의료 정보 보호를 위한 역할기반 접근제어 분석 및 고찰

전경환*, 박석천**, 김성규***
*가천대학교 일반대학원 모바일소프트웨어학과
**가천대학교 컴퓨터공학과 정교수(교신저자)
***(주)MCC 이사
e-mail : aj1999@hanmail.net

The Study and Analysis of Role-Based Access Control Model for Protecting the Information

Gyeong-Hwan Jeon*, Seok-Cheon Park**, Sung-Gyu Kim***
*Dept. of Mobile Software, Gachon University
**Dept. of Computer Engineering, Gachon University(Corresponding Author)
***Dept. of Business, MCC co., ltd

요 약

개인의 의료 정보는 개인의 프라이버시에 관련되므로 민감하게 취급되어야 하는 정보이다. 이러한 개인정보 유출은 유출된 정보의 해당 당사자의 사회적 고립과 정보의 질에 따라 당사자의 생명도 위협하게 되므로 철저한 관리가 필요하다. 따라서 의사, 간호사, 환자, 일반인 등의 사용자 식별을 통해 병원 기록의 접근 통제 및 사용 권한에 따른 정보의 암호화 수준과 해당 정보에 특화된 역할기반 접근제어(Role-Based Access Control)를 제정해야 한다. 환자 자신이 자신의 의료정보를 특정한 사람에게 접근 권한을 주어 확인할 수도 있게 하고 그 외의 다른 부분들도 제어 할 수 있게 권한을 부여 할 수 있어야 한다. 본 논문은 현재 의료 및 진찰 정보 관리를 위해 RBAC모델을 기반으로 의료정보보호를 위한 접근제어 방법을 분석하고 각 정보의 객체들과 사용자 간의 효율적인 역할 분담과 한계를 통해 의료 정보의 보호방안을 고찰한다.

1. 서론

의료 기관의 환자의 의료정보는 환자 개인에게 있어 민감한 부분이다. 이는 개인의 프라이버시를 중시하는 현대 사회에서 가장 민감한 정보라고 할 수 있다. 그러므로 어느 분야의 정보데이터 보다 우선적으로 안전하게 보호되어야 한다.

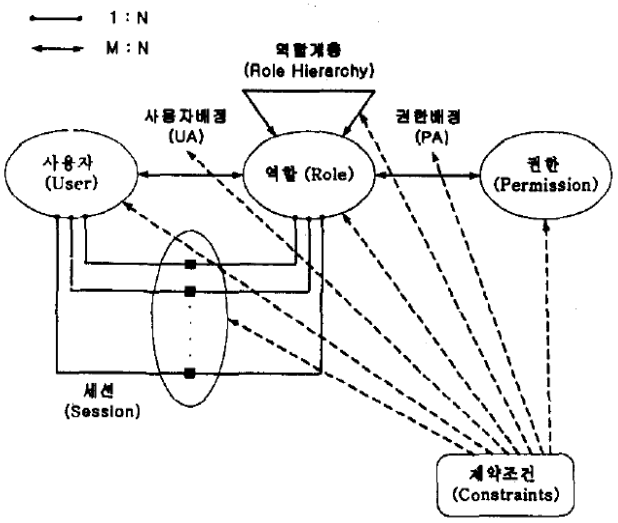
환자 개인의 의료정보는 의료법에 따라 환자 본인외에는 알리지 않는 것이 원칙이다.[8] 환자의 배우자나 자식 등 환자가 정보를 공유해도 된다고 판단되는 경우 정보를 공유 할 수는 있다. 그러나 상황에 따라서는 같은 정보가 듣는 입장으로 하여금 다른 의미를 가진다. 따라서 의료정보 만큼은 철저한 보안과 보호를 필요로 한다. 의료 정보에 접근 할 수 있는 직원에 의해 유출되는 사례는 빈번하게 나타나고 있다. 현재 의료 체계상 환자의 의료정보에 대한 모든 보호 및 보안은 의료기관이 책임지고 있다. 의료정보에 대한 관심이 고조되어 가면서, 자신 또는 가까운 사람의 의료정보를 자신이 관리하거나 감독을 하는 경우도 많이 있기 때문에 의료기업은 이에 대한 고찰이 필요하다. 게다가 스마트폰, 인터넷 등의 발달로 의료 정보의 전송이 빈번해지고 있는 추세이다. 따라서 의료 정보는 법, 의료진, 환자, 타인 등 사용자 식별을 통해 진료 기록의 접근을 통제하고 사용 권한에 따라 의료 정보접근의 제한 또는 암호화를 하여 역할기반의 접근제어를 수행하고 지금까지의 미비점에 대해서 개선해야 할 필요가 있다. 이를 위해 본 논문에서는 의료정보 객체들과 사용자간의 효율적인 역할 분담과 한계를 통해 의료정보 보호 방안을 고찰한다

