RBAC 기반의 UI 컴포넌트 권한 관리

김원종*
*고려대학교 컴퓨터 정보통신대학원 디지털정보 미디어공학과
Email : innrang@gmail.com

Permission Management of UI Components based on RBAC

Won-Jong Kim*
Dept. of Digital Information and Media , Korea University

요 약

많은 기업들이 전사적인 사용자 권한을 관리하기 위해 통합 사용자 권한관리 솔루션을 도입하고 있으며, 이를 통해 외부 사용자의 접근제어, 사용자 인증, 사용자 권한에 대한 효율적인 관리를 추구하고 있다. 그러나, 이러한 권한 관리의 중심이 시스템 별 사용자를 분류하고 사용자의 그룹을 분류하는 사용자 위주로 진행되고 있다. 즉, 사용자가 사용하는 기업의 정보시스템에 해당하는 업무시스템의 구성요소(이를 테면 화면 및 화면의 구성요소인 UI 컴포넌트 등)의 권한 관리를 위한 연구는 상대적으로 이루어지지 않고 있다. 따라서 본 논문에서는 기업 내 정보시스템의 최소 단위로 볼 수 있는 화면 및 UI 컴포넌트에 대한 접근 권한을 효율적으로 관리할 수 있는 모델을 제안한다.

1. 서론

기업 내/외부 정보시스템의 다양한 채널(PC, 스마트폰, 태블릿 등)에서의 사용이 확대되고 있으며 이에 따라 사용자 관리의 복잡성 또한 증대되고 있다. 이에 사용자의 권한에 대한 인가체계(Authorization)수립을 추진하는 경향이 증가하고 있으며, 사용자의 권한을 통합적으로 관리하는 툴의 도입이 확산되고 있다. 이러한 사용자 권한체계를 구현하기 위한 대표적인 솔루션으로는 EAM 을 들 수 있다.

통합 사용자 권한 관리란 전사 시스템의 사용자 정보에 대한 접근을 제어하고 일관된 정책으로 권한관리를 하고자 하는 것이다. 이를 구현하고 활용할 수 있는 방법으로 RBAC(Role-Based Access Control)개념이 있으며, RBAC 체계는 사용자의 역할을 기준으로 접근 권한을 형성 및 관리하기 때문에 관리의 용이성을 확보하고 복잡하지 않는 관리 체계를 제공하는 장점을 제공한다. 기업에서 도입하고 있는 솔루션 또한 RBAC 의 기본 개념을 도입 활용하고 있다. 그러나, 이러한 권한 관리의 연구 중심이 시스템 별 사용자를 분류하고 사용자의 그룹(Group)을 분류하는 사용자 위주로 진행되고 있다. 즉, 사용자가 사용하는 기업의 정보시스템에 해당하는 업무시스템의 구성요소(이를 테면 화면 및 화면의 구성요소인 UI Component 등)의 권한 관리를 위한 연구는 상대적으로 이루어지지 않고 있다.

실제 업무시스템 설계 시 해당 화면의 구성요소들에 대해 사용자 별로 어떻게 보여줘야 하는지, 버튼(Button)은 누구에게만 활성화 되야 하는지 등에 대한 요구사항이 항상 존재하게 된다. 따라서, 효율적이고 복잡하지 않으며 최소한의 관리 체계를 가질 수 있는 화면 및 UI Component 에 대한 권한 관리 방법이 필요하다. 이에 본 논문에서는 기업 내 업무처리시스템의 화면에 접근하고자 하는 사용자의 접근권한을 미리 설정된 보안정책에 따라 판단하여 해당 사용자가 가진 권한에 따라 화면 및 화면의 구성요소(UI Component)에 대한 접근 범위를 결정하여 화면을 구성하는 각각의 구성요소에 대한 수준별 접근제어를 수행하는 방법을 제시한다. 본 논문의 전체적인 구성은 다음과 같다. 서론에서 연구의 목적 및 필요성을 간략하게 서술하고, 2 절에서 RBAC 모델과 구성요소에 대해 살펴보고, 통합 사용자 권한 관리 솔루션의 동향에 대해 소개한다. 3 절에서는 본 논문에서 제한하는 화면 및 화면 구성요소의 접근제어 모델에 대해 서술한다. 마지막으로 4 절에서는 결론 및 향후 연구과제에 대해 서술한다.

