개선된 역할 계층을 이용한 유연한 데이터베이스 보안 시스템

정민아* · 이광호*

Flexible Database security System using Improved Role Hierarchy

Min-A Jung* · Kwang-Ho Lee

요 약

병원, 행정기관, 은행과 같은 조직체의 경우 중요하고 민감한 데이터를 보호하기 위해 데이터베이스 보안이 필수적이다. 최근 대규모의 조직체에서 업무가 더욱 다양하고 복잡해짐에 따라 보안 정책에 대한 변경이 빈번히 일어나게 되었다. 따라서 보안정책의 무결성을 보존하면서 변경이 용이한 유동적인 보안 정책과 효율적인 보안 관리가 매우 중요하다. 본 연구에서는 의료정보관리시스템을 대상으로 Improved Role Hierarchy(IRH)를 이용한 유연성 있는 데이터베이스 보안 시스템을 구현하였다. 데이터 접근은 MAC 방식으로 제어하며, RBAC의 역할 계층(Role Hierarchy)을 개선한 IRH를 사용하여 유연성 있는 접근제어를 제공하고 효과적인 보안 관리를 할 수 있다. 본 시스템은 보안정책이 바뀔 경우 분산된 보안관리 방식으로 IRH를 수정함으로써 정책 변경을 용이하게 하며, 주체의 보안등급이 고정되어 있지 않은 상태에서 이를 IRH을 통해 사용자와 세션이 맺어질 때 결정되게 함으로써 정책이 바뀐 후에도 변경된 보안정책을 유연하게 적용할 수 있다.

ABSTRACT

Database security is essential to protect their data in most organizations such as hospitals, central or local governments, banks which manage the private, sensitive and important data. Because the duty of the department recently became more various and complicated, the changes of security requirement are needed more frequently. Therefore, easily changeable, flexible security policy and efficient security management with preserving the integrity of security policy are very important. In this paper, we implemented a flexible database security system in the specimen and clinical information management system of leukemic research center using IRH(Improved Role Hierarchy). Data is protected by MAC and we propose a flexible access control and effective administration by using the IRH that is an improved role hierarchy of RBAC. If security policy is needed for changes, this system can do it easily by simply modifying the IRH with the decentralized administration. The modified security policy can be applied flexibly after alteration because the security level of the subject is not fixed but can be derived automatically from the IRH when a user connects the system.

키워드

데이터베이스 보안, 역할 기반 접근 제어, 역할 계층, 보안 정책 관리

* 목포대학교 컴퓨터교육과

접수일자 : 2005. 10. 4

Ⅰ. 서 론

오늘날 기업 및 정부 조직의 보안 체제 요구가 급증하면서 권한이 있는 사용자에게 허가된 데이터 사용을 보장하기 위한 접근 제어(Access control)가 필요하게 되었다. 보안을 위한 대표적인 접근 제어 방식으로는 임의적 접근 제어(DAC: Discretionary Access Control), 강제적 접근 제어(MAC: Mandatory Access Control), 역할기반 접근 제어(RBAC: Role-Based Access Control)를 들 수 있다. 어떠한 접근 제어 방식을 사용할 것인가를 결정하는 문제는 시스템의 보안 요구 사항을 만족하는 제어 방식을 선택하거나 여러 접근 제어 방식들의 특징들을 적절하게 조합하여 다양한 보안요구를 만족시키는 방법 등을 사용할 수 있다.

