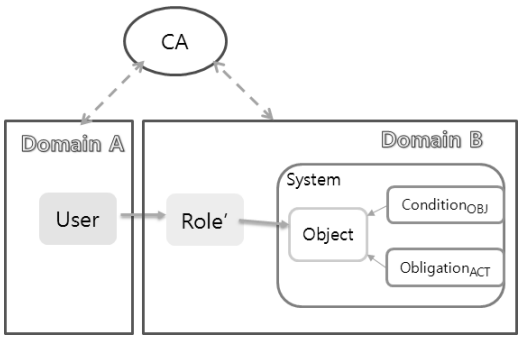
여 타 도메인 간 객체 접근을 허용한다. 타 도메인 간에 사용자가 시스템의 객체에 접근하는 방법은 다음과 같다.

1. 사용자는 인증기관(CA)으로부터 타도메인접근역할, 크래덴셜($credential_{role}$), 신상정보에 대한 인증서(certificate)를 발급받는다.
2. 사용자는 타 도메인 내 시스템의 객체에 접근하기 위해 타도메인접근역할, 크래덴셜, 인증서를 시스템에 전송
3. 시스템 관리자는
- 인증서를 검증하여 사용자가 제시한 타도메인 접근역할과 크래덴셜이 유효한지 확인
- 도메인 또는 사업자 내부 규정에 따라 사용자가 역할을 수행할 자격이 있는지 확인
- 시스템이 관리하는 역할-퍼미션 맵핑 테이블을 통해 사용자가 제시한 역할이 접근하고자 하는 객체에 어떠한 접근방법(퍼미션)이 있는지 확인
- 퍼미션 유효조건($condition_P$)을 확인하여 현재 사용자 퍼미션의 활성화 여부를 확인
- 객체에 객체접근조건($condition_{OBJ}$)이 있을 경우 시스템 관리자는 사용자에게 조건 항목을 제시하고 응답을 기다림

(4.) 사용자는 조건 항목에 대한 응답을 시스템 관리자에게 전송

5. 시스템 관리자는
- 사용자에게 객체 접근을 허가
- 객체에 의무사항($obligation_{ACT}$) 항목이 있을 경우 의무사항을 사용자에게 전달

(6.) 사용자는 의무사항을 수행



〔그림 5〕 타 도메인간 객체 접근

3.4 권한위임 방법

실제 사용자가 시스템을 통해 업무를 수행하면서 다른 사용자에게 권한의 일부를 위임해야 하는 상황이 발생할 수 있다. 하지만 무분별한 권한위임은 보안상 심각한 위협으로 작용될 수 있으므로 권한위임에 제한을 두어야만 한다. SG-RBAC 모델은 위임속성값을 이용하여 권한위임과 권한위임제한을 수행한다.

3.4.1 권한위임 방법

사용자는 시스템에 로그인하는 과정에서 자신의 속성값을 UR관리자에게 전송하여 속성에 맞는 역할을 부여받게 된다. 사용자는 자신에게 부여된 역할 중 위임가능한 역할(role∈ROLE*)을 다른 사용자에게 위임할 수 있으며 〔정의 4〕와 같이 표현된다.

정의 4. 권한위임 표현

모든 사용자는 유일한 속성값(att)을 가지며, 속성값은 사용자와 관리자만이 알고 있는 값이다. 사용자는 자신의 속성값을 이용하여 위임속성값 (D_att∈D_ATT)을 생성하고 자신에게 부여된 역할 중 위임가능한 역할(role∈ROLE*)을 다른 사용자에게 위임할 수 있다. 위임 속성값은 사용자 속성값과 위임하려는 역할, 위임 조건값의 해시연산을 통해 구하게 된다. 사용자 A가 역할 role*을 위임하기위한 위임 속성값은 다음과 같다.

$D\_att_A(role^* \wedge condition_D) = hash(att\_A || role^* || condition_D)$,

$role^* \in ROLE_A \wedge role^* \in ROLE^*$

$role^* \rightarrow Drole$ □

시나리오 4. 〔표 4〕는 위임이 일어나지 않은 상태의 사용자-역할 맵핑 테이블의 일부분이며 〔표 5〕는 위임이 발생한 후의 사용자-역할 맵핑 테이블이다. 사용자 A는 자신의 역할 중 $role_2$*만을 사용자B에게 위임하고자 한다고 가정하자(* 기호는 위임가능한 역할을 나타낸다. role* ∈ ROLE*). SG-RBAC에서 사용자 A는 위임 속성값(D_att_A)을 생성하고 사용자B에게 전송한다. 이후 사용자는 사용자A의 $role_2$ 역할이 필요할 경우 사용자의 A로부터 받은 위임속성값을 이용하여 UR 관리자에게 역할을 부여받을 수 있게 된다. 따라서 사용자 A의 권한 일부가 사용자 B에게 일정시간동안 위임될 수 있다.

