RBAC 에 기반한 의료 정보 보호 시스템의 설계 및 구현

노승민[1] 이수철[1] 황인준[1] 박상진[2] 김현주[2]
[1]아주대학교 정보통신전문대학원 정보통신공학과
email: {anycall[1], juin[1], ehwang[1]}@ajou.ac.kr
[2]아주대학교 대학원의학과
email: sangjpark@empal.com, genetics@soback.kornet.net

MIPS: Design and Implementation of Medical Information Protection System based on RBAC

SeungMin Rho[1] SooCheol Lee[1] EenJun Hwang[1] SangJin Park[2] HyonJu Kim[2]
[1]The Graduate School of Information and Communication, Ajou University
[2]Dept. Of Medical Genetics, School of Medical, Ajou University

요 약

환자의 의료 및 질환정보는 개인의 프라이버시에 관련되므로 민감하게 취급되어야 하며 이러한 의료 및 질환정보의 유출은 환자의 사회적인 고립뿐 아니라 환자의 생명도 위협하게 되므로 철저한 보안이 필요하다. 따라서, 의료진, 환자, 일반인 등의 사용자 식별을 통한 진료 기록의 접근 통제 및 사용 권한에 따른 정보의 암호화 수준과 해당 정보에 대한 역할 기반의 접근 제어(Role-Based Access Control)를 제공해야 한다. 본 논문에서는 RBAC 모델을 현재의 의료 및 질환 정보 관리에 적용시켜 각 정보 개체들과 사용자 간의 효율적인 역할 분담과 정보 보호를 위한 시스템을 설계 및 구현하여 실제 시스템에 적용하고자 한다.

1. 서론

환자의 의료정보는 환자의 진료 정보와 관련된 모든 정보를 의미하며, 이는 개인의 프라이버시 중에서도 민감하게 취급 되어야 하는 정보이다. 최근 미국을 비롯한 선진 각국에서 개인 의료 정보를 안전하게 보호하기 위한 보안 법률과 표준안을 제정하고 있으며, 의료 사고를 최소화 하기 위하여 권한 기반 인증 및 로그 데이터의 감사 기능을 제도화하고 있다. 의료 기관의 의료 및 질환 데이터는 환자 개인에게 있어서 민감한 부분인 만큼 다른 어느 분야의 정보 보다도 안전하게 보호되어야 하며, 이와 함께 자원에 대한 역할별 인증 및 그에 따른 접근 제어와 로그 데이터의 감사도 철저하게 이루어져야 한다. 또한, 환자의 생명을 다루는 분야이기 때문에, 환자의 데이터의 기밀성을 보장하는 동시에 응급 상황에도 대처할 수 있도록 가용성을 제공하여야 한다.

의료정보는 의료법에 따라 환자 본인외에는 알리지 않는 것이 원칙이지만, 환자의 배우자나 그 직계 또는 배우자의 직계 그리고 환자가 지정하는 대리인 등에게 알려줄 수가 있다. 하지만 어떠한 경우에는 환자 이외의 사람에게 절대로 발설해서는 안되는 사항도 있다. 즉, 의료정보는 매우 다양하고 가지는 의미가 매우 심오하기 때문에 상황에 따라서 매우 다른 의미를 가진다. 이렇게 다양한 의미를 가진 의료정보의 무단 유출은 실제로 환자의 사회적인 고립뿐 아니라 생명도 위협하게 된다. 따라서 의료정보는 철저한 보안과 보호를 필요로 한다. 현재 의료 체계상 환자의 의료정보에 대한 모든 보호 및 보안은 의료기관이 책임지고 있다. 하지만 자신의 의료정보에 대한 환자와 일반인의 관심이 고조돼 가면서, 자신의 의료정보를 자신이 관리하거나 감독을 하는 경우가 많이 있기 때문에 이에 대한 대책이 필요하다.

의료정보를 다루는 많은 시스템이 전산화되면서 의료기관간에도 의료정보의 전송이 빈번해지고 있는 형편이다. 따라서 의료정보를 보호하기 위한 여러 방면에 걸친 지침이 준비돼야 한다. 이를 위해서, 법제도의 보호와 함께 기술적인 측면에서의 보안에도 신경을 써야하며 이를 위해 많은 국내외 단체들이 기술적인 표준화를 추진중에 있다. 이러한 의료정보는

매우 방대하기 때문에 의료정보를 보호한다는 것은 간단하지 않다. 따라서, 의료정보는 의료진, 환자, 일반인 등 사용자 식별을 통해 진료 기록의 접근을 통제하고, 사용 권한에 따라 의료정보의 암호화(Data Encryption) 수준과 해당 정보에 대한 역할 기반의 접근을 제어하여 보호해야 한다.

