프라이버시 보호를 갖는 확장된 역할기반 접근제어 모델

정회원 박 종 화*, 김 동 규**

An Extended Role-based Access Control Model with Privacy Enforcement

Chong-Hwa Park*, Dong-Kyoo Kim** *Regular Members*

요 약

최근 프라이버시 적용이 IT분야의 가장 중요한 문제의 하나로 대두되고 있다. 프라이버시 보호는 조직의 데이터 처리 시스템에 프라이버시 정책을 적용함으로써 달성 될 수 있다. 전통적인 보안 모델은 다소간 프라이버시 바인딩과 같은 기본적인 프라이버시 요구를 적용하기에 부적절하다. 본 논문은 조직에 프라이버시 정책을 적용할 수 있는 하나의 확장된 역할기반 접근제어 모델을 제안한다. 이 모델은 RBAC과 도메인-타입 적용, 그리고 프라이버시 정책을 결합함으로써 프라이버시 보호와 함께 문맥기반 접근제어를 제공한다. 프라이버시 정책은 역할에 프라이버시 등급을, 데이터에 고객의 프라이버시 선호에 따른 데이터 프라이버시 등급을 부여하는 데이터 사용 정책을 적용함으로써 달성한다. 또 이 모델을 응용에 적용하기 위하여 작은 병원 모델이 사용되었다.

Key Words : Privacy Protection, Context-Based Access Control, Purpose Binding, Data Usage Policy, Extended Role-Based Access Control

ABSTRACT

Privacy enforcement has been one of the most important problems in IT area. Privacy protection can be achieved by enforcing privacy policies within an organization's data processing systems. Traditional security models are more or less inappropriate for enforcing basic privacy requirements, such as privacy binding. This paper proposes an extended role-based access control (RBAC) model for enforcing privacy policies within an organization. For providing privacy protection and context based access control, this model combines RBAC, Domain-Type Enforcement, and privacy policies. Privacy policies are to assign privacy levels to user roles according to their tasks and to assign data privacy levels to data according to consented consumer privacy preferences recorded as data usage policies. For application of this model, small hospital model is considered.

Ⅰ. 서 론

오늘날 인터넷의 발달과 함께 건강관리 환경에서 내부적으로 컴퓨터 시스템들 사이에, 그리고 지역적으로 분산된 기관들 사이에 정보 교환에 대한 욕구가 크게 증가하고 있다. 또한 인구의 유동성 증가와 함께 환자의 데이터는 지역적으로 분산된 여러 의료 기관에 위치하게 되며, 이들 데이터를 지역적인 범위에서 또는 범국가적인 범위로 관리하여 접근이 가능하도록 할 필요가 있다. 이와 같은 분산된

* 세명대학교 소프트웨어학과 (chpark@semyung.ac.kr)
** 아주대학교 정보 및 컴퓨터공학부 (dkkim@ajou.ac.kr)
논문번호 : 030584-1231, 접수일자 : 2003년 12월 31일

의료 정보 시스템에의 접근은 무결성, 비밀성, 부인 방지 등을 제공할 뿐 만 아니라, 환자 개인의 프라이버시 보호도 제공되어야 한다. 그러나 인터넷 기술은 정보보호 보다는 정보 공유를 목적으로 최적화하기 위해 설계되어 있어, 적정 수준의 보안을 제공하지 못하고 있다. 이러한 인터넷 보안을 만족스러운 수준으로 유지하기 위한 최근의 노력들이 활발히 진행되고 있으며, 이들 대부분은 공개키 암호학(public-key cryptography)에 기반을 두고 있다. 여기서, 공개키 기반구조(PKI : Public-Key Infrastructure)는 사용자의 신원확인 등의 인증기능을 제공하기 위해 사용되고, 권한관리 기반구조(PMI : Privilege Management Infrastructure)는 사용자의 임무, 지위, 역할 등의 속성정보를 제공하기 위해 사용된다. 이와 같은 PKI, PMI 환경에서 건강관리 인트라넷 응용에 적정 수준의 보안과 환자의 프라이버시 보호를 제공하기 위해서는 PKI와 PMI 환경에서 공존할 수 있는 프라이버시 보호를 갖는 적절한 보안정책이 수반되어야 한다.

프라이버시 보호는 조직의 데이터 처리 시스템에 프라이버시 정책을 적용함으로써 이루어질 수 있다. 시스템에 적용된 프라이버시 정책은 데이터의 비밀성과 무결성을 제공한다는 측면에서 보안정책과 중복되는 면이 없지 않다. 그러나 프라이버시 보호는 접근제어를 확장하는 것에 의하여 조직에 보안정책과 함께 제공되어야 함이 제안되고 있다[12].

강제적 접근 제어(MAC: Mandatory Access Control)[9]나 임의적 접근 제어(DAC: Discretionary Access Control)[10]와 같은 전통적인 보안 모델들은 프라이버시 정책을 적용하기 위해 설계되지 않았다. 참고문헌[11]에 발표된 잘 알려진 보안 모델에 대한 프라이버시 평가 요약에서 전통적인 보안 모델들은 목적 결합(purpose binding)(하나의 목적으로 수집된 데이터는 고객의 동의 없이 다른 목적으로 사용되어서는 안 된다.)이나 필요의 원칙(principle of necessity)(데이터의 분배와 처리는 적절한 일을 위해 필요할 때 만 허용되어야 한다)과 같은 기본적인 프라이버시 보호의 요구 사항을 적용하는데 다소 부적절함을 보이고 있다.