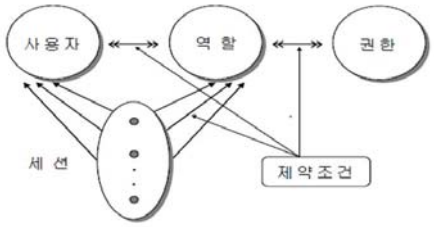
2. 관련 연구

2-1. RBAC 모델

RBAC 의 중심 개념은 사용자가 기업이나 조직의 객체에 임의적인 접근을 하지 못하도록 하는 것이다. 대신에 접근권한은 역할과 연관되고 사용자는 적절한 역할의 구성원이 된다.[1]. 즉, RBAC 을 사용한 접근제어에서 접근 결정은 개인 사용자들의 조직의 부분으로서 가지는 역할에 기반을 두고 있다.[2,3]

기능적인 측면에서 RBAC 의 중심 개념은 역할, 역할의 구성원인 사용자, 그리고 연관된 행동을 나타내는

권한(Permission)이다. [그림 1]은 RBAC 구성요소의 관계를 표현하고 있으며, 두 개의 화살표가 의미하는 것은 한 명의 사용자가 하나 혹은 그 이상의 역할과 연관될 수 있고 하나의 역할은 하나 혹은 그 이상의 사용자 구성원을 가질 수 있다는 것을 의미한다. 역할과 권한도 동일한 관계를 가질 수 있다.[4]



[그림 1] 역할기반 접근제어 모델

사용자가 객체에 대해 수행할 수 있는 권한을 직접 사용자에게 부여하지 않고 대신 조직의 업무 수행에 필요한 역할에 부여하였다. 이를 통해서 사용자를 쉽게 역할에 추가하거나 제거할 수 있고, 역할 또한 권한과만 관련이 있으므로 사용자에게 할당된 업무의 기능이 바뀌거나 삭제되어도 권한만을 수정하면 된다. 사용자는 세션을 통해 자신에게 할당된 역할을 수행할 수 있고 한 명의 사용자는 여러 개의 세션을 동시에 수행할 수 있다. 제약조건의 예로는 한 역할에 최대로 할당될 수 있는 사용자의 수를 의미하는 최대 사용자 수(cardinality)와 임무분리 등이 있다. 다음의 [표-1]은 RBAC 구성요소를 보여준다.[4]

[표-1] RBAC **구성요소 1**.

구성요소	설명
사용자(users)	사용자의 집합으로 시스템을 사용하는 사람들을 의미한다.
역 할(roles)	조직내의 업무들의 집합으로 수행 가능한 권한과 책임으로 구성된다.
연산(operation)	하나 혹은 그 이상의 RBAC 객체들의 집합에 접근하기 위한 특정한 접근 방식이다.
주 체(subject)	일-대-다 관계를 가진 활성화된 사용자 프로세스이다.
제약조건(constraint)	사용자 배정, 역할 할당, 권한 배정, 그리고 세션 등 모든 구성요소에 적용될 수 있다.
객 체(object)	시스템에 의해 관리되는 대상을 의미한다.
권 한(permission)	특정한 객체에 대해 수행 가능한 연산들의 집합이다.