〔표 4〕 위임 전 사용자-역할 맵핑 테이블

사용자	사용자속성값	역할
A	att_A	$role_1$, $role_2^*$
B	att_B	$role_3$, $role_4^*$
C	att_C	$role_2^*$, $role_5$

〔표 5〕 위임 후 사용자-역할 맵핑 테이블

사용자	사용자 속성값	위임속성값 (역할,조건)	역할
A	att_A	-	$role_1$, $role_2^*$
B	att_B	$D\_att_A(role_2^* \wedge condition_D)$	$role_3$, $role_4^*$, $Drole_2$
C	att_C	$D\_att_B(role_4^* \wedge condition_D)$	$role_2^*$, $role_5$, $Drole_4$

3.4.2 권한위임 제한

무분별한 권한위임은 보안상 심각한 위협이 될 수 있으므로 권한위임에 제한을 두어야만 한다. SG-RBAC 모델은 권한 위임이 발생하는 과정에서 위임속성값에 포함된 조건을 이용하여 위임속성값의 유효기간, 사용자의 시간, 위치정보에 따른 다양한 제한을 가할 수 있게 되며, 이벤트 조건을 추가하여 전력수급상 위기 상황이 발생할 경우 각 상황을 예외적으로 처리하여 해당 담당자가 없더라도 위임된 권한이 활성화되어 필요한 기능을 수행할 수 있도록 한다. 또한 역할 계층이 서로 다른 사용자에게 각각 다른 역할을 위임할 수 있게 된다. SG-RBAC 모델에서 권한 위임 제약은 다음과 같이 표현된다.

정의 5. 권한위임 제약 표현

사용자는 위임속성값에 $condition_D$를 추가하여 위임된 역할의 사용을 제한한다.

$condition_D = \langle T, L, ET, event \rangle$

$T = \langle [t\_begin, t\_end], P \rangle$, $L = \sum_{i=1}^{n} P_i \cdot S_i$ $ET = \langle t\_begin, t\_end \rangle$, event = ○ or ×

$D\_att_A(role^* \wedge condition_D) = hash(att_A || role^* || condition_D)$ □

시나리오 5. 정의 4와 정의 5의 권한위임과 제한 방식에 따라 사용자 C가 사용자 B로부터 위임받은 역할에 대한 퍼미션을 사용하는 과정은 다음과 같다.

1. 사용자 B는 role에 대한 D_att_B를 생성
2. 사용자 B는 D_att_B, role 명칭, $condition_D$를 사용자 C에게 전송
3. 사용자 C는 역할 role를 사용해야 할 경우, D_att_B와 $condition_D$를 UR관리자에게 전달
4. UR관리자는 role ∈ ROLE* 이고 D_att_B가 정당한 값인지 확인
5. UR관리자는 D_att_B가 정당한 값일 경우, 위임된 role임을 나타내는 Drole과 $condition_D$를 반영한 credential_Drole을 생성하여 사용자 C에게 부여하고 위임 상태를 기록
6. 사용자 C는 credential_Drole을 이용하여 $condition_D$를 만족하는 상태에 한하여 제한적으로 Drole의 퍼미션을 이용

3.4.3 다양한 권한위임 방법

다양한 권한위임 방법을 제공하여 사용자에게 편의를 제공하면서 동시에 필요한 권한만 세분화하여 위임할 수 있도록 하여 직무분리를 제공한다. 제안된 위임 방법은 사용자간에 위임속성값을 전송하여 사용자간 위임을 제공하고, 여러 사용자에게 동일한 위임속성값을 브로드캐스트(broadcast) 방식으로 전송하여 다중 위임이 가능하다. 역할 간 위임을 위해 RP 관리자가 R_2^*의 퍼미션을 R_1에 추가하는 방법으로 R_2^*역할을 R_1역할에 위임 할 수 있으나 위임 시 조건(condition)을 적용하는데 어려움이 있다.

3.5 권한 상속 제한

역할계층을 사용하는 RBAC에서는 상위 계층 역할이 하위 계층 역할의 퍼미션을 상속받게 된다. 이때 모든 역할의 퍼미션이 역할계층의 레벨에 따라 상속될 경우 상위 계층 역할을 부여받은 사용자에게 필요이상의 객체접근이 허용될 수 있으므로 상속제한조건을 사용하여 상속이 부분적으로 일어나도록 제한할 수 있다.