2. RBAC의 개념

역할기반 접근통제(RBAC : Role Based Access Control)는 다중사용자, 다중 프로그램이 환경에서의 보안처리 요구를 만족시키기 위해 제안된 방식으로 사용자의 역할에 기반을 두고 접근을 통제하는 모델이다. RBAC은 임의적 접근통제 방식의 단점과 강제적 접근통제 방식의 단점을 보완한 접근통제 기법으로써 관리자에게 편리한 관리능력 제공, 비기술적인 정책 입안자들이 쉽게 이해할 수 있다. 사용자가 개인별로 접근권한을 설정하는 것이 아니라 사용자에게 부여된 임무를 기반으로 역할을 설정하고, 그 역할에 허용된 연산을 허용함으로써 조직이 기능변화에 따른 관리적 업무의 효율성을 꾀할 수 있다. 직무분리 원칙에 의해 조직 내에서 부여된 개인의 직무에 따라 결정되므로 시스템 상에서 오용을 일으킬 정도의 충분한 특권이 사용된 사용자를 없게 한다[3].

또한 최소한의 원칙에 따라 사용자에게 최소의 권한만

을 허용하여 권한의 남용을 방지하고 해킹 등으로부터 시스템을 보호한다. 주체와 객체의 상호관계를 통제하기 위해서 역할을 설정하고 관리자는 주체를 역할에 할당한 뒤 그 역할에 대한 접근 권한을 부여하는 방식이다. 역할이 기존 접근제어의 그룹 개념과 가장 큰 차이점은 그룹은 전형적으로 사용자들의 집합이지만 권한은 집합이 아니며, 역할은 사용자들의 집합이면서 권한들의 집합이라는 것이다. (그림 1)은 RBAC의 기본적인 모델을 보여준다. 사용자(U: User), 역할(R: Role), 권한(P:Permission), 세션(S:Session)으로 구성되어있다[8].



(그림 1) RBAC 모델

• User(U): USER는 기계나 네트워크, 또는 지능을 가진 자율적인 대리인이나 사람들이 될 수 있으며, 컴퓨터 시스템내의 정보를 사용하는 주체이다. 보통은 사람을 지칭하는 것으로 한 사용자는 한명의 사람에 대응된다. 그리고 임무분리 성질을 만족하기 위해서는 한사람이 여러 개의 사용자 식별자를 소유하지 않아야 한다.

• Role(R): 접근제어 정책을 실현하는 중요한 구조로서, 조직 내의 직급을 나타내며 고유의 의무와 권한을 갖는다. 역할로도 해석할 수 있으며 조직이나 기업에서 정의된 업무의 기능을 의미하기도 한다. 이 역할에 배정된 사용자에게는 그 업무의 기능에 따른 권한과 책임이 주어진다.

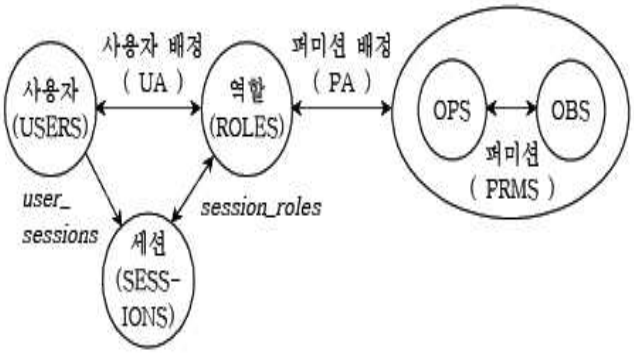
• Permission(P): 시스템의 하나 또는 그 이상의 객체에 대한 접근 모드(읽기, 쓰기, 수정 등)의 승인을 나타낸다. 퍼미션은 객체와 객체에 수행할 수 있는 연산의 집합으로 나타낼 수도 있다.