RBAC 을 사용하는 시스템 관리자는 기업이 일반적으로 사업을 수행하는 방법처럼 추상화의 단계에서 접근을 제어할 수 있다 이것은 역할, 역할 계층구조, 관계, 그리고 제약조건의 수립과 정의를 통해서 정적 혹은 동적으로 사용자들의 역할을 조절함으로써 가능하다.[5]

2-2. 통합 사용자 권한 관리 솔루션의 동향

사용자 권한 체계를 구축하기 위한 솔루션으로는 EAM과 IAM 등이 있다. 이는 여러 솔루션 공급 업체들이 제시하는 개념으로 Gartner Group은 EAM 제품이 외부 사용자 접근제어, 사용자 인증, 사용자 권한에 대한 정교한 제어 등을 가능하게 하는 단일의 통합된 프레임워크를 제공한다고 하였다.[6] IAM 솔루션 또한 서로 다른 기종의 IT 환경에서 사용자 계정과 접속 권한 정보를 효과적으로 관리한다는 측면에서 EAM 솔루션과 동일하다. 두 솔루션 모두 어플리케이션 개발 및 보안관리 비용의 절감을 가져올 수 있으며 유지보수 인력에 대한 감축 및 절감 측면에서 효과를 기대할 수 있다.[7]

일반적으로 EAM 솔루션이 제공하는 기능 및 기대 효과로는 분산된 사용자 관리 및 통합관리로 인한 업무 효율성 증대 및 사용자 불편을 감소할 수 있으며 사용자 및 업무시스템 증가로 인한 관리 시간 및 비용을 절감할 수 있다. 또한, 강력한 인증 및 권한 관리로 내외부의 위협에 따른 침해사고 예방 및 보안 증대를 가져올 수 있고 PC, 스마트폰, 태블릿 등 다양한 접속 채널을 통합 중복 접속(Login)을 방지하는 기능을 제공한다. 시스템 개발 측면으로는 시스템의 통합 및 개발의 유연성을 제공한다. 국내 시장에는 2001년 EAM 개념이 처음 소개되었으며 당시 보안기능에 중점을 두었던 솔루션들과 달리 비용 절감과 효율적인 관리 중심의 솔루션이라는 차별성을 추구했다.[8]

3. 화면 및 화면 구성요소에 대한 접근제어 모델

본 절에서는 역할기반 접근제어 정책을 기반으로 권한 관리의 확장을 통한 화면 및 화면 구성요소에 대한 접근제어를 수행하는 확장 모델을 제안한다. 즉, 기존 화면 전체에 대한 접근을 제어하는 것에서 화면 및 화면을 구성하고 있는 UI Component 에 대한 접근제어를 수행할 수 있도록 하였다. 또한, RBAC 모델의 권한(Permission) 확장을 통해 기존에 사용되고 있는 EAM 솔루션의 권한 관리 정책과 원할 한 통합을 할 수 있도록 하였다. 제안된 접근제어 모델의 구조와 각 요소들에 대해 살펴보면 다음과 같다.

3-1. 접근제어 객체

접근제어 객체로는 업무처리에 사용되는 화면과 해당 화면을 구성하고 있는 UI Component 로 분류할 수 있으며, [표-2]는 각각의 객체에 대해 설명하고 [표 3]에서는 UI Component 의 분류의 예를 보여준다.

[표 2] 접근제어 객체

객체	설명
화면(screen)	기업 내 업무시스템을 사용하기 위한 자료를 입력하거나 조회하기 위한 화면
UI Component	화면을 구성하고 있는 구성요소로 텍스트(text), 선택을 위한 Combo Box, 처리를 위한 Button 등 사용자와 시스템간의 인터페이스 역할을 담당한다.

[표 3] UI Component 분류

컴포넌트	설명
Text Input	일반적인 입력 및 수정을 할 수 있는 컴포넌트로 이하 "TXT"로 표현한다.
Label	입력 및 수정을 할 수 없으며, 자료를 보여만 주는 컴포넌트로 이하 "LBL"로 표현한다.
Combo Box	사용자가 다수의 정의된 값 중 원하는 값을 선택할 수 있는 기능을 제공하는 컴포넌트로 이하 "CMB"로 표현한다.
TextArea	다량의 텍스트를 입력 및 수정할 수 있는 컴포넌트로 이하 "TAE"로 표현한다.
Button	버튼형태를 가진 컴포넌트로 클릭(click) 및 더블클릭(double click)과 같은 기능을 제공한다. 이하 "BTN"으로 표현한다.
Linked	일반 텍스트 형태로 보여지지만 클릭(click) 및 더블 클릭(double click)과 같은 기능을 제공한다. 이하 "LNK"로 표현한다.