역할기반 접근제어(RBAC: Role-Based Access Control)는 최근 임의적 접근제어와 강제적 접근제어의 유망한 대안으로 주목을 받고 있다. RBAC에서 역할(role)의 특성은 프라이버시 정책의 중요한 요소인 목적(purpose)과 관계를 갖고 있다. RBAC에서 역할은 그 역할에 할당된 사용자에게 책임과 권한이 부여된 조직에서의 일의 기능으로 정의된다. 이때 역할에 부여된 책임은 역할의 목적을 함축적으로 포함한다. 또한, RBAC은 프라이버시 보호에 중요한 문맥기반 접근제어(context-based access control)를 적용하는데 적당한 환경을 제공한다.

환자의 프라이버시를 보호해야 하는 건강관리 응용시스템의 보안정책은 HIPAA 보안 표준[1]에 따를 것을 권고 받게 되는데, 이 표준에서 건강관리 응용시스템은 사용자기반(user-based) 접근제어, 역할기반(role-based) 접근제어, 그리고 문맥기반(context-based) 접근제어의 특징을 가져야 함을 규정하고 있다. 문맥기반 접근제어는 데이터에 접근하는 사용자와 접근하는 데이터의 유형을 고려할 뿐만 아니라, 시도된 처리의 문맥까지도 고려한다. 프라이버시를 인식할 수 있는 환경에서 문맥은 역할의 책임, 특정 고객에 의해 동의 된 데이터 사용 정책, 그리고 역할의 데이터 접근을 위한 주체 등이 될 수 있다.

문맥기반 접근제어를 제공하는 모델로 DAFMAT (Dynamic Authorization Framework for Multiple Authorization Types)[6] 는 RBAC과 DTE가 조화된 건강관리 응용 시스템을 제안하였다. DAFMAT의 가장 중요한 특성은 문맥기반 권한부여, 긴급 권한부여와 같은 다중 유형의 권한부여를 지원하는 것이며, 또 권한부여 요청을 체계화하여 요청의 정당성을 결정하기 위한 논리 유도 권한부여 엔진을 사용하는 것이다. 그러나 프라이버시 보호 정책을 적용하는데 있어 DAFMAT의 한계는 목적과 데이터 사용 정책을 모델링 하지 못하고 있다는 것이다.

따라서 본 논문에서 제안한 모델은 DAFMAT를 기반으로 목적 결합(purpose binding)과 정책에 의한 데이터 사용제어를 적용하여 프라이버시 보호를 제공하는데 그 목적이 있다. 즉, 역할기반 접근제어(RBAC) 모델에 다음의 사항들을 결합하여 프라이버시 보호를 갖는 문맥기반 접근제어를 제공한다.

- 사용자 역할의 책임에 따라 프라이버시 등급 할당
- 고객의 프라이버시 선호에 따라 데이터에 프라이버시 등급을 부여하는 데이터 사용 정책 적용
- DTE(Domain-Type Enforcement) 메커니즘

본 논문의 구성은 다음과 같다. Ⅱ장에서 관련 기술이 언급되고, Ⅲ장에서 본 논문에서 제안된 모델이 기술되며, Ⅳ장에서 제안된 모델의 응용이 다루어지고, Ⅴ장에서 결론을 맺는다.

Ⅱ. 관련 기술

1. 역할기반 접근제어(Role-Based Access Control : RBAC)

RBAC는 보안 분야에서 전통적인 임의적 접근제어와 강제적 접근제어의 유망한 대체로서 주목을 받아왔다. 1996년 이래로 ACM RBAC/SACMAT 일련의 워크숍은 이 연구 경향이 주목받고 있음을 보이는 예이다. 최근 RBAC는 NIST 표준으로 제안되었다[2].

RBAC에서 사용자는 객체에 접근이 허용된 허가를 가진 역할에 할당되었을 경우, 해당 객체에 접근할 수 있다. RBAC의 중요한 이정표는 RBAC96 모델이다[3]. RBAC96은 여러 사용자와 여러 자원 사이의 복잡한 시스템에서 권한부여를 관리하는 RBAC 모델 family를 정의하였다. RBAC의 역할의 개념은 조직의 기능적 역할과 유사하다. 따라서 RBAC은 조직의 보안정책을 모델링하는데 직관적인 방법을 제공한다. 후에 RBAC은 정책 중립적인 모델임이 입증됐는데 이는 RBAC이 어느 특정한 보안 정책을 포함하는 대신 그 정책을 표현하는 방법이기도 하다는 것이다. 또한 RBAC은 전통적인 강제적이고 임의적인 접근제어 정책을 포함하는 구성을 가질 수 있다[7]. 그리고 RBAC은 여러 잘 알려진 보안 원칙인 정보 은폐(information hiding), 특권 최소화(least privilege), 의무 분리(separation of duties), 데이터 추상화(data abstraction) 등을 지원한다. RBAC의 또 다른 장점은 역할이 사용자의 교체나 일의 재 할당에 비해 지속적이므로 권한부여의 관리가 전통적인 보안 모델에 비해 쉽다는 것이다. RBAC에서 조직 내의 역할에 허가를 할당함은 복잡성, 비용, 오류의 가능성을 줄이는데 기여하기도 한다. 또한 RBAC은 웹 상에서 보안 정책을 적용하기 위해 사용되기도 했고[4], 다중 도메인 환경에서의 사용 가능성이 확인되기도 했다[5].