• Session(S): System의 로그인 통해 User가 수행하기 위한 작업에 대한 역할을 활성화 시킨 상태이다. 한 사용자와 여러 개의 역할들로 구성된 집합으로 사용자는 세션을 통해 자신에게 배정된 역할들 중 일부 또는 전부를 수행할 수 있다. 각각의 세션은 반드시 한 사용자와만 관련을 맺지만 각 사용자는 여러 세션과 관련을 맺을 수 있다.

• 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. 역할기반 접근제어 분석

RBAC의 기본적인 개념은 퍼미션 역할에 배정되며 사용자를 그 역할의 구성원에 소속되도록 함으로써 사용자가 퍼미션을 획득하도록 하는 것이다. 코어 RBAC(Core RBAC)은 RBAC을 수행하는데 꼭필요한 RBAC의 기본적인 개념들을 포함시켜 놓은 것으로 (그림2)와 같다.



(그림 2) 코어 RBAC

코어 RBAC는 몇 개의 데이터 요소와 관계, 그리고 기능으로 구성되어 있다. 이들 구성요소에 대한 추가된 용어와 의미에 대해 간단히 설명하면 아래와 같다. 코어 RBAC은 한 세션에 의해 활성화된 역할들이 무엇인지를 알려주는 'session_role'기능을 갖는다. 또한 한 사용자가 어떤 세션과 관련을 맺고 있는지를 알려주는 'user_ session'기능도 있어야한다. 추가된 용어 설명은 다음과 같다[5].

• 객체(OBS : Objects)는 RBAC을 구현하는 시스템에 따라 여러 가지 측면으로 간주될 수 있다. 운영체제 시스템은 객체를 파일이나 디렉토리로 정의하고, 데이터베이스 관리 시스템은 객체를 뷰나 테이블 또는 행이나 열로 간주한다. 이와는 달리 다른 시스템은 객체를 프린터나 디스크, 또는 중앙처리장치 사이클과 같이 소모성 시스템 자원으로 간주하기도 한다. 모든 경우의 객체를 코어 RBAC에서는 수용한다.

• 연산(OPS : Operations)은 RBAC시스템이 보호하는 정보객체(OBS)에 대해 수행 가능한 접근모드를 의미하는 것이다. 시스템의 형태에 따라 다르게 정의된다. 예를 들면, 파일 시스템에서의 연산은 '읽기','쓰기','수행'으로 정의될 수 있고, 데이터베이스 관리 시스템에서의 연산은 '삽입','삭제','추가','갱신' 등으로 정의할 수 있다.

• 사용자 배정

사용자 배정관계(UA : User Assignment)는 사용자가 수

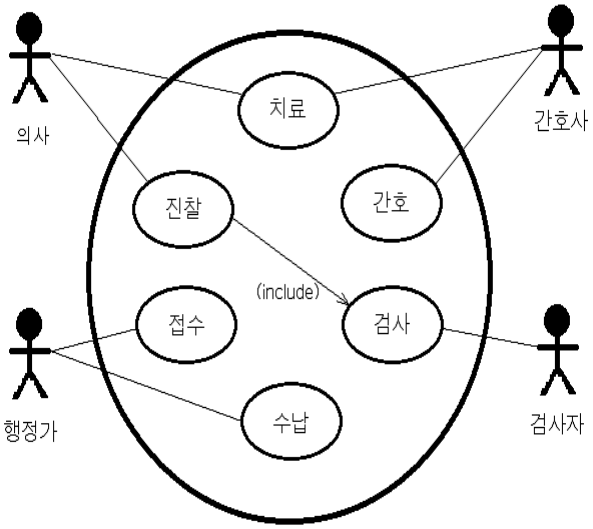
행할 수 있는 역할들을 지정하는 것이며 사용자와 역할 간에는 다대다(n to n) 관계가 성립된다. 따라서 동일한 사용자는 많은 역할에 배정될 수 있으며 하나의 역할 또한 많은 사용자에 배정될 수 있다.

• 퍼미션 배정

퍼미션 배정 관계(PA : Permission Assignment)는 역할이 수행할 수 있는 퍼미션을 배정한 관계로 역시 서로 간에는 다대다의 관계를 지니고 있다. 하나의 퍼미션은 많은 역할에 배정될 수 있고, 하나의 역할 역시 많은 퍼미션에 배정될 수 있는 특징이 있다.

