변형된 RBAC 정책에 기반한 효율적인 데이터베이스 보안 관리 시스템

강주미° 정민아 김정자 원용관
전남대학교 컴퓨터공학과
{jmkanga°, majung, jjkim, ykwon}@grace.chonnam.ac.kr

A Effective Database Security Management System based on the Modified RBAC

Jumi Kang° Mina Jeong Jungja Kim Yonggwan Won
Dept. of Computer Engineering, Chonnam National University

요 약

병원, 은행과 같이 중요한 정보를 다루는 조직체들은 그들 데이터를 보호하기 위해 기업 환경과 어플리케이션 특성에 맞는 특별한 데이터베이스 보안 정책을 사용하고 있다. 이러한 대규모의 조직체에서는 업무가 다양하고 복잡하므로 보안정책에 대한 변경이 빈번하게 발생한다. 따라서 보안정책의 무결성을 보존하면서 수시로 변경되는 보안 요구사항을 반영하고 효율적으로 보안관리를 할 수 있는 보안 시스템이 요구된다. 본 연구에서는 조혈계 질환 시료정보관리시스템을 대상으로 IRH(Improved Role Hierarchy)를 이용한 유연성 있는 데이터베이스 보안 시스템을 구현하였다. 데이터 접근은 MAC 방식으로 통제하며, RBAC의 역할계층(Role Hierarchy)을 개선한 IRH를 사용하여 유연성 있는 접근제어를 제공하고 효과적인 보안관리를 할 수 있다. 본 시스템은 보안정책이 바뀔 경우 분산된 보안관리 방식으로 IRH를 수정함으로써 정책 변경이 용이하고 주체의 보안등급이 고정되지 않은 상태에서 IRH을 통해 사용자와 세션이 맺어질 때 결정되므로 정책이 바뀐 후에도 변경된 보안정책이 유연하게 적용된다.

1. 서 론

오늘날 기업 및 정부 조직의 보안 요구가 급증하면서 권한이 있는 사용자에게 허가된 데이터 사용을 보장하기 위한 접근통제(Access control)가 필요하게 되었다. 보안을 위한 대표적인 접근통제 방식으로 임의적 접근통제(DAC), 강제적 접근통제(MAC), 역할기반 접근통제(RBAC)가 있다. 데이터베이스 보안 모델들은 주로 이러한 정책기반 접근통제를 이용하고 있다.

본 논문에서 제안한 데이터베이스 보안 시스템은 조혈계 질환 시료정보관리시스템을 위한 것이다. 이 시료정보관리시스템은 환자의 질병 및 개인정보와 같은 사적이고 기밀한 데이터를 다루므로 특별한 데이터 보안이 요구된다. 또한 데이터가 추가되는 일이 빈번하여 그때마다 새로운 업무가 추가 발생하고 업무에 인력을 새로 배치하거나 또는 재배치하는 상황이 야기된다. 이러한 상황에 대처할 수 있도록 보안정책의 변경이 쉽고 변경된 보안정책이 잘 반영이 될 수 있는 유동적인 보안 시스템이 필요하다.

또한 이와 같이 규모가 크고 업무 처리가 매우 다양한 시스템에서 보안 정책이 수정 되어야 할 경우 보안정책의 변경이 어렵고 보안 관리의 업무도 매우 부담스럽다. 특히 중앙 집중형 보안 관리 방식은 소수의 보안 관리자에게 심각한 부담을 주면서 비효율성을 초래하게 된다. 따라서 보안 관리를 비집중화하여 관리 부담을 줄일 수 있는 보안모델이 요구된다. RBAC은 MAC이나 DAC의 특성을 모두 가진 상업용 환경에 적합한 정책으로 보안관리를 간단하고 용이하게 해주는 큰 장점을 갖고 있다[1][2][3]. 따라서 본 논문에서는 이러한 RBAC의 특징들을 사용하고 데이터의 보안등급에 기반하여 데이터 접근을 통제하는 MAC을 혼합한 보안 시스템을 구현한다.

이를 위해 본 논문은 기업 환경과 업무가 변할 수 있는 상황에서 유동적으로 변경될 수 있는 보안정책을 제안하고, 분산된 보안 관리 방식으로 보안정책이 쉽게 변경되는 방법을 제시한다.