2. 메인-유형의 적용(Domain-Type Enforcement : DTE)

DTE[13]은 주체에 도메인 라벨 그리고 객체에 유형 라벨을 사용하므로 객체에 대한 주체의 접근을 제한하는 하위 수준의 강제적 접근제어 기법이다. DTE과 RBAC 사이에 다른 점은 RBAC은 사용자와 역할이 관련되어 있어, 역할이 어떻게 사용자에게 가능한 연산을 제한하는지를 설명한다. 반면에 DTE은 주체를 도메인에 연관지어, 어떻게 도메인이 주체에 가용한 연산을 제한하는지를 설명한다. 그러나 본 논문에서는 역할에 도메인 라벨 그리고 주체에 유형 라벨을 사용하여 역할이 다른 도메인에 접근을 어떻게 제한하는지 또 어떻게 가용한 연산을 제한하는지를 설명한다.

3. 프라이버시 보호(Privacy Protection)

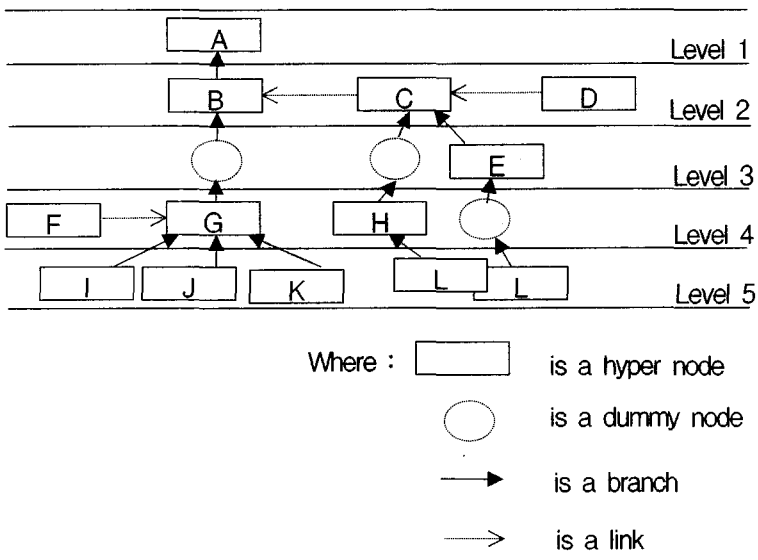

그림 1. Hyper Node Hierarchy(HNH)

프라이버시는 자주 사회적, 도덕적, 그리고 법적인 개념에서 고려되어진다. 프라이버시는 간단히 말해서 혼자가 되기 위한 권리이다. 프라이버시를 더 명확하고 공통적으로 정의하면 프라이버시는 개인, 그룹, 기관에서 그들의 정보를 다른 사람에게 언제, 어떻게, 어느 정도의 범위까지 공개 할 것인지를 결정하기 위한 권리이다. 이와 같은 프라이버시의 보호는 건강관리나 금융 등 많은 분야에서 인터넷과 전자상거래의 발달과 함께 중요한 관심의 대상이 되고 있다.

건강 정보 시스템(Health Information System : HIS)에서 진료 활동이나 또는 병원의 병동에서 치료 등에 관한 환자의 개인적인 자료나 진료 자료는 엄격하게 보호되어야만 한다. 이러한 보호는 명확하게 한정된 프라이버시 등급(privacy level)을 역할과 고객의 프라이버시 선호에 따른 데이터에 적용함으로써 얻어 질 수 있다. 프라이버시 등급과 RBAC에서의 역할과는 강한 유사성이 있다. 프라이버시 등급은 역할 계층에서 역할(노드)의 위치(position)의 수단으로 적용될 수 있다. 역할 계층의 역할에 미리 정의된 한계를 초과 할 수 없는 프라이버시 등급이 할당된다. 따라서 이것은 계층의 구성을 지배하는 하나의 제한이 된다. 즉 하나의 주어진 역할에 프라이버시 등급을 부여함에 있어 필연적으로 자신의 직속 조상의 역할의 프라이버시 등급 보다 하나 적은 프라이버시 등급을 할당하지는 않는다(예를 들면 하나의 역할에 프라이버시 등급 2가 부여되고 그 조상 역할에 프라이버시 등급 4가 할당된 경우). 이를 위해 아래의 (그림 1)에서와 같이 두 역할 노드 사이에 빈 노드(dummy node)가 사용된다. 모든 계층은 최소한 최상(최하)의 프라이버시 등급이 할당되는 초기 노드들의 한 등급을 갖는다. 다른 모든 노드들은 그 노드들의 조상의 자손이 되고 다른 등급에 위치한다.

위와 같은 특징들을 지원하기 위해 eMEDAC[7]에서 보안등급을 위해 사용한 (그림 1)과 같은 Hyper Node Hierarchy(HNH)를 본 논문에서는 프라이버시 보호를 위해 사용한다.