본 논문에서는 의료정보관리시스템에서 데이터베이스 접근 제어와 보안 관리가 어떻게 이루어지는지 소개한다. 이 시스템은 환자의 질병 및 개인정보와 같은 사적이고 기밀한 데이터를 포함하기 때문에 데이터베이스 보안이 요구된다. 또한 이 시스템은 새로운 종류의 데이터가 추가되는 일이 빈번하기 때문에 그럴 때마다 이 데이터를 사용하는 새로운 업무가 추가 발생하고 업무에 인력을 새로 배치하거나 또는 재배치하는 상황이 야기된다. 이러한 상황을 만족시킬 수 있는 보안 관리를 위해 보안정책이 수시로 바뀌고 변경될 때마다 이를 쉽게 반영할 수 있는 유동적인 보안 모델이 만들어져야 한다. 또한, 이 시스템은 규모가 크고 업무처리가 매우 다양한 시스템이다. 이런 환경에서 보안정책을 관리하고 수정사항이 생겼을 경우 이를 변경하는 일이 매우 어려우며 업무의 부담 또한 크다. 특히 중앙 집중형 관리 방식은 소수의 보안 관리자에게 심각한 업무 부담을 주면서 비효율성을 초래하게 된다. 따라서 관리를 비집중화하여 관리 부담을 줄일 수 있는 보안모델이 요구된다. RBAC은 MAC이나 DAC의 특성을 모두 가진 상업용 환경에 적합한 정책이다. 동시에 보안 관리를 간단하고 용이하게 해주는 큰 장점을 갖고 있다[1, 2, 3, 4, 5]. 따라서 본 논문을 위한 연구는 이러한 RBAC의 특징들을 사용하면서 데이터의 보안등급에 기반하여 데이터 접근을 제어하는 MAC의 방식을 혼합하여 보안모델을 구현한다.

아울러 본 논문은 기업 환경과 업무가 변할 수 있는 상황에서 보안정책이 유동적으로 변경될 수 있는 방안을 제안하고, 분산된 보안 관리 방식으로 보안정책이 쉽게 변경되는 방법을 제시한다. 본 논문은 다음과 같이 구성된다. 2장에서는 관련연구를 제시하고, 3장에서는 본 논문에서 제안하는 보안정책과 보안관리를 논하고, 4장에서는 시스템 설계 및 구현에 관하여 설명한다. 마지막 5장에서는 결론과 향후 연구 방향에 대해서 논한다.

Ⅱ. 관련연구

2.1 ARBAC

RBAC은 보안 정책 관리를 위해 RBAC을 관리하는 Administrative RBAC(ARBAC)을 제안한다[9]. ARBAC은 URA(User-Role Assignment), PRA(Permission-Role Assignment), RRA(Role-Role Assignment) 컴포넌트로 나뉜다[1, 6]. URA는 사용자를 역할에 할당하는 보안 관리에 대해서 명세하고, PRA는 권한을 역할에 할당하는 보안 관리를 수행하며, RRA는 역할을 역할에 할당하는 보안 관리를 수행한다[2, 3, 4].

RRA에 의해 역할을 역할에 할당함으로써 역할 계층이 생성되고 자식의 역할은 부모 역할에 할당된 권한을 상속해서 사용할 수 있게 된다. 또한, 역할간의 관계가 변하거나 보안 정책이 변경될 때 이 역할 계층만을 수정함으로써 보안 관리가 용이하다[1, 4, 6].

2.2 eMEDAC

eMEDAC은 기존에 구현된 MEDAC(Medical Database Access Control)이라 불리는 의료 정보 데이터베이스 접근 제어 시스템을 확장한 시스템이다[7]. MEDAC은 DAC과 MAC을 혼용하여 보안 요구사항을 만족하는 의료정보 데이터베이스 시스템이고, eMEDAC은 RBAC의 일부 특징을 혼합하여 MEDAC을 확장하였다. 이 시스템은 HNH(Hyper Node Hierarchy) 모델을 적용하여 사용자 역할 계층(URH: User Role Hierarchy)과 데이터 집합 계층(DSH: Data Set Hierarchy)을 구성한다[7, 8, 9]. 사용자등급이나 데이터등급은 저장되어 고정되어 있지 않고 이 두 계층을 통해서 사용자의 접근이 있을 때 사용자의 등급과 데이터의 등급이 계산되어 접근을 제어한다. 따라서 이 두 계층에 의해 유동적으로 변경이 가능한 보안 정책을 만족시킬 수 있다[7, 8].

Ⅲ. 데이터베이스 보안 시스템의 구조 및 기능

3.1 시스템 요구사항

보안 관리자는 제안하는 보안 시스템은 다음의 요구사항을 만족한다.