본 논문은 다음과 같이 구성된다. 2장에서는 관련연구를, 3장에서는 본 논문에서 제안하는 보안정책과 보안관리를 논하고, 4장에서는 결론과 향후 연구 방향에 대해서 서술한다.

2. 관련연구

2.1. eMEDAC

MEDAC(Medical Database Access Control)은 DAC과 MAC을 혼합하여 의료정보시스템의 보안 요구사항을 만족시키는 보안정책이고 eMEDAC은 RBAC의 일부 특징을 혼합하여 MEDAC을 더욱 강화시킨 보안정책이다[4][5]. 이 보안정책은 HNH (Hyper Node Hierarchy) 모델을 적용하여 구성된 사용자 역할 계층과 데이터 집합 계층을 사용한다. 사용자등급이나 데이터등급은 고정되지 않고 사용자의 접근이 있을 때 이 두 계층을 통해서 사용자의 등급과 데이터의 등급이 계산되어 접근을 통제한다. 따라서 이 두 계층에 의해 보안정책이 유동적으로 변경될 수 있다.

2.2. ARBAC

Administrative RBAC(ARBAC)은 RBAC을 관리하는 보안정책이다[3]. ARBAC은 URA, PRA, RRA 컴포넌트로 나뉜다. URA(User-Role Assignment)는 사용자를 역할

에 할당하는 보안관리에 대해서 명세하고, PRA (Permission-Role Assignment)는 권한을 역할에 할당하는 보안관리를 명세하며, RRA(Role-Role Assignment)는 역할을 역할에 할당하는 보안관리를 명세한다 [1][2].

RRA에 의해, 역할을 역할에 할당함으로써 Role Hierarchy가 생성이 되고 자식의 역할은 부모 역할에 할당된 권한을 상속받아 사용할 수 있다. 또한 보안정책이 변경될 때 이러한 Role Hierarchy를 수정함으로 보안정책 관리가 용이하다 [3][6].

3. 제안하는 보안 모델과 보안 관리

3.1. 시스템 요구 사항

제안하는 보안 시스템은 다음의 요구사항을 만족한다.

① 사용자는 세분화 된 업무체제에서 해당되는 업무만을 수행한다.

② 시스템은 다수의 사용자와 대량의 데이터를 다루며 사용자와 데이터는 계속 증가한다.

③ 새로운 업무가 추가 발생되고 사용자간의 부서 이동 및 업무 변경이 빈번하다.

④ 따라서 보안 정책이 자주 바뀐다.

위와 같은 사항을 만족하기 위하여 본 시스템은 MAC과 RBAC에서 필요한 특징들을 혼합하여 적용하였다. 데이터접근은 MAC으로 통제하고 사용자는 RBAC의 역할에 할당된다. MAC은 BLP 모델[7]에 근거하여 데이터등급과 사용자등급을 비교했을 때 지배관계를 만족하는 접근을 허용한다. 여기에 필요한 데이터등급은 5단계로 정의하고 사용자등급은 할당된 역할의 등급이 이를 대신하게 된다. 이때 역할등급은 데이터보안등급에 따라 최대 값 5로 제한한다. 보안정책이 바뀔 수 있다는 가정 하에 역할등급은 고정되어 있지 않고 사용자와 세션이 맺어질 당시에 역할등급과 역할범주가 결정이 되도록 한다. 따라서 사용자의 부서가 바뀌거나 업무가 변경 되어 보안정책이 수정됐을 경우 이를 쉽게 반영할 수 있다. 이러한 환경에서는 보안 관리가 소수 관리자에 의한 중앙 집중형 방식이라면 관리 업무의 부담이 늘게 되어 보안관리는 비효율적이게 된다. 제안하는 시스템은 이를 해결하기 위해 여러 명의 부관리자를 두고 역할계층의 일부분을 관리하게 함으로써 관리를 분산시킨다. 그리고 부관리자는 보안정책의 무결성을 깨지 않는 범위에서 개선된 역할 계층에 대해 역할관계를 수정할 수 있게 한다.