HNH는 hyper node들로 구성된다(그림 1). 각각의 hyper node는 다른 hyper node에 branch 나 link에 의해 연결된다. 이 때 branch들은 HNH를 구성하기 위해 hyper node들을 연결하는 데 사용되며, 다중 상속이 지원된다. 각 hyper node의 branch는 같은 HNH에 있는 직속 상위 등급의 hyper node를 지향한다. link들 또한 방향성 연결로 같은 등급의 hyper node들 간의 연결을 위해 사용되는데, 이로 인해 다른 HNH가 시작된다.

보안 등급을 유도하기 위해 HNH 개념을 사용하는 eMEDAC은 모든 사용자가 데이터베이스에 접근하기 위해 반드시 통과해야 하는 3단계로 구성된 보안정책이다. 첫 번째 단계에서는 사용자의 신원확인과 인증이 수행되며, 인증 후에 그 사용자에게 하나의 역할에 할당된다. 두 번째 단계에서는 허가를 상속하기 위해 HNH에 기반을 둔 URH(User Role Hierarchy)가 이용되어 지며, 세 번째 단계에서는 보안 등급을 유도하기 위해 URH가 사용되어진다. 어쨌든 eMEDAC은 두 번째 단계에서 필요한 임의적 접근제어(DAC)를 지원하기 위해 RBAC의 허가 메커니즘과 접근 행렬을 사용하고 있고, 세 번째 단계에서는 민감한 환자 데이터에 접근하기 위해 강제적 접근제어(MAC) 요구사항들을 만족하는 역할 계층과 URH를 사용하고 있다. 우선 임의적 접근제어 방식이나 강제적 접근제어 방식과 같은 전통적인 보안 모델들은 프라이버시 정책들을 적용하기에 부적절하고, 접근 행렬이나 시스템 테이블의 사용은 프라이버시 보호에 적합한 문맥 기반 접근제어를 지원하기 위한 기반을 제공할 수 없다.

Ⅲ. 제안된 모델

이 논문에서 제안한 모델은 확장된 역할기반 접근제어 모델로서, RBAC과 DTE를 결합하여 문맥기반 권한부여와 긴급 권한부여와 같은 다중 권한부여를 지원하는 DAFMAT[6]의 하부구조에 프라이버시 보호를 위해 역할의 책임에 따라 프라이버시 등급을 할당하는 목적 결합(purpose binding)을 적용하고, 고객의 선호에 따른 정책 유도 데이터 사용 제어를 사용하여 프라이버시 보호를 갖는 문맥기반 권한부여를 제공한다. 이 장에서는 이 모델의 구성요소들과 그 들의 관계를 상세하게 설명한다.

1. 제안된 모델의 프라이버시 정책

이 논문에서 제안한 모델은 DAFMAT 보안모델에 기반을 두며, 다음의 원칙에 기초한다.

-. 모든 인가된 사람은 시스템에 접근할 권한을 갖는다. 이로 인해 시스템에 직접 접근하려는 사용

자는 시스템에 로그인 할 수 있는 계정을 가져야만 한다. 이 계정은 미리 정의된 사용자 역할에 연관되어진다. 그리고 이 역할은 응용에서 사용자의 일을 나타낸다.

-. 모든 사용자 역할은 프라이버시 등급을 가지며, 그 프라이버시 등급은 사용자 역할의 책임과 목적을 나타낸다.

-. 모든 데이터 세트에는 고객의 프라이버시 선호에 따라 프라이버시 등급이 부여되는 데이터 사용 정책이 적용한다.

-. 접근요청에 대한 권한부여에서 프라이버시 보호를 목적으로 한 지배관계는 Bell-LaPadula[8] 모델에 기초한다. 즉 접근을 요청하는 사용자 역할의 프라이버시 등급이 접근하고자 하는 데이터에 데이터 사용정책에 의해 부여된 데이터 프라이버시 등급보다 크거나 같아야 한다.

2. 제안된 모델의 구성 요소

제안된 모델은 사용자, 역할, 프라이버시 등급, 주체, 도메인, 주체, 객체 유형, 객체 정책 등으로 구성된다. (그림2)는 제안된 모델의 구조를 보이고 있다.

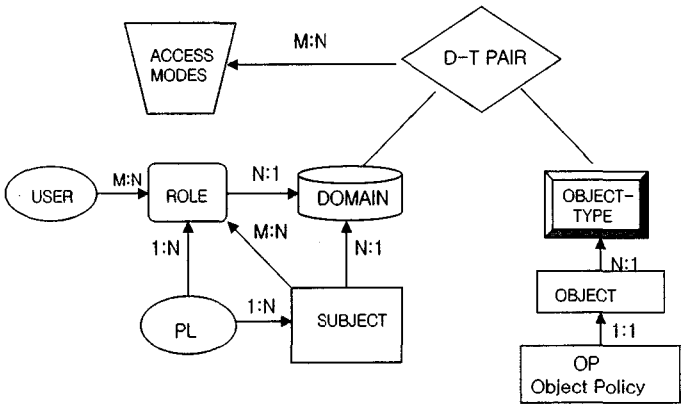

그림 2. 제안된 모델

3. 제안된 모델에서의 개체간의 관계

제안된 모델(그림2)에서 개체들 간의 관계는 출발개체와 목적개체 사이에 다대다(M:N), 다대일(N:1), 일대다(1:N), 또는 일대일(1:1) 관계의 사상을 화살표로 나타낸다.