3-2. 접근제어 객체의 권한 유형

3-2-1. 화면의 접근 권한 부여 유형

화면의 접근권한의 유형을 분류하면 세가지 유형으로 정의할 수 있다. 1 번째 유형은 화면을 볼 수만 있는 유형이다. 이 유형은 화면 조회만 가능하며, 화면의 구성요소인 UI 컴포넌트에 대한 접근 권한을 가지고 있지 않는 경우이다. 이하 READ 권한으로 정의한다. 2 번째 유형은 화면을 볼 수 있고 수정도 할 수 있는 유형이다. 이 유형은 화면을 통해 조회된 내용을 볼 수 있으며, 신규 자료의 입력 및 조회된 UI 컴포넌트의 내용을 수정할 수 있는 경우이다. 이하 EDIT 권한으로 정의한다. 마지막인 3 번째 유형은 화면을 볼 수 없는 유형이다. 이 유형은 화면에 대한 접근을 할 수 없는 경우로 사용자는 해당 화면을 볼 수 없는 경우이다. 이하 NONE 권한으로 정의한다.

3-2-2. UI 컴포넌트의 접근 권한 부여 유형

UI 컴포넌트의 접근권한 유형을 분류하면 네 가지 유형으로 정의할 수 있다. 1 번째 유형은 UI 컴포넌트의 내용을 볼 수만 있는 유형이다. 이 유형은 UI 컴포넌트의 내용을 볼 수만 있는 권한을 가지고 있는 경우이다. 이하 READ 권한으로 정의한다. 2 번째 유형은 UI 컴포넌트의 내용을 볼 수 있고, 입력 및 수정을 할 수 있는 유형이다. 이 유형은 UI 컴포넌트의 내용을 볼 수 있으며 입력, 수정 및 클릭(click)등을 처리할 수 있는 유형이다. 이하 EDIT 권한으로 정의한다. 3 번째 유형은 UI 컴포넌트의 내용을 특정문자(예, *)로 대체한 형태로 볼 수 있는 유형이다. 이 유형은 UI 컴포넌트의 내용이 변형된 형태(일부 자료만 *로 표현)로 볼 수 있는 경우이다. 이하 MARK 권한으로 정의한다. 마지막인 4 번째 유형은 UI 컴포넌트의 내용을 볼 수 없는 유형이다. 이 유형은 UI 컴포넌트에 대한 접근을 할 수 없는 경우로 화면에 해당 UI 컴포넌트가 표시되지 않는 경우이다. 이하 NONE 으로 정의한다.

3-2-3. 권한 유형에 대한 정리

[표 4]는 위에서 설명한 접근제어 객체의 권한유형 및 표현방법에 대해 정리한 내용이며, 화면의 권한 유형과 UI 컴포넌트의 권한 유형에서는 화면의 권한이 UI 컴포넌트의 권한을 지배하고 있으며, 이들의 관계는 계층 구조로 표현할 수 있다. 이 경우 상위 권한 유형은 하위 권한 유형에 대해 묵시적인 지배 권한을 가지게 된다.

[표 4] 접근제어 객체의 권한 유형

객체	권한유형	표현방법
화면(screen)	READ	R
	EDIT	E
	NONE	N
UI 컴포넌트	READ	R
	EDIT	E
	MARK	M
	NONE	N

3-3. 접근제어 객체의 권한 부여

화면의 권한 부여 방법은 [화면아이디][권한유형 1, 권한유형 2, 권한유형 3]의 형태로 표현할 수 있으며, 보험업무시스템에서 사용하는 "보험계약내용조회(화면아이디:SCLI001)" 화면을 예로 부여 될 수 있는 권한의 종류를 살펴보면 [표 5]와 같이 정의할 수 있다.