본 논문의 구성은 다음과 같다. 2 장에서는 RBAC 에 대한 간략한 설명을 하며, 3 장에서는 RBAC 을 이용한 접근 제어 모델을 제안하고 이를 구현하며 마지막으로 4 장에서는 결론 및 향후 계획에 대해서 논의한다.

2. RBAC (Role-Based Access Control)

RBAC [4]은 역할에 기반을 두고 사용자의 시스템 자원에 대한 접근을 제어하는 기법이다. RBAC 모델의 가장 큰 특징은 권한을 부여하는 단위가 사용자 대신 사용자가 수행하는 기능에 따라 분류에 역할이라는 점이다. 따라서, 사용자는 보호대상 정보나 자원에 대한 접근권한을 얻기 위해서는 해당 접근권한이 배정된 역할의 구성원이 되어야 한다. 권한부여 및 관리 단위가 사용자가 아닌 역할이라는 이 특성은 많은 사용자로 구성된 시스템의 효율적 권한관리를 가능하게 한다. 또한, 역할간 계층구조를 통해 하위 역할에 배정된 권한이 상위 역할에 의해 사용될 수 있는 권한상속(permission inheritance) 특징을 제공한다. 권한상속 특성을 이용하여 계층구조를 가진 역할들에 대한 권한부여를 효과적으로 실행할 수 있다. 이러한 방식은 권한 관리를 매우 단순화 시켜주고, 특정한 보안정책을 구현하는데 있어서 유연성을 제공하는 장점이 있다. 또한, 사용자는 그들의 업무적 권한과 책임에 따라 특정 역할의 구성원이 되며 접근 구조의 변경없이도 역할의 변경을 쉽게 할 수 있다. 그림 1 은 RBAC 의 기본적인 모델을 보여주며, 사용자(U: User), 역할(R: Role), 권한(P: Permission), 세션(S: Session)으로 구성되어 있다.

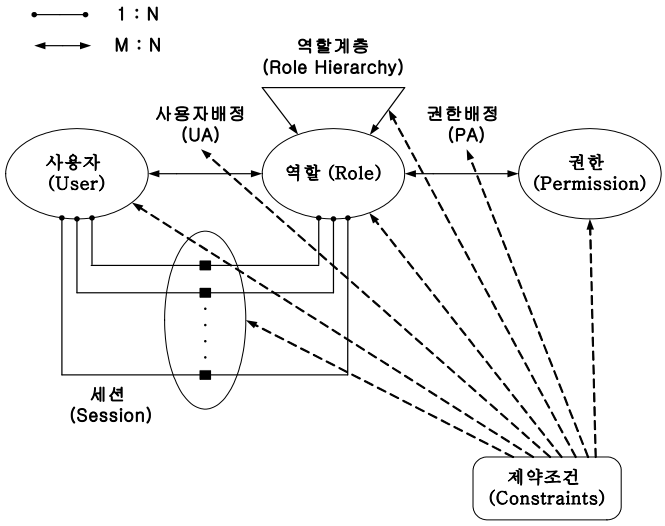

그림 1. RBAC 모델

User(U): 시스템을 통하여 시스템내의 정보를 사용하는 객체로서 한 사용자는 한 명의 사람에 대응된다.

Role(R): 접근제어 정책을 구현하는 중요한 의미적 구조로서, 조직내의 직급을 나타내며 고유의 권한과 의무를 갖는다.

Permission(P): 시스템의 하나 또는 그 이상의 객체에 대한 특정 접근 모드(읽기, 쓰기, 수정 등)의 승인을 나타낸다.

Session(S): 시스템의 로그인을 통해 사용자가 수행하기 위한 작업에 대한 역할을 활성화 시킨 상태. 이때 각 세션은 하나의 사용자와 여러 개의 권한을 매칭한다.

User Assignment(UA) & Permission Assignment(PA): 사용자 배정과 권한 배정은 다대다의 관계이며, 사용자가 정보 객체들에 대해 실행할 수 있는 연산들을 직접 사용자에게 부여하는 대신 역할로 배정하고(PA), 사용자는 해당 역할의 구성원이 됨으로써(UA) 정보 객체에 대한 연산을 수행한다.