- User_Role(user, role) : 다대다
한 사용자에 여러 역할들이 부여될 수 있고, 또 하나의 역할에 여러 사용자가 할당될 수 있다.
- Role_Domain(role, domain) : 다대일
하나의 도메인은 조직에서의 한 기능적 분야를 나타낸다. 따라서 여러 역할이 한 도메인에 연관되어지며, 하나의 역할은 항상 특정 도메인에 속한다.
- Role_PL(role, privacy level) : 다대일
하나의 프라이버시 등급이 하나의 역할에 할당되어진다. 그리고 여러 역할이 하나의 프라이버시 등급을 가질 수 있다.
- Subject_Role(subject, role) : 다대다
주체는 사용자를 대신하여 특정한 일(task)을 수행한다. 따라서 하나의 주체가 여러 역할들에 의해 호출될 수 있다. 또 하나의 역할은 지정된 일을 수행하기 위해 여러 주체를 호출할 수 있다.
- Subject_PL(subject, privacy level) : 다대일
주체는 특정 데이터 프라이버시 등급을 갖은 데이터에 대해서만 일을 수행한다. 여러 주체들이 하나의 데이터 프라이버시 등급에 연관될 수 있다.
- Subject_Domain(subject, domain) : 다대일
각 주체는 하나의 특정 도메인과 연관되어지며, 하나의 도메인에 여러 주체들이 관련된다.
- Object_ObjectType(object, object-type) : 다대일
하나의 객체유형(object type)은 관련된 정보를 가지는 객체들의 모임이다. 따라서 각 객체는 특정한 객체유형에 사상되며, 하나의 객체유형은 여러 객체를 포함한다.
- Object_ObjectPolicy(object, object-policy) : 일대일
각각의 객체(object)는 그 객체의 사용에 관한 유일한 정책을 갖는다.

- DTE_Entry(domain, object-type, access-modes) : 다대다

도메인-유형이 도메인-유형 접근 행렬 표(Domain-Type Access Matrix : DTE table)에 나타낸다. DTE table의 각 항목에 허용 할 수 있는 접근모드가 표시된다.

4. 역할의 프라이버시 등급

역할의 프라이버시 등급은 eMEDAC의 HNH에 기초한 사용자 역할계층(User Role Hierarchy : URH)으로부터 유도되어진다. 사용자 역할 계층(URH)은 최소한 하나의 "All Users"라는 사용자 역할을 포함한다. 이는 모든 사용자에게 할당되는 공통 역할을 나타낸다. 이 역할은 특정한 사용자 역할들로 구성되는 하나 또는 그 이상의 등급으로 세분화된다. 사용자 역할 계층에서 프라이버시 등급의 수는 사전에 정의되어 지며, 필요한 세분화의 한계에 의존한다. 사용자 역할 계층의 가장 위(top)에 위치하는 사용자 역할은 가장 낮은 프라이버시 등급인 등급 1이 된다. 차례로 링크(link)의 사용은 새로운 계층에 이르게 하고 같은 절차가 특정 응용에서 만족되어 질 때까지 반복되어 진다.

주어진 역할의 프라이버시 등급을 유도하기 위해, 우리는 프라이버시 등급을 1로 초기화한다. 그때 계층에서 처음 특정 역할을 발견하면 상위 역할로 connection(branch 또는 link)을 따라 계층의 top으로 올라가게 된다. 만약 그 connection이 branch면 등급에 1을 더한다. 이 과정은 사용자 역할 "All Users"에 도달할 때까지 계속된다.

다음의 사용자 역할 계층은 eMEDAC에서 사용한 예를 도메인별로 수정 분류한 것이다. 역할들은 데이터 집합과 마찬가지로 Medical Decisions, Administration, Patient Hospitalization 그리고 Logistics 등 4개의 도메인으로 나누어진다.

표 1. 정의된 사용자 역할들

Domains	User roles	Abbrev.	Domains	User roles	Abbrev.
Medical Decisions	Doctor	D	Patient Hospitalization	Nurse	N
	Personal doctor	DP		Head Nurse	NH
	On duty doctor	DO		On duty nurse	NO
	Head doctor	DH		Training nurse	NT
	Medical	M		Ward	W
Administration	Administration	A	Logistics	Logistics	L
	Administration Staff	AS		Logistics Staff	LS