[표 5] 화면 ID SCLI001 의 권한 예시

권한부여	권한설명
SCLI001[R,-,-]	해당 화면에 대한 조회 권한만 가지고 있는 경우이다.
SCLI001[R,E,-]	해당 화면에 대한 조회 및 UI 컴포넌트에 대한 입력, 수정 및 클릭(Click)등의 처리를 할 수 있는 경우이다.
SCLI001[-,-,N]	해당 화면을 사용할 수 없는 경우이다.

UI 컴포넌트의 권한 부여 방법은 [공통(Common 의 C)/개별(Personal 의 P)구분][화면아이디][UI 컴포넌트 아이디][권한유형 1, 권한유형 2, 권한유형 3, 권한유형 4]의 형태로 표현할 수 있다. 단, UI 컴포넌트의 경우 여러 화면에서 사용되는 공통 UI 컴포넌트가 존재 할 수 있으며, 이 경우 특정한 화면에 종속되지 않기 때문에 화면아이디를 별도 부여한다. 본 논문에서는 SCNN001 로 정의한다. "보험계약내용조회(화면아이디:SCLI001)" 화면의 UI 컴포넌트 중 Text Input 컴포넌트에 부여 될 수 있는 권한의 종류를 살펴보면 [표 6]과 같이 정의할 수 있다.

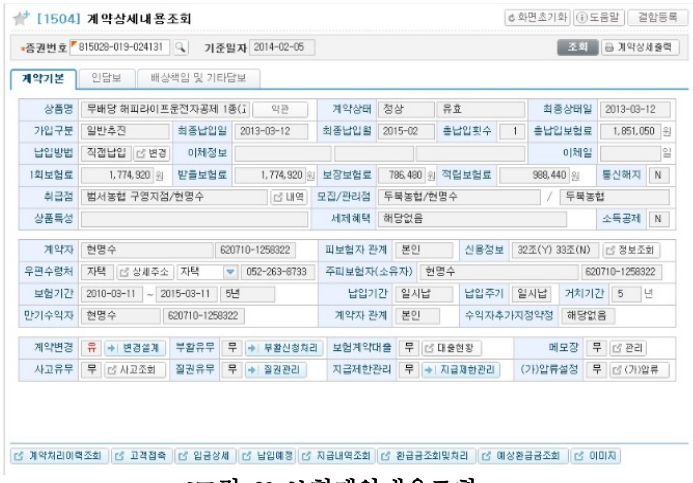
[표 6] UI 컴포넌트의 권한 예시

권한부여	권한설명
PSCLI001TXT0001[R,-,-,-]	개별속성이고 SCLI001 화면에 종속되며, 해당 UI 컴포넌트에 대한 조회권한만 가지고 있는 경우이다.
PSCLI001TXT0001[R,E,-,-]	개별속성이고 SCLI001 화면에 종속되며, 해당 UI 컴포넌트에 대해 조회 및 입력, 수정 등을 할 수 있는 경우이다.
PSCLI001TXT0001[R,-,M,-]	개별속성이고 SCLI001 화면에 종속되며, 해당 UI 컴포넌트에 대해 조회권한을 가지고 있으나, 일부 내용이 특정문자(예, *)로 대체된 형태로 보여지는 경우이다.
PSCLI001TXT0001[-,-,-,N]	개별속성이고 SCLI001 화면에 종속되며, 해당 UI 컴포넌트에 대해 접근 권한을 가지고 있지 않는 것으로 화면에 보여지지 않는 경우이다.

