역할기반 접근 제어에서 사용자수준의 위임과 상속을 위한 역할 계층의 구조

조기천(충북대학교 데이터베이스연구실) kicheon@dblab.chungbuk.ac.kr
신문선(충북대학교 데이터베이스연구실) msshin@dblab.chungbuk.ac.kr
류근호(충북대학교 데이터베이스연구실) khryu@dblab.chungbuk.ac.kr

요 약

역할기반 접근제어는 지금까지 사용되었던 기존의 임의적 접근제어나 강제적 접근제어를 개선해서 여러 분야에 적용시키기 위해서 많은 연구의 대상이 되어왔다. 이 접근제어 방법은 역할과 사용자, 그리고 권한 사이의 관계를 정의하고, 역할계층을 통해서 역할에 따른 사용자의 권한 관리를 효율적으로 할 수 있도록 한다. 하지만, 역할계층을 현실세계에서의 조직체계에 적용시키는 것에는 문제가 있다. 따라서, 본 논문에서는 기존의 역할계층에서 위임과 상속의 문제점을 제시하고, 새로운 접근방식의 위임과 상속을 제안한다.

1. 서 론

역할기반 접근제어(RBAC : Role-Based Access Control)의 개념은 1970년대에 개발된 온라인 시스템에서 다중 사용자와 다중 응용에 의해서 시작되었다. RBAC의 핵심적 요지는 권한(Permission)이 역할(Role)과 연관되어 있고, 사용자는 적절한 권한에 배정된다는 것이다.

역할은 사용자가 어떤 작업에 대한 권한을 부여받을 수 있는 일종의 권리이다. 따라서, RBAC는 현실 세계의 조직체계와 비슷하다. 임의적 접근제어(DAC : Discretionary Access Control)나 강제적 접근제어(MAC : Mandatory Access Control)를 통해서 현실 세계를 표현하는데 한계가 있기 때문에 그 대용으로 RBAC가 연구되고 있다.

역할은 역할계층(Role Hierarchy)에 따라서 권한의 위임이나 상속이 일어나는데 현실 세계에 적용하기에는 부적절하다. 지금까지 역할 위임의 경우는 어떤 역할에게 위임되는지, 역할 상속의 경우는 최소권한 법칙과 의무 분리 법칙을 명확히 정의하지를 않았다.

이 논문에서는 RBAC의 기본 개념과 역할, 역할계층에 대해서 설명하고, RBAC에서 일반적으로 정의했던 역할계층의 개념을 현실세계의 조직체계에 적용한다. 이렇게 적용된 모델을 이용해서 역할의 위임이나 상속이 있을 때 제약조건의 위배 유무를 분석하고 제약조건을 위배하지 않는 역할계층의 새로운 구조를 제안한다.

2. RBAC의 기본개념

현실세계에 대한 접근방식에 있어서 임의접근 방식은 사용자가 소유하고 있는 자원에 대한 정보의 흐름을 제어할 수 없고, 강제접근 방식은 자원의 접근에 대한 유연성이 부족해서 군대와 같은 제한된 환경 아래에서 구현되고 있다. 따라서, 새로운 접근방식으로 RBAC를 적용하려고 많은 연구가 되고 있다. RBAC의 중요한 목적은 현실세계의 자원에 대한 임의적인 접근을 제어하는 것이다. 현실세계의 조직체계가 다양화되고 복잡해졌기 때문에 기존의 접근방식을 모델링 하는데는 적

합하지가 않다. 따라서, 이러한 다양화되는 조직체계에 적용시킬 수 있는 가장 이상적인 접근제어 방식이 RBAC이다.

그림1은 Ravi Sandhu에 의해서 정의된 RBAC96모델이다.