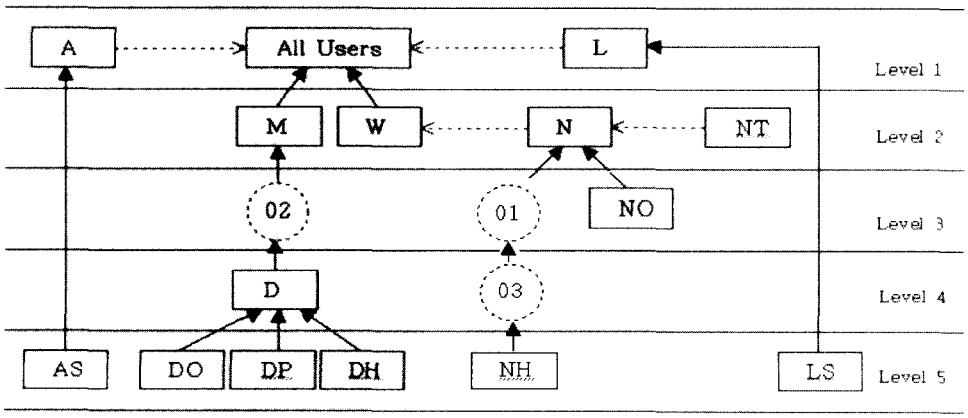

그림 3. 사용자 역할 계층

5. 데이터 사용 정책

그림 2의 제안된 모델에서 Object-policy는 실제적으로 데이터 사용 정책이다. 데이터 사용 정책은 고객의 선호에 따라 각각의 데이터에 프라이버시 등급을 부여하는 정책으로 프라이버시 등급에 따른 데이터 집합 계층(Data Set Hierarchies : DSH)으로 표현될 수 있다. 데이터 집합 계층의 가장 위(top)에 위치한 데이터 집합은 가장 낮은 수준의 프라이버시를 갖으며 프라이버시 등급 1로 초기화한다. 데이터 프라이버시 등급(data privacy level)의 수는 사전에 정의되어 지며, 계층을 따라 아래로 내려갈 때 프라이버시 등급이 1 씩 증가한다.

각 노드에 할당된 데이터 집합은 사용자 역할들이 역할 수행을 위해 알 필요와 책임 그리고 프라이버시 보호를 위한 설계 방법에 의해 적용되는 특정 프라이버시 제한에 의존한다. 다음의 데이터 집합 계층에 대한 실행 예는 (그림 4) 그리고 (표 2)와 같다.

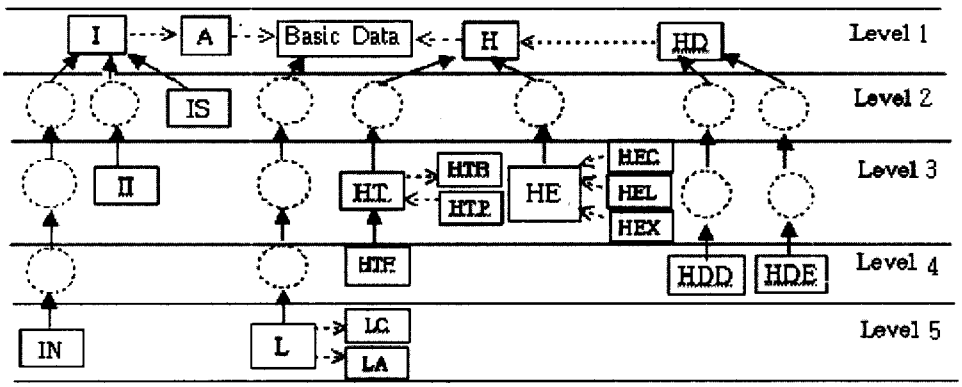

그림 4. 데이터 집합 계층(DSH)

표 2. 도메인별 데이터 집합

Domains	Data Sets	Abb	Domains	Data Sets	Abb
Administration	Administration	A	Patient Hospitali--zation	Patient Hospitalization	H
	Patient Identification	I			
	Patient Demographic Data	IN		Therapeutic Treatments	HT
	Patient Social Data	IS		Physiotherapy	HTP
	Insurance Data	II		Pharmaceutical	HTF
Logistics	Logistics	L		Radio Treatment	HTR
	Cost-accounting	LC		Exam Orders & Results	HE
	Administrative data	LA		Clinical	HEC
Medical Decisions	Medical Decisions	HD		Laboratory	HEL
	Diagnoses	HDD		X-ray	HEX
	Expectations	HDE			

6. 개체 간 관계에 대한 제한

개체들간의 관계는 제한들에 의해 한정되어질 수 있다. 제한들은 RBAC에서 가장 중요한 특징 중의 하나이며, 의무분리(separation of duties)와 같은 보안요구를 표현하는데 사용된다. 다음의 제한에서 ∀은 "for any"를, ∃는 "there exists"를, ∧는 "logical and"를, 그리고 ⇨는 "implies"를 나타낸다.

제한 1 : 주체를 불러일으키는 모든 역할들은 주체와 연관된 같은 유일한 도메인에 할당되어져야 한다.

∀(subject, domain, role),
Subject_Domain(subject, domain) ∧
Role_Domain(role, domain) ⇨
Subject_Role(subject, role)

제한 2 : 모든 역할에는 각각 하나의 프라이버시 등급이 주어지고, 이 프라이버시 등급이 주체의 데이터 검색과 연관되어 질 때 그 역할과 주체는 관련되어 진다.

∀(role, subject, privacy-level), Role_PL(role, privacy-level) ∧ Subject_PL(subject, privacy-level) ∧ GTE(RolePL(role), SubjectPL(subject)) ⇨ Role_Subject(role, subject)

*(GTE: greater than or equal)

Ⅳ. 제안된 모델의 응용

제안된 모델을 설명하기 위해 간단한 응용을 제시한다. 이 응용에서 4명의 사용자(John, Smith, Susan, Patricia)에게 병원의 각각 다른 부서에 4개의 역할이 할당되었다고 가정하자. 이 때 개체와 개체간의 관계가 다음과 같다.