3-4. 제안된 모델을 응용한 권한 부여 사례

[그림 2]는 N 사 차세대 프로젝트에서 수행했던 보험업무시스템에서 가장 많은 빈도로 사용되는 "보험계약내용조회" 화면을 나타내며, [그림 3]은 해당 화

면의 권한 관리 대상이 되는 UI 컴포넌트의 목록을 보여주고 있으며, 해당 화면을 기준으로 제안된 모델을 응용해서 접근 권한 유형을 정의하면 [그림 4]와 같이 구성할 수 있다.



[그림 2] 보험계약내용조회

화면명	화면ID	개별/공통구분	UI Type	UI Prefix	UI Component 명	SEQ
계약상세내용조회	CTRDTLVW001					
계약상세내용조회	CTRDTLVW001	P	TextInput Box	TXT	상품명	0001
계약상세내용조회	CTRDTLVW001	P	TextInput Box	TXT	계약상태	0002
계약상세내용조회	CTRDTLVW001	P	TextInput Box	TXT	계약세부상태	0003
계약상세내용조회	CTRDTLVW001	P	TextInput Box	TXT	최종납입일	0004
계약상세내용조회	CTRDTLVW001	P	TextInput Box	TXT	1회보험료	0005
계약상세내용조회	CTRDTLVW001	P	TextInput Box	TXT	계약자	0006
계약상세내용조회	CTRDTLVW001	P	TextInput Box	TXT	계약자주민등록번호	0007
계약상세내용조회	CTRDTLVW001	P	TextInput Box	TXT	피보험자와관계	0008
계약상세내용조회	CTRDTLVW001	P	TextInput Box	TXT	주피보험자	0009
계약상세내용조회	CTRDTLVW001	P	TextInput Box	TXT	만기수익자	0010
계약상세내용조회	CTRDTLVW001	P	TextInput Box	TXT	보험기간	0011
계약상세내용조회	CTRDTLVW001	P	Button	BTN	변경설계	0012
계약상세내용조회	CTRDTLVW001	P	Button	BTN	계약처리이력조회	0013
계약상세내용조회	CTRDTLVW001	P	Button	BTN	입금상세	0014
계약상세내용조회	CTRDTLVW001	P	Button	BTN	납입예정	0015
계약상세내용조회	CTRDTLVW001	P	Button	BTN	지급내역조회	0016

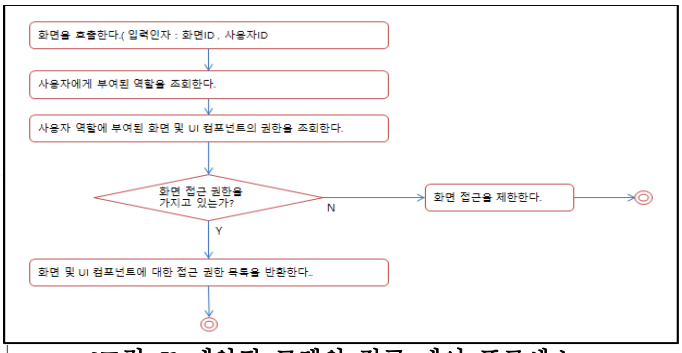
[그림 3] 보험계약내용조회 화면의 UI 컴포넌트 분류

SEQ	UI Component ID	장기보험		고객지원팀(손해)	
		계약관리팀	계약변경팀	고객지원팀	콜센터
		[R,-,-]	[R,-,-]	[R,-,-]	[R,-,-]
0001	PCTRDTLVW001TXT0001	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]
0002	PCTRDTLVW001TXT0002	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]
0003	PCTRDTLVW001TXT0003	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]
0004	PCTRDTLVW001TXT0004	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]
0005	PCTRDTLVW001TXT0005	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]
0006	PCTRDTLVW001TXT0006	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]
0007	PCTRDTLVW001TXT0007	[R,-,-,-]	[R,-,-,-]	[R,-,M,-]	[R,-,M,-]
0008	PCTRDTLVW001TXT0008	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]
0009	PCTRDTLVW001TXT0009	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]
0010	PCTRDTLVW001TXT0010	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]
0011	PCTRDTLVW001TXT0011	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]
0012	PCTRDTLVW001BTN0012	[-,-,-,N]	[R,E,-,-]	[-,-,-,N]	[-,-,-,N]
0013	PCTRDTLVW001BTN0013	[R,-,-,-]	[R,-,-,-]	[-,-,-,N]	[-,-,-,N]
0014	PCTRDTLVW001BTN0014	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]
0015	PCTRDTLVW001BTN0015	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]
0016	PCTRDTLVW001BTN0016	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]	[R,-,-,-]