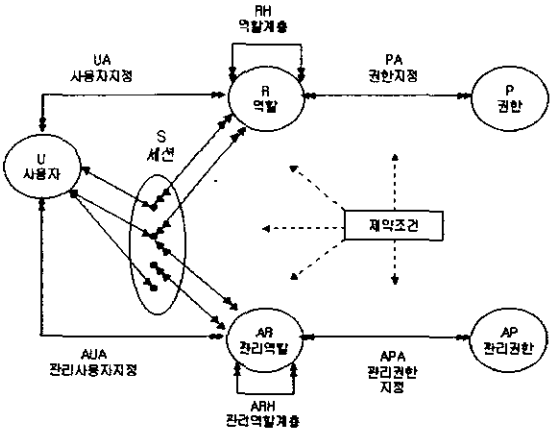


그림1. RBAC96 모델

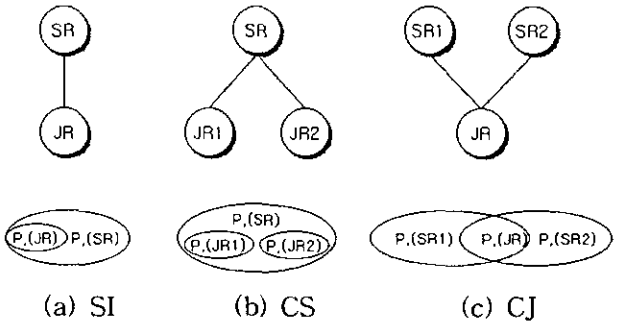
RBAC96 모델의 구성요소들을 간단히 정리하면 다음과 같다.

- U, S : 사용자 집합, 세션의 집합
- R과 AR : 정규역할과 관리역할
- P와 AP : 정규권한과 관리권한
- PA⊆P×R : 권한과 역할지정 관계
  APA⊆AP×AR : 권한과 관리역할 지정 관계
- UA⊆U×R : 사용자와 역할지정 관계
  AUA⊆U×AR : 사용자와 관리역할 지정 관계
- RH⊆R×R : 역할계층이나 역할의 유전 관계를 부분 순서로 나타냄
  ARH⊆AR×AR : 부분 순서화된 관리역할 계층
- Constraint : 제약조건

3. RBAC의 역할계층

역할계층은 조직내의 권한과 책임을 부분순서로 나타내기 위해서 역할을 구성하는 일반적인 방법이다. 역할계층은 격자구조(lattice structure)로 표현된다. 격자구조는 권한과 의무를 선으로 나타내기 때문에 역할을 계층적으로 구성하는 가장 일반적인 방법이다.

역할계층의 특징은 상위(Senior)역할이 하위(Junior)역할의 권한을 상속받고, 상위역할의 권한을 하위역할이 위임받을 수 있는 구조이다. 즉, RBAC에서 상위역할은 하위역할의 권한을 모두 상속하게 된다. 역할 계층의 접근권한에 대한 상속성은 그림2와 같다.



(a) SI (b) CS (c) CJ

그림2. 역할의 구성 (SR : Senior Role, JR : Junior Role)

역할계층의 상속에는 단순 접근권한 상속(SI:Simple Inheritance), 공통 상위 접근권한 상속(CS:Common Senior inheritance), 공통 하위 접근권한 상속(CJ:Common Junior inheritance)의 세 가지 유형으로 구분된다. 계층 구조는 부분순서로 나타나기 때문에 부분순서가 갖는 특징을 갖게 되는데, 특징에는 반사성(Reflexion), 이행성(Transitiveness), 비대칭성(Anti-Symmetry)이 있다. 반사성은 역할 자신이 갖고 있는 권한을 상속하기 때문에 반사성이 있다. 이행성은 하위역할의 권한을 서로 다른 상위역할이 상속을 받게 되면, 권한을 상속받은 상위역할은 같은 역할로부터 상속받았을지라도 다른 권한을 가지게 된다.

역할계층의 정의에 있어서 고려해야할 점은 다음의 두 가지로 요약할 수 있다.

첫째, 하위역할에서 상위역할로의 상속에 있어서 하위역할이 가지고 고유권한을 제외한 나머지 권한 중에서 일부만을 상속해야 한다.

둘째, 상위역할이 하위역할에게 고유권한을 위임할 경우 위임되어지는 권한의 지정과 위임할 대상의 지정이 명시되어야 한다.

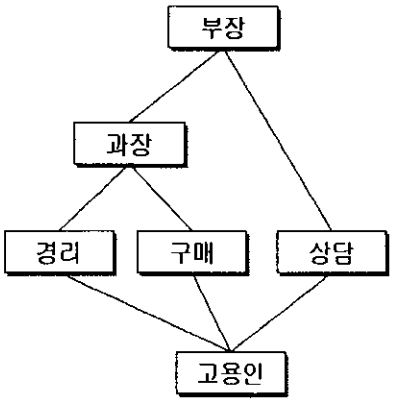
위의 문제점을 해결하기 위해서 현실세계 조직에 적용 가능한 RBAC의 새로운 역할계층을 제안한다.

4. 새로운 역할계층 제안

현실세계에서는 상위역할에 지정된 사용자가 하위역할에 지정된 사용자의 권한을 상속받아서 업무를 처리하는 경우는 거의 없다. 하지만, 상위역할에 할당된 작업을 하위역할에게 위임해주는 경우는 발생할 수가 있다.