4. 역할기반 접근제어 고찰

(그림 3)은 종합병원의 의료정보시스템에 대한 사용사례 다이어그램이다. 의료정보시스템 사용사례를 기반으로 역할기반 접근제어 방안을 고찰하면 다음과 같다.



(그림 3) 의료정보 시스템 사용사례

의사는 진료를 목적으로 환자의 식별정보를 제외한 모든 진료기록을 액세스(Read 또는 Write)할 수 있으며, 정밀한 진단을 위해 필요한 검사를 검사부서에 의뢰하고, 검사결과를 바탕으로 치료를 담당한다. 간호사는 간호를 목적으로 의사의 처방을 액세스(R)할 수 있으며, 의사의 처방에 따라 투약과 주사 등의 처치를 수행하고, 간호를 목적으로 환자의 간호기록을(R, W)할 수 있다. 검사자는 의사의 검사 의뢰에 따라 검사를 수행하며, 환자의 검사기록을 액세스(R, W)할 수 있다. 행정가는 병원 원무를 목적으로 환자의 검사기록을 액세스(R, W)할 수 있으며, 환자의 진료를 위한 접수 및 치료결과에 따른 수납행위를 수행할 수 있음을 나타낸다. 고찰해보면 현재의 의료정보보호에 있어 상대적으로 취약한 부분은 가장 핵심적인 인력인 의사들의 윤리성에서 비롯될 가능성이 크다.

4. 결론 및 향후 연구 방향

RBAC은 개인정보를 보호 하는데 있어서 완벽하다고 말할 수는 없다. 현재까지 정보보호의 취약점을 보면 엔드포인트에서 발생할 가능성이 크다. 이 때문에 네트워크를 제어하고 로그분석 기술을 도입하여 시스템 안정성 및 정보보안의 효율성을 강화하는 것이 우선시 되어야 한다. 이미 다른 분야의 내부정보 유출방지 솔루션은 SCM, OCC, CMF 등 다양하게 분류되어 사용되고 있다. 최근에는 내부자에 의한 정보 유출 방지에 초점을 맞춘 DLP(Data Loss Prevention)도 등장했다. DLP는 일반적으로 기업 내 인사관리 DB와 연결해 RBAC를 수행하는 기능이 제공된다. 여기서 제공하는 접근제어는 일반적으로 매체제어를 의미한다. 특정 시스템에 대한 USB, 블루투스, 와이파이, 스마트폰, CD/DVD 등의 기억매체의 접근은 인가된 내부인만이 수행한다. 그리고 내부정보에 대한 외부의 불법침입, 송수신 상의 정보 유출 등을 방지하기 위해 암호화 기술을 제공하고 필터링 기술도 사용되고 있다.

중소규모 이하의 사업체에서는 모든 보안 시스템을 도입하기란 비용적인 문제도 있지만 우선 관리 인력자체가 부족한 것이 현실이다. RBAC의 확장모델을 연구하거나 DLP, DB암호화 서비스, 방화벽 임대 서비스 등 저비용으로 보안을 할 수 있는 영역들을 차후 검토해 최소의 비용으로 최대의 효과를 낼 수 있는 연구를 하는 것이 효율적이다.

사사의 글

본 논문은 미래창조과학부의 2015년 고용계약형 SW석사과정 지원사업(과제번호:H0116-15-1003)을 지원받아 수행한 결과입니다.

참고문헌

[1] 송제민, “RBAC에 기반한 개인 맞춤형 건강 정보 제공 헬스케어 서비스 플랫폼”, 2014.

[2] 김태형, “중소 기업,병원,학교에서 필요한 개인정보보호서비스는?”, 2014.

[3] http://blog.naver.com/skddms/110185229979

[4] http://kibani.blog.me/220150763173

[5] 이봉근, “유헬스케어 서비스 환경을 위한 RBAC 기반의 프라이버시 모델”, 2011.

[6] 이정규, “클라우디 컴퓨팅에서의 역할기반 젭근제어 모델 제안”, 2011.

[7] 이형효, “RBAC 기반 개인정보보호 통합 모델”, 2010.

[8] 노승민, “의료 정보 보호를 위한 역할기반 접근 제어 모델 설계”, 2004.