3. 제안 모델의 설계 및 구현

본 장에서는 기존의 사용자 기반 접근제어 기법의 단점을 보완하고자 제안된 역할기반 접근제어 기법을 실생활에 맞게 설계하고 구현하는데 있어서 필요한 요구들에 대해서 소개하고 이러한 요구들을 만족하는 모델을 제안하고 의료정보 보호시스템(MIPS: Medical Information Protection System)을 구현한다.

3.1 RBAC 을 이용한 접근 제어 모델

본 논문에서 제안하는 접근 제어 모델은 앞서 설명한 기존 역할기반의 접근 제어 모델을 보완하고 있으며 다음의 사항들을 만족한다.

- User role associations
- Role hierarchies
- Conflict of interest
- Separation of duty constraints

우선, 사용자가 가지는 역할은 다음과 같은 속성들에 의해서 결정 되어진다.

{UserID, UserName, Domain}

UserID 와 UserName 은 사용자의 고유한 아이디와 이름을 의미하고, Domain 은 사용자가 속한 그룹과 그들의 지위 등을 의미한다. 예를 들면, 사용자가 의사나 간호사인 경우에는 “의료진” 그룹에 속하며, 환자의 가족인 경우에는 “환자” 그룹에 속하게 되는 것이다. 또한 각각의 역할은 사용자 그룹(Domain)에 속하며, 같은 그룹내에서는 대부분 비슷한 권한을 가지게 된다. 이렇게 같은 그룹내에서 가지는 일반적인 권한은 그룹내의 사용자에게 동일하게 적용이 되며, 서브

그룹에 속하는 사용자는 상위 그룹으로부터 권한을 상속 받게 된다. 예를 들어, 연구원의 경우에는 담당 의사나 의사의 서브 그룹에 속하며, 수석 간호사의 경우에는 간호사의 일반적인 권한을 상속 받게 된다.

Nyanchama[3]의 논문에서는 역할 그래프 상에서 생길 수 있는 서로 상반되는 요구들의 충돌을 해결하기 위해 5 가지의 충돌을 정의하고, 그 중에서 권한간의 충돌과 역할간의 충돌에 대한 해결방안을 제시하였다. 하지만 이러한 충돌 처리 방식은 현실에 비추어 볼 때 너무 엄격하고 제한적이기 때문에, 논문 [2]에서는 충돌하는 권한을 세분화하여 기존의 역할 그래프 모델의 엄격한 충돌 처리 방식보다 좀 더 현실에 맞는 유연한 충돌 처리 방식을 제안하였다.

또한 사용자는 최소한 하나 이상의 역할을 가질 수 있는데 예를 들면, 한 사용자가 의사인 동시에 환자 또는 보호자 등의 역할을 가지는 경우가 그러하다. 하지만, 동시에 모든 역할을 만족할 수는 없다. 이렇듯 사용자가 다중 역할을 가지게 될 경우, 의료 및 질환 정보나 특정 리소스 등의 접근을 위해서 이들이 가지는 역할과 권한과의 관계(Role-Permission Relationship)를 정의해야만 한다. 각 권한들은 환자의 의료정보나 특정 리소스 등에의 접근을 허용하거나 거부하는 것뿐만 아니라 읽기, 쓰기, 수정 등의 해당 리소스에 대한 구체적인 권한들을 사용자에게 할당하게 된다. 이러한 역할과 권한과의 관계는 5 개의 튜플로 이루어진 하나의 집합으로 표현할 수 있으며 이들의 구성요소는 다음과 같다.

{ID, r, {operation}, t, constraint(r,t,p)}

- ID: 권한 식별자
- r(role): 해당 권한을 처리하기 위한 역할
- operation: 역할에 의해 처리되어지는 실제 행위
- t(target): 해당 행위가 실행되어지게 될 개체
- constraint(r,t,p): 해당 권한에 대한 제약조건을 의미하며, role과 target 및 privilege에 의해서 결정

예를 들어, “John”이라는 의사가 질환 정보에 대해 읽기 및 수정 권한을 가지는 경우 역할과 권한과의 관계는 다음과 같이 표현될 수 있다.

