MMDBMS의 안전한 응용을 위한 T-RBAC 기반의 접근제어 미들웨어 프로토타입 설계[1)]

변창우°, 박 석, 최 완*
서강대학교 컴퓨터학과, *한국전자통신연구원
{chang°, spark}@dblab.sogang.ac.kr, wchoi@etri.re.kr

Access Control Middleware Prototype Design based T-RBAC for secure applications with MMDBMS

Chang-Woo Byun°, Seog Park, Wan Choi*
Dept. of Computer Science, Sogang University, *Network S/W Platform Team, ETRI

요 약

최근 인터넷 및 이동 통신이 발달하면서 많은 사용자를 동시에 서비스할 수 있는 고성능 메인 메모리 데이타베이스 관리 시스템에 대한 연구가 활발히 진행되고 있지만, 특정 응용에 한정되도록 개발됨으로써(ad-hoc designed system) 시스템의 범용성이 떨어질 뿐만 아니라, 고객 지향적 요구 사항을 적시에 반영할 수 있는 유연한 구조 및 다른 응용 분야로의 적용(customizing)이 어렵다. 특히, 정보 보안에 대한 문제를 해결하지 못하기 때문에 적용 영역의 확대에 걸림돌이 되고 있다.

본 논문은 접근제어에 초점을 두고 저장된 데이타에 대한 권한 없는 접근, 고의적인 파괴 및 변경으로부터 데이타베이스를 보호하여 고신뢰성을 추구하고, 다중 사용자들의 이질성을 해결하며 다양한 보안 정책을 유연하게 지원하는 고성능 메인 메모리 데이타베이스 관리 시스템을 위한 접근제어 미들웨어 시스템에 대한 프로토타입을 제시한다.

1. 서 론

메인 메모리 데이타베이스 관리시스템(이하, MMDBMS)은 빠른 결정을 내려야 하는 정보 시스템에서 실시간적인 작업들을 수행하는 고성능의 목적을 두고 이용되고 있으며[1], 그 적용 환경을 인터넷/인트라넷 환경, 분산 시스템 환경 및 점점 더 기업환경으로 확산됨에 따라 기업환경을 구성하는 다양한 다른 조직체들은 자신에 맞는 접근제어를 요구하고 있다.

그러나, 기업환경에서 접근제어가 어려운 이유는 기업 내에 많은 수의 사용자와 정보 자원이 존재해서 접근제어 정보를 유지관리 하기가 어렵고, 기업환경의 보안 시스템은 일차적인 목표인 기밀성을 요구할 뿐만 아니라 정보의 원활한 공유와 사용을 보장해야 한다는 요구를 만족시켜야 하기 때문이다. 기업환경에서의 접근제어 특징은 다음과 같다.

- *불특정 다수의 이용뿐만 아니라 트랜잭션 발생 예측이 어렵다.*
- *이용 대상이 상당히 다양하다.*
- *권한 부여의 빈번한 변경이 요구된다.*
- *일반 사용자는 임의적으로 보안 속성(security attributes)을 변경할 수 없다. 오직 보안 관리자만이 할 수 있다.*
- *접근제어 모델은 융통성이 있어야 하고, 정보시스템의 조직체계 혹은 프로세스 체계를 반영해야 한다.*
- *정보시스템의 조직체계상 전체적인 혹은 부분적인 권한 계승(상속)을 지원해야 한다.*
- *제약사항(least of privilege, SOD, etc)을 지원해야 한다.*
- *과업의 다양한 유형을 위한 접근제어를 지원해야 한다.*