3.1. IRH: Improved Role Hierarchy

본 논문에서는 HNH의 Dummy node, Link 이 두 가지 요소를 도입하여 역할계층을 개선하였고 이를 IRH라 한다. IRH는 RBAC의 역할계층을 사용함으로써 얻을 수 있는 장점들을 가지면서 동시에 HNH의 역할등급과 역할범주를 결정해줄 수 있는 기능을 제공하며 다중 상속관계를 표현할 수 있다. 따라서 본 시스템의 역할체제를 완벽히 표현할 수 있고 보안요구사항을 충분히 만족시킬 수 있다. 그림1은 본 시스템의 업무체제에 맞게 설계된 *IRH이다.*

IRH는 본 시스템에서 크게 3가지 용도로 쓰인다.

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

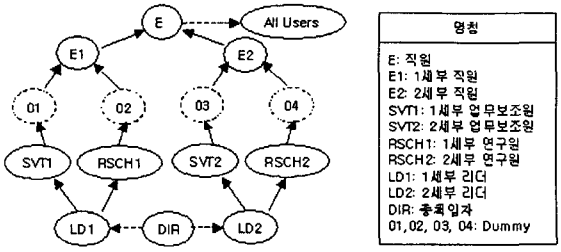


그림 1. Improved Role Hierarchy

② 역할 인가등급과 역할 범주 자동 결정: 역할등급과 역할 범주가 세션이 연결될 때 이 IRH를 통하여 자동 결정된다. 그림 2의 알고리즘1,2는 각각 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
    return level
End:
```

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 ∪ fcs( UR[k] )
    endwhile
    return cs
EndFunction
```

그림2. 사용자 역할등급과 역할범주 결정 알고리즘

③ 보안 관리의 분산: 업무의 유사성에 따라 IRH의 역할범위를 나누어 여러 명의 보안 관리자들에게 일부를 관리하도록 범위를 지정함으로써, 보안 관리를 분산 시킬 수 있다. 예를 들어 1세부 보안관리자는 2세부 업무에 관계된 역할계층에 영향을 주지 않고 1세부 역할계층을 수정함으로써 1세부의 보안정책을 변경할 수 있다.

3.3. 데이터베이스 보안정책

그림3은 본 연구에서 제안하고 있는 데이터베이스 보안 시스템의 구조도이다.

① 사용자 인증: 사용자가 들어오면 할당 받은 역할이 활성화 된다.

② ARBAC: 할당 받은 역할이 관리자 역할일 경우 IRH를 정의하거나 관리한다.

③ 권한부여: 할당 받은 역할이 일반 사용자 역할일 경우 IRH에서 알고리즘1,2를 이용하여 역할등급과 역할범주를 결정한다.

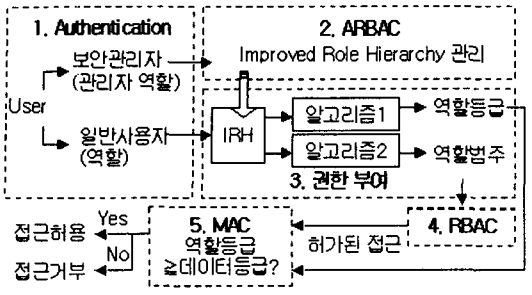


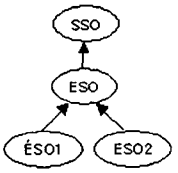
그림3. 데이터베이스 보안시스템 구조

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

3.3. 보안 관리

본 시스템은 보안 관리의 분산을 위하여 그림4와 같이 여러 명의 부관리자에게 IRH내의 역할계층의 일부분을 관리할 수 있도록 역할 범위(Authority Range)를 할당한다. 부관리자는 지정된 역할계층 범위 내에서 보안정책을 관리하고 역할 관계를 변경할 수 있다.



(a) 관리자 역할계층

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

(b) 관리 범위

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

그림 4. ARBAC

본 연구에서는 IRH의 보안 관리를 위해 역할을 추가 변경하는 방법을 제시한다. 먼저 그림4와 같이 필요한 표기를 명시하고 IRH에 역할을 추가하는 함수를 정의한다.