1. 응용에서 개체와 개체간의 관계

Users = {John, Smith, Susan, Patricia}
Roles = {A, L, NH, DP}
A: Administration, L: Logistics
NH: Head Nurse, DP:Personal Doctor
Domains = {AD, LD, PHD, MDD}
AD: Administration Domain,
LD: Logistics Domain
PHD: Patient Hospitalization Domain,
MDD: Medical Decision Domain
Subjects = {IDP, CAP, XRP, DGP}
IDP: Insurance Data Proc,
CAP: Cost Accounting Proc
XRP: X-Ray Proc,
DGP: Diagnoses Proc

User-Role Assignment = {User_Role(John, A), User_Role(Smith, L), User_Role(Susan, NH), User_Role(Patricia, DP)}
Role-Domain Mapping = {Role_Domain(A, AD), Role_Domain(L, LD), Role_Domain(NH, PHD), Role_Domain(DP, MDD)}
Subject-Domain Mapping = Subject_Domain (IDP, AD), Subject_Domain(CAP,LD), Subject_Domain(XRP, PHD), Subject_Domain(DGP, MDD)}
Subject-Role Mapping = {Subject_Role(IDP, A), Subject_Role(CAP, L), Subject_Role(XRP, NH), Subject_Role(DGP, DP)}

Domain-Type Access Matrix(C: create, U: update, D: delete, V: view) :

표 3. 도메인-타입 접근 행렬

Domain	Object-Type / Access Modes			
	Administration Type	Logistics Type	Patient Hospitalization Type	Medical Decision Type
AD	C,U,D,V	V		
LD	V	C,U,V		
PHD	V		C,U,V	V
MDD	V		V	C,U,V

2. 제안된 모델에서의 프라이버시보호

앞에서 제안한 권한부여 절차를 통해 여러 데이터 사용자의 요청들을 시험하고, 그 요청들을 허가할 것인지 또는 거부할 것인지를 분석한다.

요청 1: 사용자 John이 Insurance Data Procedure (IDP)를 호출하여, Insurance Data에 접근을 요청한다.

Ⅲ-6의 개체 간 관계에 대한 제한 1에 의해 John의 역할인 Administration(A)이
Administration Domain과 연관되는지
Role-Domain Mapping을 통하여 확인하고, IDP가

Administration Domain에 속하는지를 Subject-Domain Mapping을 통하여 확인한 후, Subject-Role(IDP, A) 즉 A와 IDP의 연관성을 확인한다. 또 Ⅲ-6의 개체 간 관계에 대한 제한 2에 의해 John의 역할인 A의 privacy level를 계산한다 (RolePL(A)=1). 그러나 IDP가 DSH의 privacy level 3(SubjectPL(IDP)=3)에 위치하므로 제한 2가 만족되지 않아 John의 역할인 A에 의한 IDP의 접근이 허용되지 않는다.

요청 2: Head Nurse(NH)의 역할을 갖는 Susan이 X-Ray Procedure(XRP)를 호출하여 X-Ray 결과에 접근을 요청한다.

Ⅲ-6의 개체 간 관계에 대한 제한 1에 의해 NH가 Patient Hospitalization Domain(PHD)과 연관되는지 Role-Domain Mapping을 통하여 확인하고, XRP가 PHD에 속하는지 Subject-Domain Mapping을 통하여 확인한다. 또 NH와 XRP의 연관성을 Subject-Role(XRP, NH)을 통하여 확인한 후, Ⅲ-6의 개체 간 관계에 대한 제한 2에 의해 NH의 privacy level을 계산한다(RolePL(NH)=5). 이때 XRP가 DSH의 privacy level 3(SubjectPL(XRP)=3)에 위치하므로 제한 2가 만족되어 접근이 허용된다.

요청 3: Head Nurse(NH)의 역할을 갖는 Susan이 Expectations Procedure(EPP)를 호출하여 Medical Decisions 도메인의 Expectations 결과를 수정(update)할 것을 요청한다.

도메인-타입 접근 행렬(Domain-Type Access Matrix)에 의해 Patient Hospitalization Domain (PHD)에 속하며 privacy level 5를 갖는 Susan의 역할인 NH는 DSH의 privacy level 4에 위치한 Medical Decision Type인 Expectations Procedure (EPP)에 접근할 수 있다. 그러나 도메인-타입 접근 행렬에 의해 오직 참조(view) 만 허용되므로 요청 3은 거절된다.

위의 예들은 제안된 모델이 역할기반 접근제어(RBAC)에 프라이버시 보호 개념을 바인딩 할 수 있음과 정책 유도 데이터 사용 제어(policy-driven data usage control)를 적용 할 수 있음을 보이기 위한 것이다. 본 논문은 많은 역할과 많은 주체를 갖는 커다란 조직의 경우는 고려하지 않았다.

Ⅴ. 결 론

프라이버시 보호는 조직의 데이터 처리 시스템 안에 프라이버시 정책을 적용함으로써 이루어질 수 있다. 따라서 프라이버시 보호는 시스템 보안과 함께 고려되어야 하고, 데이터 관리 기술들과 결합되어야 한다. 이 논문에서 제안한 모델은 프라이버시를 적용하기 위하여, 문맥기반 접근제어를 제공하는 확장된 역할기반 접근제어 모델에 사용자 역할의 책임에 따라 프라이버시 등급을 할당하고, 고객의 프라이버시 선호에 따라 데이터에 프라이버시 등급을 부여하는 데이터 사용 정책을 적용하여, 접근을 요청하는 사용자 역할의 프라이버시 등급이 접근하고자 하는 데이터의 데이터 프라이버시 등급보다 크거나 같아야하는 프라이버시 관리를 결합하였다. 이 모델은 조직의 관점에서 보안을 제공할 뿐 아니라, 고객의 관점에서 고객의 프라이버시를 보호한다.