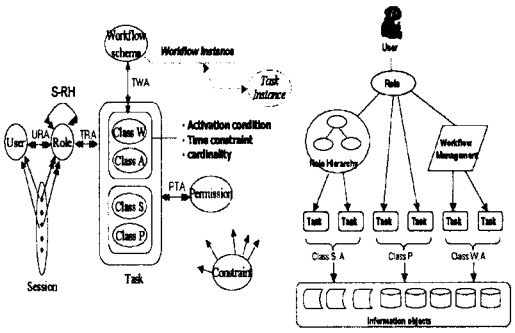
본 논문은 Tachyon MMDBMS[1]을 기반으로 하여 내부에 접근제어 모듈이 들어가 있는 방식보다는 미들웨어 기반의 T-RBAC 모델을 추가로 구성하여 기존의 Tachyon MMDBMS의 변경을 피하고 기업환경이 요구하는 접근제어를 만족시키는 Tachyon MMDBMS 기반의 접근제어 미들웨어 프로토타입을 설계하였다.

본 논문의 구성은 2장에서 접근제어를 위한 기본 정보를 관리하기 위한 보안 스키마 카타로그를 소개하고, 3장에서는 T-RBAC 기반의 미들웨어 프로토타입을 제시하고, 4장에서 결론을 기술한다.

2. 접근제어에서의 보안 스키마 카타로그

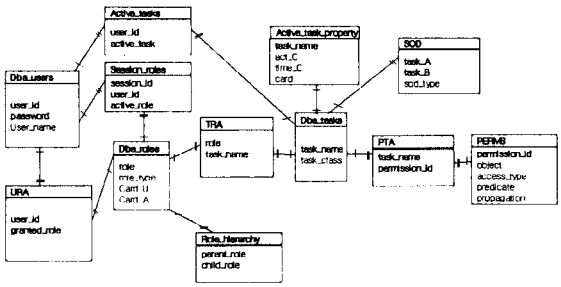
본 논문에서 인용하고 있는 T-RBAC 접근제어 모델[3,4,5]은 [그림 1]과 같으며, RBAC 모델[2]을 기업환경

에 적합하게 변형, 개선한 모델이다. RBAC 모델은 기업과 같은 조직의 구조를 자연스럽게 반영할 수 있는 역할 구조와 제약사항들을 지원하는 정책 중립적인 모델로 평가받고 있으며 역할개념의 사용으로 다중 사용자에 대한 이질성을 해결하고 권한관리가 쉬워 그 비용을 줄여주는 특징을 갖고 있다. 한편, T-RBAC 모델은 역할은 행위자에 초점이 맞춰져 있지만 과업(task)은 행위에 초점이 맞춰져 있다고 구별하여 RBAC 모델의 권한부여 및 회수의 용이성, 정책 중립성 그리고 관리의 편리성 등의 장점을 그대로 이용하면서 역할과 과업의 개념을 모델에 사용하고 있다. 사용자는 역할을 할당 받지만 자원에 대한 접근권한을 얻기 위해서는 역할에 속한 과업을 통해야만 하는 특징을 갖고 있다. 특히, T-RBAC 모델은 기업 내의 과업을 해당 과업이 비즈니스 프로세스에 속하면 active access 과업(Class A(계승가능), Class W(계승불가)), 그렇지 않으면 passive access 과업(Class S(계승가능), Class P(계승불가))으로 분류하여 보다 기업환경에 적합하면서 신뢰성을 주는 모델로 평가받고 있다.



[그림 1] T-RBAC 모델

일반적으로 접근제어가 이루어지기 위해서는 이를 위한 기본 정보가 관리되어야 한다. [그림 2]에서 T-RBAC 모델 기반의 보안 스키마를 제시하고 있으며, 그에 대한 설명을 나타내고 있다.



System_classes	Description
Dba_users	로그인 사용자 정보
URA	사용자에게 허가된 Role 정보
Dba_roles	데이타베이스에 존재하는 Role 정보
Session_roles	사용자가 현재 가용가능한 Role 정보
Dba_tasks	과업들의 집합
Active_tasks	Active 접근제어를 요하는 과업들의 집합
Active_task_property	Active 접근제어를 요하는 과업들의 제약사항 정보
Role_hierarchy	다른 Role에 허가된 Role에 대한 정보
TRA	Role에 허가된 과업 정보
Sod	SOD 정보
PTA	과업에 할당된 권한 정보
PERMS	객체에 대한 권한에 대한 정보