① 사용자는 세분화된 업무체계에서 해당되는 업무만을 수행한다.

② 시스템은 다수의 사용자와 대량의 데이터를 다룬다.

③ 새로운 업무가 추가되고 사용자간의 부서 이동 및 업무 변경이 빈번하다.

④ ③사항에 따라 보안 정책이 자주 바뀐다.

위와 같은 사항을 만족하기 위하여 본 시스템은 MAC과 RBAC의 특징들을 조합한다. 먼저 데이터접근은 MAC으로 제어한다. MAC은 BLP 모델[7]에 근거하여 데이터등급과 사용자등급을 비교했을 때 지배관계(dominance relation)를 만족하는 접근을 허용한다. 본 시스템의 데이터등급은 4단계로 정의한다. 사용자는 역할에 할당되고 해당하는 역할의 등급이 사용자의 보안등급을 대신하게 된다. 이때, 역할등급은 데이터보안등급에 따라 최대값 4로 제한한다. 보안 정책이 바뀔 수 있다는 가정 하에 역할등급은 고정되어 있지 않고 사용자와 세션이 맺어질 당시에 역할등급과 역할범주가 결정된다. 따라서 사용자의 부서가 바뀌거나 업무가 변경 되어 보안 정책이 수정되는 경우 이를 쉽게 반영할 수 있다. 또한, 이러한 환경에서 보안 관리가 소수 관리자에 의한 중앙 집중형 방식이라면 관리 업무의 부담이 커지므로 보안관리가 비효율적이다. 이를 해결하기 위해 여러 명의 부 관리자를 두고 역할 계층의 일부분을 관리하게 함으로써 관리를 분산시킨다. 부 관리자는 보안정책의 무결성을 보장하는 범위(Create Range)에서 개선된 역할 계층에 대해 역할관계를 수정할 수 있으며 본 논문에서는 추가 변경만을 고려한다[1, 9].

3.2. IRH(Improved Role Hierarchy)

본 논문에서 제안한 시스템의 역할 계층은 eMEDAC에서 사용하는 HNH만으로는 모두 다 표현할 수가 없다. 이 HNH는 단일상속만을 허용하고 다중상속을 지원하지 않기 때문이다. 따라서 본 연구에서는 다중상속을 지원하고 본 시스템의 목적에 맞는 보안 모델을 구축하기 위해 HNH의 Dummy node, Link 이 두 가지 요소를 도입하여 기존 RBAC의 역할 계층(Role Hierarchy)을 개선하여 이를 IRH라 한다. 그림 1은 본 시스템에서 사용하는 IRH를 나타낸다. 역할들 간의 관계가 상속 관계에 있지만 역할 보안등급의 차이가 없을 때 Link로 연결하고, 상속 관계에 있으면서 보안등급의 차이가 한 등급 있을 때 Branch로 연결한다. 상속 관계에 있는 역할들이 보안 등급의 차이가 한 등급 이상일 때 역할 사이에Dummy Node를 삽입하고 이를 Branch로 연결하여 표현한다.

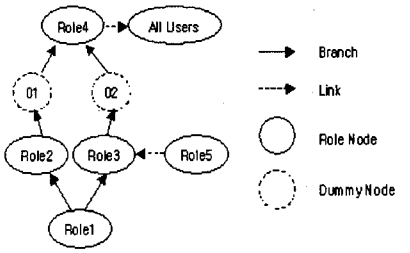


그림 1. 개선된 역할 계층
Fig. 1 Improved Role Hierarchy

① 역할 상속: 할당된 역할은 역할 계층에서 부모 역할을 상속하여 권한을 수행할 수 있다.

② 역할등급과 역할범주 자동 결정: 역할등급과 역할범주가 세션이 맺어질 때 이미 생성된 IRH를 바탕으로 자동 결정된다. 그림 2의 알고리즘 1과 그림 3의 알고리즘 2 각각은 사용자의 역할등급과 역할범주를 결정하는 알고리즘이다.