{John, physician, {read, modify}, disease_info,
domain_user(physician) and satisfy(privilege) and
belong(physician, disease_info)}

이때의 제약조건은 “physician”의 도메인에 속한 사용자의 역할을 가지며, 특정 개체인 질환 정보에 접근할 수 있는 권한과 privilege 를 소유하였는지를 판단하는 다음의 함수들로 정의된다.

- domain_user(r) - 해당 역할을 가지며 도메인에 속해있는 사용자
- satisfy(p) - 해당 privilege를 만족하는 사용자
- belong(r,t) - 해당 역할을 가지며 특정 개체에 접근할 수 있는 권한을 소유한 사용자

이러한 의료 및 질환 정보들은 의사가 환자를 진료할 때에 얻을 수 있는 정보나 또는 환자 자신이 자가 진단을 통해서 얻을 수 있는데, 이렇게 얻어진 정보들에 접근할 수 있는 사용자를 환자 자신이 등록할 수 있어야 한다. 이때, 환자는 모든 사용자에 대해 모든 역할과 권한에 대해서 제어할 수 있는 것은 아니다. 대부분의 역할과 권한은 역할-권한 브로커(Role-Permission Broker)가 수행하도록 하며, 그 외의 질환 정보들에 대해서만 환자 본인이 역할과 권한을 부여할 수 있다. 환자의 질환 정보에 대한 등록시에 환자는 브로커가 수행하지 않는 정보들 중 (예를 들어, 이메일이나 전화번호 등) 자신의 개인 정보에서 각 그룹별로 권한을 부여함으로써, 자신의 정보에 대한 책임을 지게 된다.

```
Access Control Algorithm:

Input: access_request(userID, role,
                      target_data, privilege)
Output: accept/reject
Function:
  is_role_member(userID, role) {
    If userID is authorized for role
      return true
    Else return false
  }
  is_operation(privilege, role) {
    If privilege is associated with role
      return true
    Else return false
  }
  satisfy_constraint(userID, role
                target_data, privilege) {
    If target_data and userID satisfies
      the constraints that are associated
      to the role
       return true
    Else return false
  }
Method:
  If (is_role_member(userID, role) and
    is_operation(privilege, role)) then
    If (satisfy_constraint(userID, role
        target_data, privilege)) then
        return accept
    Else
        return reject
  Else
    return reject
```

그림 2. 접근 제어 알고리즘

그림 2 는 사용자가 접근하고자 하는 의료 및 질환 정보에 대한 요청을 하고, 해당 정보에 접근할 수 있는 역할과 privilege 를 만족하는 권한을 가지고 있는지를 판단하여 접근 제어를 하는 알고리즘을 보여준다.

3.2 구현

MIPS 는 다양한 사용자들이 여러 의료정보나 민감한 질환정보의 접근과 공유를 위하여 RBAC 모델을 적용시킨 웹 기반의 보안 응용으로 기본 보안 요소인 기밀성(confidentiality), 가용성(availability), 무결성(integrity) 이외에도 데이터의 인증(authenticity of data), 부인방지(non-repudiation) 등의 요구들을 만족한다.

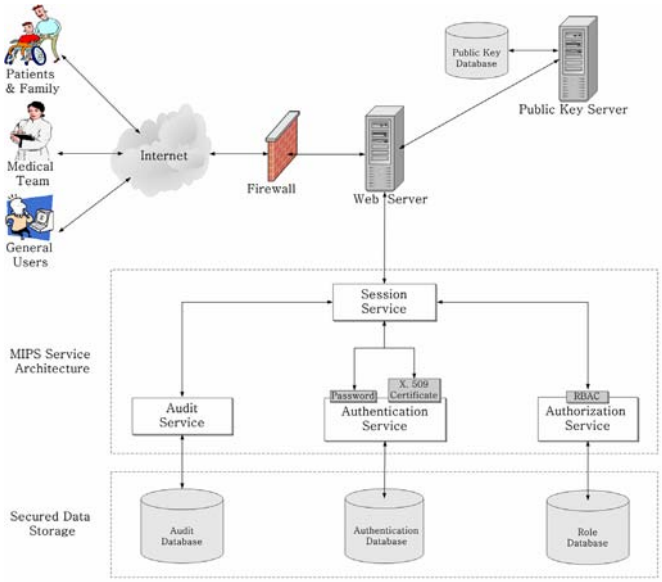

그림 3. MIPS 서비스 구조

그림 3 은 MIPS 의 전체적인 서비스 구성을 보여주고 있으며 다음과 같은 보안 서비스를 제공한다.