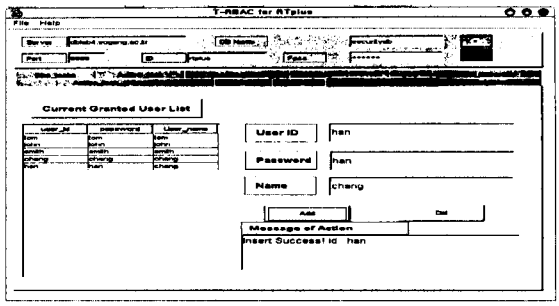
[그림 2] 접근제어를 보안 스키마 카타로그

다음 장에서는 제안한 보안 스키마 카타로그를 기반으로 설계된 프로토타입을 설명한다.

3. T-RBAC 기반의 미들웨어 프로토타입 설계

일반적으로 상업용 데이타베이스 관리시스템을 이용한 응용에서의 사용자와 자원에 대한 접근제어 정책은 응용 프로그램 내부에 구현한다. 이러한 방식의 문제점은 접근제어가 응용프로그램에 종속되어 있기 때문에 접근제어 방식의 변경 및 개선 시 유지보수가 어렵다는데 있다. 본 논문은 접근제어 부분을 응용 프로그램 및 MMDBMS 사이에 독립적으로 두어 응용 프로그램에서의 주체의 객체에 대한 권한부여의 잦은 변경에 융통성 있게 대처하고, 객체의 접근 레벨에 대한 빈번한 변경이 응용에 영향을 주지 않게끔 하여 다양한 보안정책을 유연하게 제공할 수 있는 미들웨어 접근 방식을 취한다.

[그림 3]은 T-RBAC 기반의 미들웨어 프로토타입에 대한 보안관리자를 위한 사용자 인터페이스를 보여주고 있다. 하부 절에서는 이들에 대한 특징을 설명한다.



[그림 3] T-RBAC 기반의 미들웨어 프로토타입의 사용자 인터페이스

3.1 사용자 · 역할 · 과업 지정

사용자(혹은 프로세스가 될 수 있는데 본 논문에서는 사람으로 함)는 모델의 간략화를 위해서 사용자 ID, 비밀번호 그리고 이름으로 지정한다. 역할은 조직 내의 직위나 비즈니스 역할로 간주한다. 역할에 사용자 수 및 역할 활성화 수에 제한을 두고, 활성화된 역할에 대한 정보를 갖춘다. 추가로 과업을 분류하고 활성화 조건, 시간조건 그리고 차수에 대한 제약사항 및 활성화되어 있는

과업에 대한 정보를 갖춘다. 객체는 Tachyon MMDBMS의 클래스와 속성 및 응용과 관련된 파일이 된다.

3.2 권한 지정(Permission Assignment)

권한이란 시스템의 하나 또는 그 이상의 객체에 대한 특정 접근 모드(예 : 판독, 갱신, 수정, 기타 등등)의 승인을 나타낸다. 본 본문에서 객체는 Tachyon MMDBMS의 클래스와 속성뿐만 아니라 이것과 연동하여 기업 또는 조직 내의 정보시스템을 구성하고 있는 자료(data)나 시스템 자원(system resource)을 말한다.

3.3 사용자-역할 할당(User-Role Assignment)

일반적으로 시스템 관리자(혹은 보안 관리자)가 회사나 조직의 업무 기능에 따라 역할을 생성하고 사용자에게 역할을 부여한다. 사용자는 시스템에 로그인을 통해 그들이 가진 역할의 부분집합을 활성화할 때 세션을 형성한다. 각 세션은 하나의 사용자와 여러 개의 접근 권한을 매핑(mapping)한다. 사용자에게 사용 가능한 접근 권한은 그러한 세션에 활성화된 모든 역할이 가진 접근 권한의 합집합이다.