알고리즘1. 역할등급 결정 알고리즘

```
Start:
    level = 1
    UR=User Role
    while Connection(UR) ≠ 'All Users'
        if Connection_Type(UR) == 'branch'
        then level = level + 1
        UR[ ] = Connection(UR)
        UR = UR[0]
    endwhile
```

그림 2. 사용자 역할등급 결정 알고리즘
Fig. 2 User role level determination algorithm

알고리즘2. 역할범주 결정 알고리즘

```
Start:
    UR = User Role
    CS = fcs( UR )
    return CS
End:

Function fcs(A)
    while Connection(A) ≠ 'All Users'
        if Node_Type(UR) == 'hyper'
        then cs = Category(A)
        UR[ ] = Connection(A)
        for ( k = 0 ; k < sizeof ( UR[ ] ) ; k++)
            cs = cs U fcs( UR[k] )
     endwhile
     return cs
EndFunction
```

그림 3. 사용자 역할범주 결정 알고리즘
Fig. 3 User role category determination algorithm

③ 보안 관리의 분산: 업무의 유사성에 따라 IRH의 역할범위를 나누어 보안 부 관리자에게 일부분씩 관리하도록 범위를 지정함으로써, 보안 관리를 분산 시킬 수 있다. 예를 들어 1세부 보안정책을 변경할 경우 1세부 업무 보안 관리자는 2세부 업무에 관계된 역할 관계에 영향을 주거나 역할 계층 전체를 건드리지 않고 1세부 역할관계를 간단하게 변경할 수 있다.[1]

3.3. 데이터베이스 보안 정책

그림 4는 본 논문에서 제안한 데이터베이스 보안 시스템의 구조도를 보이며, 각 구성요소의 기능은 다음과 같다.

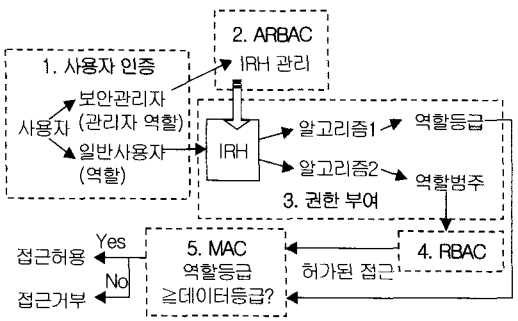


그림 4. 데이터베이스 보안시스템 구조
Fig. 4 Database security system architecture

① 사용자 인증 : 사용자의 계정을 확인하고 사용자에게 역할이 할당된다.

② ARBAC: 할당 받은 역할이 관리자 역할일 경우 역할과 역할의 권한들을 정의하고 IRH를 생성하거나 관리하며 사용자에게 역할을 할당한다.

③ 권한부여: 할당받은 역할이 일반 사용자 역할일 경우 IRH를 통하여 알고리즘 1,2를 이용하여 역할등급과 역할범주를 결정한다.

④ RBAC: 역할범주와 역할에 부여된 권한 집합에 의해 접근하려는 객체와 모드가 사용자에게 허가된 접근인지 판단한다. 여기서 비 권한 요청이면 접근이 거부되고 권한이 있는 요청이면 다음 단계로 MAC의 제어를 받는다.

⑤ MAC: RBAC에서 권한이 있는 접근일지라도 지배관계(dominance relation)에 있는 객체에만 접근이 허가된다. 즉 객체의 보안등급이 역할 인가등급보다 더 낮거나 같을 경우에만 접근이 허가된다.[10]

Ⅳ. 설계 및 구현

4.1 역할 정의 및 IRH 설계

본 시스템의 역할은 다음 표 1과 같이 정의된다.