정의 7. 상속 제약 표현

UR 관리자는 역할에 상속제한조건($condition_I$)을 추가하여 특정 유효시간과 역할계층 레벨까지만 역할이 상속되도록 제한하며, 상속제한조건과 역할은 각각 다음과 같이 표현된다.

$condition_I$={T, LEVEL},
T=〈{t_begin, t_end}, P〉,
Level={n|n∈N∧1 ≤n≤ depth(RH)}
$role_A$=〈{$role_x$},{$Irole_y$||$condition_I$}〉,
$role_x$, $role_y$∈ROLE

T는 사용자 A의 역할중 상속가능한 역할(Irole)이 활성화 될 수 있는 시간으로 t_begin부터 t_end 이내의 시간에만 상위레벨의 역할이 Irole 역할을 사용할 수 있도록 제한한다. LEVEL 은 Irole이 상속될 수 있는 상위레벨의 수를 나타낸다. □

IV. 결 론

본 논문은 스마트그리드 환경을 분석하여 접근제어 요구사항들을 정리하고 제안한 요구사항들을 모두 만족하는 SG-RBAC 모델을 제안하였다. 기존 모델〔11,12,13,14,15,16,17,18〕들은 요구사항의 일부만을 만족하고 있다. SG-RBAC 모델은 GTRBAC〔11,12,13〕의 시간에 따른 권한활성화 제약 특성과 PRBAC〔17,18〕의 조건·의무 개념을 동시에 가지며, 다양한 권한 활성화 제약 방식과 권한 위임 방식을 가진다. SG-RBAC 모델은 사용자 특성, 역할 특성, 시스템 특성에 따라 권한 활성화 제약이 가능하며, 인증기관을 이용하여 타 도메인 간 객체 접근이 가능하다. 또한 다양한 권한위임방법을 가지며 권한위임과 권한 상속 시 제약이 가능하다. 이러한 다양한 제약방법은 문서로 정의된 접근제어 정책을 실제 시스템에 유연하게 반영하고 불필요한 권한 활성화, 권한 위임, 권한 상속이 발생하지 않도록 하여 직무분할의 요구사항을 만족시킨다. 본 논문에서 제안한 SG-RBAC 모델은 향후 스마트그리드 접근제어 시스템 개발에 활용 가능할 것으로 기대된다.

참고문헌

〔1〕 Elisa Bertino, Sushil Jajodia, Pierangela Samarati, "Enforcing Mandatory Access Control in Object Bases," Security for Object-Oriented Systems, pp. 96-116, Sep. 1993.

〔2〕 Matunda Nyanchama, Sylvia L. Osborn, "Modeling Mandatory Access Control in Role-Based Security Systems," DBSec, pp. 129-144, Aug. 1995.

〔3〕 Lindqvist, H. Mandatory access control. Master's thesis, Umea University, Sweden, 2006. http://www.cs.umu.se/education/examina/Rapporter/HakanLindqvist.pdf.

〔4〕 Klaus R. Dittrich, Martin Hartig, Heribert Pfefferle "Discretionary Access Control in Structurally Object-Oriented Database Systems," DBSec, pp. 105-121, Oct. 1988.

〔5〕 Jonathan D. Moffett, Morris Sloman, Kevin P. Twidle, "Specifying discretionary access control policy for distributed systems," Computer Communications (COMCOM), vol. 13, no. 9, pp. 571-580, Nov. 1990.

〔6〕 Elisa Bertino, Claudio Bettini, Pierangela Samarati, "A discretionary access control model with temporal authorizations," NSPW, pp. 102-107, Aug. 1994.

〔7〕 D. Ferraiolo and R. Kuhn, "Role-Based Access Controls," Proc. 15th NIST-NCSC National Computer Security Conf., pp. 554-563, Oct. 1992.

〔8〕 Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, Charles E. Youman, "Role-Based Access Control Models," IEEE Computer(COMPUTER) vol. 29, no. 2, pp. 38-47, Feb. 1996.

〔9〕 David F. Ferraiolo, Ravi S. Sandhu, Serban I. Gavrila, D. Richard Kuhn, Ramaswamy Chandramouli, "Proposed NIST standard for role-based access control," ACM Trans. Inf. Syst. Secur. (TISSEC), vol. 4, no. 3, pp. 224-274, Aug. 2001.