① AddRole(r, p, d): 그림5(a), (b)처럼 새로운 역할(r)이 자식역할(c) 관계는 없고 부모역할(p)과의 관계(d)만 설정된 경우. (Leaf인 경우)

- d=0 : 새로운 역할(r)은 부모역할(p)과 Link로 연결된다.(그림5(a))
- d≠0 : 부모역할(p)과 새로운 역할(r) 사이에 d-1개의 Dummy Node가 추가되고 branch로 연결 된다.(그림5(b))

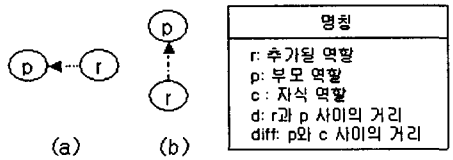


그림 5. Leaf인 경우

② AddRole(r, p, c, d): 그림6(a), (b)처럼 새로운 역할(r)이 부모역할(p)과 자식역할(c) 사이에 관계(d, diff)가 설정된 경우.(Leaf가 아닌 경우)

-d=0 && diff=0 : 부모역할(p)과 새로운 역할(r) 사이는 Link로 연결되고, 새로운 역할(r)과 자식역할(c) 사이도 Link로 연결된다.(그림6(a))

-d=0 && diff≠0 : 부모역할(p)과 새로운 역할(r)은 Link로 연결되고, 새로운 역할(r)과 자식역할(c)은 diff-1개의 Dummy Node와 branch로 연결 된다.(그림6(b))

-d≠0 && diff≠0

* d = diff : 부모역할(p)과 새로운 역할(r)은 d-1개의 Dummy Node와 branch로 연결 되고, 새로운 역할(r)과 자식역할(c)은 Link로 연결 된다.(그림6(c))
* d ≠ diff : 부모역할(p)과 새로운 역할(r)은 d-1개의 Dummy Node와 branch로 연결 되고, 새로운 역할(r)과 자식역할(c)은 diff-d-1개의 Dummy Node와 branch로 연결 된다.(그림6(d))

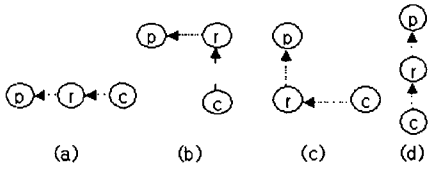


그림 6. Leaf가 아닌 경우

4. 결론 및 향후 계획

본 논문에서는 IRH를 이용하여 유연성 있는 데이터베이스 보안 시스템을 제안하였다. 데이터는 MAC으로 통제하여 데이터를 보호하고 주체의 보안등급을 IRH의 역할등급으로 대신하여 보안관리를 용이하도록 하였다. 또한 정책이 바뀌었을 때 IRH를 수정하여 간단히 변경할 수 있고, 사용자 접속 시에 역할등급과 역할범주가 IRH를 통해 결정 되므로 보안정책이 매우 유연하게 수행된다.

향후에는 IRH에 역할에 대한 추가변경 뿐만 아니라 보안정책의 무결성을 보존하면서 IRH를 수정할 수 있는 방법에 대한 연구가 필요하다.

5. 참고 문헌

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

[2] R. Sandu & Q. Munawer, "The ARABC97 Model for Role-Based Administration of Roles," *ACM Transactions on Information and System Security*, pp. 105-135, 1999

[3] R. Sandu & Q. Munawer, "The RRA97 Model for Role-Based Administration for Role Hierarchies," *ACSAC*, 1998

[4] I. Mavridis & G. Pangalos, "eMEDAC: Role-Based Access Control Supporting Discretionary and Mandatory Features," *IFIP Workshop on Database Security*, 1999

[5] G. Pangalos & M. Khair, "Design of Secure Distributed Medical Database Systems," DEXA '98, 1998

[6] S. Gavrila & J. Barkley, "Formal Specification for Role Based Access Control User/Role and Role/Role Relationship Management," *In Proceedings of 3rd ACM Workshop on RBAC*, pp.81-90, 1998

[7] 심갑식, "데이터베이스 보안," 다성출판사, 2001