표 1. 역할 정의
Table. 1 Role definition

역할명	약칭	역할 설명	역할명	약칭	역할 설명
Employee	E	직원	Employee of 2 Part	E2	2 세부직원
Employee of 1 Part	E1	1 세부직원	Servant of 2 Paart	SVT2	2 세부 업무 보조원
Servant of 1 Paart	SVT1	1 세부 업무 보조원	Reseacher of 2 Part	RSCH2	2 세부 연구원
Reseacher of 1 Part	RSCH1	1 세부 연구원	Leader of 2 Part	LD2	2 세부 책임자
Leader of 1 Part	LD1	1 세부 책임자	Director	DIR	총책임자

그림 5는 "Employee" 역할과 "Employee of 1 Part" 역할에 환자정보 테이블에 대해서 각각 select, insert, update 모드의 권한들이 부여된 것을 보여주고 있다. "Employee1"은 "Employee"역할을 상속함으로 권한을 중복 부여하지 않고도 "Employee1"에서 할 수 있는 연산들을 수행할 수 있다.

```
Employee : Inherit → Employee
select case_info (num, code, name, hospital, exam_date, pro, pro_tel, medical, reg_user, reg_date, edit_date)
{where code like '1%'};
insert case_info (num, code, name, hospital, exam_date, pro, pro_tel, medical, reg_user, reg_date, edit_date);
update case_info (num, code, name, hospital, exam_date, pro, pro_tel, medical, reg_user, reg_date, edit_date)
{where code like '1%'};

Employee1 : Inherit → Employee
select case_info (sec_num, phone, add_no, address1, address2)
{where code like '1%'};
insert case_info (sec_num, phone, add_no, address1, address2);
update case_info (sec_num, phone, add_no, address1, address2)
{where code like '1%'};
```

그림 5. 역할에 권한 부여
Fig. 5 Role-Authority assignment

그림 6은 이 시스템의 보안 요구 사항과 역할들의 관계성에 맞게 설계된 IRH이다.

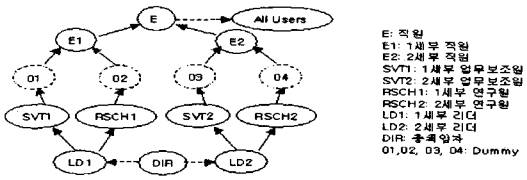


그림 6. 개선된 역할 계층
Fig. 6 Improved Role Hierarchy

그림 7은 역할 "Servant of 1 Part" 역할에 할당된 사용자가 접속했을 때 알고리즘1, 2에 의해 결정된 역할등급과 역할범주다. 이처럼 사용자의 등급이 시스템에 접속할 때 보안등급과 역할범주가 결정이 되기 때문에

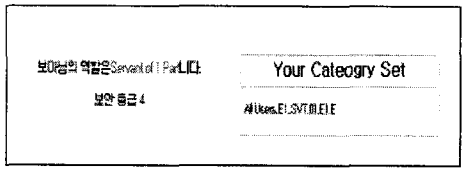
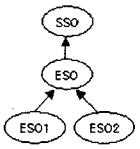


그림 7. "Servant of 1 Part"의 역할등급과 역할범주
Fig. 7 Role level and category of "Servant of 1 Part"

어떤 역할을 수행하는 사용자들의 보안등급이 바뀌었을 때 해당하는 사용자들의 보안등급을 바꿔줄 필요없이 IRH의 역할 관계만을 수정해줌으로써 매우 간단하게 보안 등급이 바뀔 수 있다.

이러한 시스템에서 사용자는 환자 정보에 대한 데이터에 대해서 "insert" 모드로 환자정보 데이터에 접근할 경우 접근하려는 데이터가 역할에 부여된 권한이 아닐 때 "not permitted"라고 표시되고 권한이 부여된 역할에 의한 사용이지만 이 역할을 상속하는 더 높은 역할등급의 사용자가 기록한 데이터에 대해서 MAC의 지배 관계를 만족하지 않기 때문에 접근이 거부될 때 "unauthorized"라고 표현된다. 그림 8은 이 시스템을 관리하는 관리자 역할 계층과 각 관리자에 지정된 관리 범위(Authority Range)이다.