[그림 4] 보험계약내용조회 화면의 권한 유형

3-5. 접근 제어 프로세스

제안된 모델에서 접근제어를 위한 프로세스는 [그림 5]와 같다. 프로세스의 시작은 사용하고자 하는 화면에 대한 권한 요청에서 시작되며 최종적으로 권한이 적용된 화면을 받는 것을 목표로 하고 있다. 그러나, 권한이 적용된 화면은 별도 화면을 재구성을 해야 하는 과정이 필요하기 때문에, 적용된 권한 목록을 반환 받는 것까지만 수행하는 것으로 한다.



[그림 5] 제안된 모델의 접근 제어 프로세스

4. 결론 및 향후 연구

본 논문에서는 기업 내 업무처리시스템의 화면에 접근하고자 하는 사용자의 접근권한을 미리 설정된 보안정책에 따라 판단하여 해당 사용자가 가진 권한에 따라 화면 및 화면의 구성 요소(UI 컴포넌트)에 대한 접근 범위를 결정하여 화면을 구성하는 각각의 구성요소에 대한 수준별 접근제어를 수행하는 방법을 제안하였다. 또한, 많은 기업에서 사용하고 있는 EAM 시스템에서 도입한 RBAC 의 권한 확장을 통해 관리의 용이성 및 손쉬운 확장을 고려하였다. 향후에 추가적으로 연구되어야 할 부분은 다음과 같이 요약된다. 먼저 제안된 모델의 보안을 강화하기 위해 화면 및 화면 구성요소의 권한에 따른 동적인 화면구성을 할 수 있도록 하는 기법 연구가 필요하다. 즉, 최종 사용자에게 반환되는 화면은 모든 권한이 적용된 화면이며, 화면의 스크립트에서 부여된 권한에 따라 제어하는 것을 배제할 수 있어야 한다. 또한, 이와 같이 동적으로 화면에 권한을 부여함으로써 다양한 채널에 따른 화면 구성 및 제어를 할 수 있다.

참고문헌

[1] FERRAIOLO, David; CUGINI, Janet; KUHN, D. Richard. Role-based access control (RBAC): Features and motivations. In: Proceedings of 11th Annual Computer Security Application Conference. 1995. p. 241-48.

[2] RAMASWAMY, Chandramouli; SANDHU, Ravi. Role-based access control features in commercial database management systems. In: Proc. 21st Nat'l Information Systems Security Conf. 1998. p. 503-511.

[3] SANDHU, Ravi. Access control: The neglected frontier. In: Information Security and Privacy. Springer Berlin Heidelberg, 1996. p. 219-227.

[4] 이희규, 조한진, 김봉한, 이재광, "WWW 에서 안전한 역할 기반 접근 제어 시스템 구현 ", 通信情報保護學會論文誌 Vol.10 No.1, 2000.3, P. 65-75.

[5] BARKLEY, John, et al. Role based access control for the world wide web. In: 20th National Computer Security Conference. 1997. p. 331-340.

[6] Ant Allan, "Netegrity SiteMinder Extrnet Access Management(EAM) Product," Gartner, 2001.

[7] R. Witty, "ROI Drivers Identity and Access Management Implementaion", Gartner, 2002.

[8] 박석; 오세종. Web 환경에서 역할기반 접근제어 (RBAC) 의 적용에 대한 연구. 데이타베이스 연구, 2000, 16.1: 50-58.