사용자 식별 및 인증 – 해당 시스템이나 리소스에 접근하기 위한 사용자의 식별을 의미하며, 아이디와 암호를 입력 받는 단순 인증과 디지털 서명이 들어간 인증서에 의한 인증을 지원한다.

접근 제어 및 권한부여 – 사용자가 어느 특정 리소스에 어떠한 권한을 가지고 무슨 행위를 할 수 있는지에 대한 접근 제어이며 이에 대한 권한 부여와 접근 제어 모델은 RBAC 에 기반한다.

감사 (Auditing) – 모든 보안에 관련된 행위들에 대한 로그 데이터를 저장하고 사용자의 비정상적인 접근 패턴을 분석함으로써 사용자의 행위에 대한 책임을 지게 한다.

세션 관리 – 위의 세 가지 서비스를 만족하는 사용자의 세션을 관리한다.

MIPS 는 리눅스 서버에서 JSP 를 이용하여 구현되었으며, 데이터베이스 서버는 오라클 8i 를 사용하여 구축하였다. 또한 민감한 의료정보와 철저한 보안이 요구되는 관리자의 정보들은 SSL(Secure Socket Layer) 이나 X.509 인증서 등과 같은 보안관련 암호화 기술을 사용하여 전송함으로써 보다 안전한 통신을 할 수가 있다.

그림 4 는 특정 사용자가 가지는 역할로부터 권한을 할당 또는 제거하는 화면으로 보여준다. 좌측 프레임의 메뉴에서 보는 것과 같이 사용자, 역할, 권한, 접근하고자 하는 오브젝트(리소스), 역할에 의해 처리되는 행위 및 여러 관계들에 대해 정의할 수 있다.

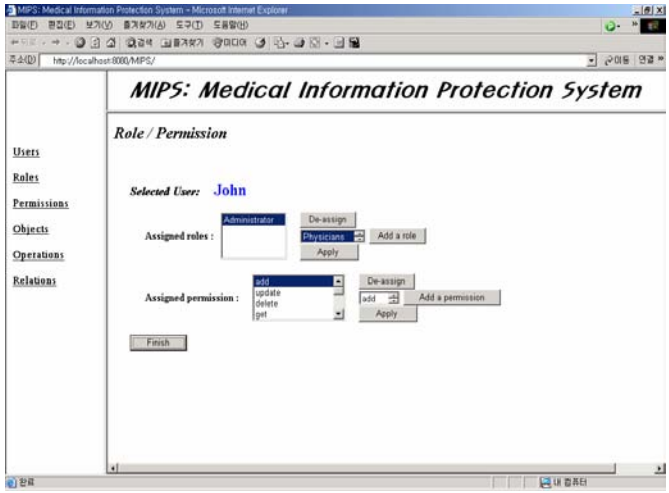

그림 4. 해당 역할에 대한 권한 할당

4. 결론 및 향후 계획

본 논문은 RBAC 을 현재의 의료 및 질환정보의 관리에 적용한 모델을 제안하였다. 또한 이러한 모델을 적용한 실제 시스템의 구현을 통해서 현재의 의료 정보 시스템에 적용하여 환자들의 의료 정보의 보호와 각 정보 개체들과 사용자간의 효율적인 역할 분담을 통한 현재 의료 정보의 관리체계를 개선하고자 하였다. 향후 계획으로는 현재 아주대학교 의학유전학 연구실에서 운영중인 한국 희귀질환 연맹 사이트[1]에 제안한 모델을 적용시키는 것이다.

참고문헌

[1] 한국 희귀질환 연맹, http://www.kard.org/

[2] 정유나, 황인준, “권한 세분화를 이용한 역할 그래프 모델에서의 유동적 권한 삽입 연산,” 2003 년도 한국정보과학회 추계 학술발표논문집 Vol.30, No.1, pp.637-639, 2003.10.

[3] Matunda Nyanchama and Sylvia Osborn, “The Role Graph Model and Conflict of Interest,” ACM Transactions on Information and System Security, Vol.2, No.1, pp. 3-33, Feb., 1999.

[4] R.S. Sandhu, “Role-Based Access Control,” IEEE…. Computer, pp. 38-47, Feb., 1996.

[5] R. Chandramouli, “A Framework for Multiple Authorization Types in a Healthcare Application System,” 17th Annual Computer Security Applications Conference (ACSAC), New Orleans, Louisiana, Dec 10-14, 2001.