관리자	관리범위
SSO	(E, DIR)
ESO	(E1, LD1) (E2, LD2)
ESO1	(E1, LD1)
ESO2	(E2, LD2)

SSO: 총보안관리자
ESO: 1,2세부 보안관리자
ESO1: 1세부 보안관리자
ESO2: 2세부 보안관리자

그림 8. 관리자 역할 계층과 관리 범위
Fig. 8 Role hierarchy and authority range of administrator

이러한 관리자 역할 계층에서 eso1 관리자는 새로운 "Assistant of 1 Part" 역할을 생성하고 IRH에 추가변경할 수 있다. 이 관리자는 역할 범위 (E1, LD1) 내에서 역할 및 보안 관리를 할 수 있고 이 범위는 생성 범위(Create Range)조건을 만족하고 있기 때문에 역할을 추가 변경을 할 수 있다[4, 6]. "Assistant of 1 Part" 역할이 다른 역할들과 어떤 관계성을 갖으며 어떤 보안등급을 가져야 하는지 충분히 검토를 하고 IRH 내에 관계를 설정할 수 있다.

V. 결 론

본 논문에서는 IRH를 이용하여 유연한 데이터베이스 보안 시스템을 제안하였다. 데이터는 MAC으로 제어하여 데이터를 보호하고 주체의 보안등급을 IRH의 역할등급으로 대신하여 보안 관리를 용이하게 할 수 있다. 또한, 보안 정책이 바뀌었을 때 IRH를 수정하여

간단히 변경할 수 있고, 사용자 접속 시에 역할등급과 역할범주가 IRH를 통해 결정 되므로 보안정책을 수행하는 있어서 매우 유연하다.

향후에는 IRH에 역할을 추가변경 하는 것 뿐 만 아니라 IRH에서 역할을 삭제하는 방법과 Link나 Branch 등의 상속 관계를 추가 삭제함으로써 보안정책을 수정하는 방법에 대한 연구가 필요하다.

참고문헌

[1] R. Sandu andQ. Munawer "The ARABC97 Model for Role-Based Administration of Roles" ACM Transactions on Information and System Security, 1(2):105-135, 1999

[2] R. Sandhu and V. Bhamidipati "The URA97 Model for Role-Based User-Role Assignment", Proceedings of IFIP WG 11.3 Workshop on Database Security, Aug 1997

[3] R. Sandhu and V. Bhamidipati "An Oracle Implementation of the PRA97 Model for Permission-Role Assignment", In Proceedings of 3rd ACM Workshop on Role-Based Access Control, Oct. 1998.

[4] R. Sandu andQ. Munawer "The RRA97 Model for Role-Based Administration for Role Hierarchies" ACSAC, 1998

[5] NIST "Role Based Access Control (Draft 4/4/2003)" American National Standards Institute, Inc, 2003

[6] S. I. Gavrila and J. F. Barkley. "Formal Specification for Role Based Access Control User/Role and Role/Role Relationship Management" In Proceedings of Third ACM Workshop on Role-Based Access Control, p.81-90, 1998

[7] Mavridis I. andPangalos G. "eMEDAC: Role-Based Access Control Supporting Discretionary and Mandatory Features" IFIP Workshop on Database Security, July 1999

[8] M. Pangalos G. andKhair M. "Design of Secure Distributed Medical Database Systems" DEXA '98, 1998

[9] Mavridis I., Pangalos G., Khair, M. and Bozios L. "Defining Access Control Mechanisms for Privacy Protection in Distributed Medical Database", Proceedings of IFIP Working Conference on User Identification and Privacy Protection, 1999.

[10] 심갑식 "데이터베이스 보안" 다성출판사. 2001

저자소개

정민아(Min-A Jung)

1992년 전남대학교 전산통계학과 (학사)
1994년 전남대학교 대학원 전산통계학과(이학석사)
2002년 전남대학교 대학원 전산통계학과(이학박사)
2005년 ~ 현재 목포대학교 컴퓨터교육과 교수
※관심분야 : 데이터베이스, 데이터마이닝, 생물정보학, 정보보호

이광호(Kwang-Ho Lee)

1987년 서울대학교 컴퓨터공학과 (학사)
1989년 한국과학기술원(공학석사)
1996년 한국과학기술원(공학박사)
1996년 ~ 현재 목포대학교 컴퓨터 교육과 교수
※관심분야 : 인공지능, 영상처리, 알고리즘