기존의 RBAC96 모델의 경우는 이러한 현실세계의 요구조건을 충족시키지 못했다. 이 논문에서 새롭게 제안하고자 하는 역할계층은 현실세계 조직구조의 일부분을 가정해서 위의 요구조건을 충족시키는 것을 목적으로 한다. 상위역할 담당자는 하위역할 담당자의 역할을 적절히 상속을 받게 되고, 하위역할 담당자는 상위역할 담당자가 할당된 역할 중에 허락된 권한만을 위임받을 수 있도록 한다.

새로운 역할계층의 정의는 접근권한 리스트에서 권한의 위임과 상속을 원활하게 해주는 것을 목적으로 한다. 따라서, 자원에 대한 권한을 소유(P), 위임(J), 상속(S)으로 하는 방안을 제안한다.



(a) RBAC 역할계층

역할	접근권한
경리담당자	File1[R,W], File4[R,W(부재시)]
구매담당자	File2[R,W], File4[R]
상담자	File3[R,W], File5[R]
과 장	File1[R,W(부재시)], File2[R], File4[R,W]
부 장	File3[R], File4[R], File5[R,W]

(b) 현실세계의 자원에 대한 접근권한 리스트

그림3. 어느 조직의 역할 구성도 (File1:지출과 수입, File2:기자재 구매, File3:고객과의 상담, File4:예산 조정, File5:세부기획 조정)

5. 제안된 역할계층의 분석

RBAC 모델에는 최소권한(Least Privilege)과 의무분리(SOD : Separation Of Duty), 두 가지의 제약조건이 있다. 다음은 제약조건을 기반으로 한 새로운 역할계층의 분석이다. 최소권한 규칙은 하위 역할이 상위 역할에서 수행할 수 있는 권한을 모두 할당받거나, 기존의 역할에 새로운 권한을 추가하지 못하도록 제한하는 것이다. 의무분리는 두 개의 하위역할에 있는 권한들이 상위역할에게 상속됨으로써 발생할 수 있는 상위역할에서의 권한 오용을 방지하는 것이다.

역할기반 접근제어에서는 권한의 위임이나 상속이 있을 때 위임이나 상속된 권한에 대한 전파가 이뤄졌다. 제안된 역할계층은 기존의 역할계층에서 자원에 대한 권한을 소유, 위임, 상속이라는 세 가지의 부분권한으로 나눔으로써 위임이나 상속에 있어서 권한의 제약 없는 전파(Propagation)를 방지한다. 역할의 위임이 이뤄질 때 발생 가능한 보안문제를 해결하였다.

새로운 역할계층의 접근권한 리스트는 기존의 접근권한 리스트보다 훨씬 간결하고, 보기 쉬운 형태로 나타난다. 그리고, 기존 역할에 대한 위임이나 상속 등의 추가도 쉽게 할 수 있다. 하지만, 컴퓨터를 이용한 역할계층의 구현에 있어서는 소유, 상속, 위임 등의 접근권한을 나타내는데 필요한 저장공간을 고려해야만 한다.

6. 결 론

이 논문에서는 역할기반 접근제어의 개념과 기본 모델(RBAC96)을 설명하였고, 현실세계 조직체계에서 역할기반 접근제어 모델이 어떻게 적용되는지 예를 들어서 나타내었다. 역할기반 접근제어 모델은 사용자, 역할, 권한의 개념을 이용해서 현실세계 조직 체계의 접근제어를 효율적으로 구현한다. 그러나, 역할계층에서 역할에 따른 권한의 위임과 상속이 최소권한규칙이나 의무분리 규칙을 위배하는 경우가 발생할 수 있다. 이를 해결하기 위해서 소유, 위임, 상속이라는 세 가지 개념을 이용한 역할계층 구조를 제안하였다.

이 제안은 역할기반 접근제어 모델을 현실세계의 적용할 때에 발생할 수 있는 제약사항들의 위배유무를 분석하여, 최소권한을 위배하거나 역할의 위임에서 발생할 수 있는 보안문제를 해결한다.

새롭게 제안된 역할계층은 현실세계 조직 체계내의 역할에 할당된 자원에 대한 사용자수준에서의 효율적인 위임과 상속을 가능하게 한다. 향후 다중위임이나 다중상속의 개념추가를 위한 연구가 계속되어져야할 것이며, 다중위임이나 다중상속의 구현에 있어서 발생하는 문제점들을 고려해서 본 논문의 내용을 실제로 구현하고자 한다.