3.4 과업-역할 할당(Task-Role Assignment)

기업환경에서의 작업의 기본 단위인 과업을 역할과 구분함으로써 실세계의 기업조직에 보다 근접하게 객체에 대한 접근을 제어할 수 있다. 따라서, 역할에 여러 과업을 할당하는 처리과정이 요구된다.

3.5 권한-과업 할당(Permission-Task Assignment)

객체에 대한 권한을 세분화된 과업에 할당함으로써 RBAC 모델에서 권한-역할 할당의 문제-역할에 속한 다른 과업이 그 권한을 계속 사용해야 하는데 권한 철회(revoke)에 의해 수행할 수 없게 되는 문제-를 예방한다.

3.6 역할 계층과 의무 분리

정보시스템의 조직체계 상에서의 권한 계승(상속)은 전체적일 수도 있고 부분적일 수도 있어야 한다. 본 논문에서는 조직체의 직위로서의 역할과 비즈니스 측면에서의 역할로 구분하고, 이와 같은 역할에 할당되는 과업을 네 가지의 클래스로 구분하여 권한 계승(상속)의 제한을 두고 있다. 또한, 과업들 간에는 상호 배타성을 가져야 하는 경우도 있다. 이와 같은 의무 분리도 동적인 경우와 정적인 경우로 기업환경에서는 분류된다. 본 논문에서는 이런 사항들을 지원한다.

4. 결론

메인 메모리 데이타베이스 관리 시스템의 적용 영역을 기업환경의 고속 데이타 처리 시스템으로 적용 영역의 확대에 걸림돌이 되는 여러 원인 중 보안 관점의 하나인 접근제어에 초점을 두었다.

불특정 다수의 이용, 이용 대상의 다양성, 권한 부여의 빈번한 변경, 조직체들 간의 다른 접근제어 방법들에 대한 효과적인 통제 가능성 등의 기업환경의 고속 데이타 처리시스템의 기본 요구사항을 전제로 기존의 Tachyon MMDBMS의 변경을 피하고 기업환경이 요구하는 접근제어를 만족시키는 T-RBAC 기반의 접근제어 미들웨어 프로토타입을 설계하였다. 본 논문의 산출물인 접근제어 미들웨어 프로토타입은 조직 프로세스를 폭넓게 통제할 수 있는 장점과 조직체계에서 발생할 수 있는 권한의 계승(상속)을 통제함으로써 현실 세계의 조직 프로세스를 반영하고, T-RBAC 모델의 특징인 과업 단위의 접근제어를 관리함으로써 최소한의 권한 원칙 및 의무분리 등 접근제어의 필요한 제약사항을 지원하고 있다. Tachyon MMDBMS와 접근제어 미들웨어 프로토타입과의 연동을 통한 기업 조직의 한 부서의 웹 페이지에 대한 접근제어 시나리오에 대한 구현 내용은 지면상 생략한다. 제안한 프로토타입은 기업환경의 정보시스템에 유연하게 활용될 수 있을 것이라 기대한다.

5. 참고문헌

[1] Wan Choi et al., "Tachyon: the Object-Relational Real-time DBMS for Telecommunication Systems" , The 6th Intl Conf. On Electronics, Information, and Comm.(ICEIC 2002), Ullaanbaatar, Mongolia, July 2002.

[2] Ravi Sandhu, Edward J. Coyne, Hal L. Feinstein and Charles E. Youman, "Role-Based Access Control Models" , IEEE Computer, Vol.29, No.2, 1996.2, pp.38-47.

[3] Sejong Oh and Park Seog, "Task-Role Based Access Control(T-RBAC): An improved Access Control Model for Enterprise Environment", Database and Expert System Applications, LNCS 1873. pp. 264-273.

[4] Sejong Oh and Park Seog, "An Improved Administration Method on Role-Based Access Control in the Enterprise Environment", Journal of Information Science and Engineering, Vol.17. pp.927-944.

[5] Sejong Oh and Park Seog, "Task-Role-Based Access Control Model" , Information System, (to be published in 2003).