어쨌든 본 논문에서 제안한 모델이 모든 프라이버시 문제를 해결하지는 못한다. 수집된 고객의 데이터를 보호하는데 초점이 맞추어져 있으며, 또 역할기반 접근제어(RBAC)에 프라이버시 보호 개념을 바인딩 할 수 있음과 정책 유도 데이터 사용 제어(policy-driven data usage control)를 적용 할 수 있음을 보이기 위한 것이다. 여러 다른 프라이버시 문제들, 예를 들면, 데이터 마인닝(data mining)에 의한 프라이버시 침입, 익명(anonymity)과 같은 문제들은 이 모델의 범위 밖에 있다. 본 논문은 오직 역할기반 접근제어(RBAC)에 프라이버시 보호를 통합하는 모델을 제시하는데 그 목적이 있다.

참 고 문 헌

[1] Security and Electronic Signature Standards; *Proposed Rule. Federal Register*, Vol 63, No. 155, August 12, 1998.

[2] David F. Ferraiolo, Ravi Sandhu, Serban Gavrial, et al., "Proposed NIST Standard for Role-Based Access Control," *ACM Transactions on Information and System Security*, Vol 4 No.3, pp. 224-274, August 2001.

[3] Ravi S. Sandhu, Edward J. Coyne, Hall L. Feinstein, Charles E. Youman,"Role-Based Access Control Models," *IEEE Computer*, Vol

29 Issue 2, pp. 38-47, Feb.1996.

[4] Joon S. Park, Ravi Sandhu, Gail-Joon Ahn,"Role-Based Access Control on the Web," *ACM Transactions on Information and System Security*, Vol 4 No.1. pp. 37-71, Feb.2001.

[5] James B. D. Joshi, Walid G. Aref, Arif Ghafoor, Eugene H. Spafford, "Security Models for Web-Based Applications," *Communications of the ACM*, Vol 44 No.2, pp.38-44, Feb. 2001.

[6] Ramaswamy Chandramouli, "A Framework for Multiple Authorization Types in a Healthcare Application System," *Proc. of the 17th Annual Computer Security Applications Conference (ACSAC 2001)*, pp. 137-148,IEEE, 2001.

[7] Mavridis I., Pangalos G., Khair M., "eMEDAC : Role-Based Access Contorl Supporting Discretionary and Mandatory Features," *Proceedings of 13th IFIP WG 11.3 Working Conference on Database Security*, Seattle, Washington, USA, 1999.

[8] Castano S., Fugini M., Martella G., Samarati P., Database Security, *Addison Wesley publishing company*, 1994.

[9] Ravi S. Sandhu, "Lattice-Based Access Control Models," IEEE Computer, Vol. 26 Issue 11, pp. 9-19, Nov. 1993.

[10] R. Sandhu, P. Samarati, "Access Control: Principles and Practice," IEEE Communications Magazine, Vol. 32 Issue 9, pp. 40-48, Sep. 1994.

[11] Simone Fischer-Hubner, "IT-Security and Privacy," Lecture Notes in Computer Science 1958 (LNCS 1958), Springer-Verlag, 2001.

[12] Calvin S. Powers, Paul Ashley, Matthias Schunter, "Privacy Promises, Access Control, and Privacy Management," Proc. of the 3rd International Symposium on Electronic Commerce, pp. 13-21, IEEE, 2002.

[13] John Hoffman, "Implementing RBAC on a Type Enforced System," Proc. of the 13th Annual Computer Security Applications Conference, pp. 158-163, IEEE, 1997.

박 종 화(Chong-hwa Park) 정회원

1974년 2월 : 숭실대학교 전자공학과 졸업
1990년 1월 : 미국 Syracuse 대학교 컴퓨터공학과 석사
1976년~1978년 : (주)CDC
1979년~1981년 : 전자통신 연구원
2002년 : 아주대학교 컴퓨터공학과 박사수료
1994년 3월~ 현재 : 세명대학교 소프트웨어학과 조교수
<관심분야> 정보보호, 시스템 소프트웨어 보안, 네트워크 보안

김 동 규(Dong-Kyoo Kim) 정회원

1973년 2월 : 서울대학교 공과대학 응용수학과 졸업
1979년 2월 : 서울대학교 자연과학대학원 전자계산학과 석사
1984년 : 미국 Kansas State University 전자계산학과 박사
1986년~IEEE 802.4, 802.6, 802.10 Working Group Member
1979년~현재 : 아주대학교 정보 및 컴퓨터공학부 교수, Asiacrypt '96 조직위원장, 건설교통부 항공교통관제소 신공항 교통관제 시스템 평가위원회 위원, 한국과학기술연구소 연구원, 한국통신학회 상임이사, 한국정보보호학회 부회장 역임
<관심분야> 컴퓨터 통신, 정보보호, 프로토콜 엔지니어링