〔10〕 Jaime A. Pavlich-Mariscal, Laurent Michel, Steven A. Demurjian, "A Formal Enforcement Framework for Role-Based Access Control Using Aspect-Oriented Programming," MoDELS, pp. 537-552, Oct. 2005.

〔11〕 Elisa Bertino, Piero A. Bonatti, Elena

Ferrari, "TRBAC: A temporal role-based access control model. ACM Trans," Inf. Syst. Secur. (TISSEC), vol. 4, no. 3, pp. 191-233, Aug. 2001.

〔12〕 James Joshi, Elisa Bertino, Arif Ghafoor, "Hybrid Role Hierarchy for Generalized Temporal Role Based Access Control Model," COMPSAC, pp. 951-956, Aug. 2002.

〔13〕 James Joshi, Elisa Bertino, Usman Latif, Arif Ghafoor, "A Generalized Temporal Role-Based Access Control Model." IEEE Trans. Knowl. Data Eng. (TKDE), vol. 17, no. 1, pp. 4-23, Jan. 2005.

〔14〕 Chang N. Zhang, Cungang Yang, "Designing a Complete Model of Role-based Access Control System for Distributed Networks," J. Inf. Sci. Eng. (JISE), vol. 18, no. 6, pp. 871-889, Nov. 2002.

〔15〕 Eric Freudenthal, Tracy Pesin, Lawrence Port, Edward Keenan, Vijay Karamcheti, "dRBAC: Distributed Role-based Access Control for Dynamic Coalition Environments," ICDCS, pp. 411-420, Jul. 2002.

〔16〕 Songyun Liu, Hejiao Huang, "Role-Based Access Control for Distributed Cooperation Environment," CIS, pp. 455-459, Dec. 2009.

〔17〕 Anour F. A. Dafa-Alla, Eun Hee Kim, Keun Ho Ryu, Yong Jun Heo, "PRBAC: An Extended Role Based Access Control for Privacy Preserving Data Mining," ACIS-ICIS, pp. 68-73, Jul. 2005.

〔18〕 Qun Ni, Elisa Bertino, Jorge Lobo, Seraphin B. Calo, "Privacy-Aware Role-Based Access Control," IEEE Security & Privacy (IEEESP), vol. 7, no. 4, pp. 35-43, Jul. 2009.

〔19〕 Elisa Bertino, Claudio Bettini, Elena Ferrari, Pierangela Samarati, "An Access Control Model Supporting Periodicity Constraints and Temporal Reasoning," ACM Trans. Database Syst. (TODS), vol. 23, no. 3, pp. 231-285, Sep. 1998.

〈著者紹介〉

사 진

이 우 묘 (Woomyo Lee) 정회원
2010년 2월: 경북대학교 전자전기컴퓨터학부 졸업
2012년 2월: 포항공과대학교 전자공학과 석사
2011년 12월~현재: ETRI 부설연구소 연구원
〈관심분야〉 정보보호, 스마트그리드 보안, 제어시스템 보안, 네트워크 암호화 및 인증

사 진

이 건 희 (Gunhee Lee) 정회원
2001년 2월: 아주대학교 정보및컴퓨터공학부 졸업
2003년 2월: 아주대학교 정보통신 전문대학원 정보통신공학과 석사
2009년 2월: 아주대학교 정보통신 전문대학원 정보통신학과 공학박사
2009년 3월~현재: ETRI 부설연구소 선임연구원
〈관심분야〉 스마트그리드 보안, 제어시스템 보안, 유무선 네트워크 인증 및 키관리

사 진

김 신 규 (Sinkyu Kim) 정회원
2000년 2월: 연세대학교 기계전자공학부 졸업
2002년 2월: 연세대학교 컴퓨터과학과 석사
2007년 8월: 연세대학교 컴퓨터과학과 박사수료
2003년 12월~현재: ETRI 부설연구소 선임연구원/스마트그리드보안팀장
〈관심분야〉 스마트그리드 보안, 국가기반시설 보안, 취약점 분석

사 진

서 정 택 (Jungtaek Seo) 종신회원
1999년 2월: 충주대학교 컴퓨터공학과 졸업
2001년 2월: 아주대학교 컴퓨터공학화 석사
2006년 2월: 고려대학교 정보보호대학원 정보보호공학 공학박사
2000년 11월~현재: ETRI 부설연구소 선임연구원/스마트그리드보안연구실장
2011년 11월~현재: 고려대학교 정보보호대학원 겸임교수
〈관심분야〉 스마트그리드 보안, 제어시스템 보안, 원자력 사이버 보안, 취약성 분석평가, DDoS 공격 탐지 및 대응