공개키 안에서 Role-Based 접근제어 모델링에 관한 연구

방극인* · 이 준*

A Study on Role-Based Access Control Modeling in Public Key Infrastructure

Geuk-In Bang* · Joon Lee*

요 약

멀티미디어, 인터넷 환경에서 서버 시스템의 활용이 일반화 됨에 따라, 시스템에 저장된 모든 자료의 보안을 위한 권한 부여나 접근 제어와 같은 상위 수준의 보안 메카니즘이 요구되는 현실이다. 또한 분산 환경에서는 시스템내에 저장된 정보들의 정형화된 스키마의 부재, 비체계성 등으로 인하여 보다 복잡한 체계의 보호기술이 필요하게 되었다.

본 논문에서는 일반적인 접근제어 방식을 고찰, 분석하고 기본적인 모델링을 정리하여 설명하였고, RBAC(Role-Based Access Control) 모델링의 모듈들을 분리하고 각 모듈들에 대한 역할을 할당한 후, 기존의 접근제어 모델링과 RBAC 모델링을 혼합 사용하여 새로운 접근제어 모델링을 제시한다.

ABSTRACT

According as practical use of server system is generalized in multimedia and internet environment, the security of all data that is stored to system is actuality that security mechanism of high level such as competence grant or access control is required. Also, standardization of informations that is stored in system in scattered environment protection technology of more complicated system by absence of done schema, non-systemicity etc.

Therefore in this paper. General access control way explained basic modeling because enough investigate and analyze general access control way. And assigning role about each modules separating module of RBAC(Role-Based Access Control) modeling, existent access control modeling and RBAC modeling using mixing new access control modeling present.

Ⅰ. 서 론

정보화 사회에서 정보의 홍수를 헤쳐 나가기 위해서는 네트워크 상에서 정보의 보안과 안전성은 그 무엇 보다도 중요하다. 컴퓨터의 보급 확산과 공용 네트워크의 발전을 통해 세계 곳곳의 정보를 한눈에 볼 수 있는 시대가 도래하고 있는 반면에 사용자들은 단순한 통신에서 벗어나 다자간 통신회의 및 의료 분야에서 원격진단 및 상담 등 다양한 서비스를 요구하고 있다.

그러나 이러한 컴퓨터 발전 및 네트워크 환경의 대중화에 비례하여 정보의 보호와 안전성 문제는 더욱 심각해지고 있다. 네트워크 서비스 중 가장 대중화되어 있는 인터넷의 경우 데이터 전송중 제 3자에 의해 정보가 가로채질 수 있으며 또한 서버가 침입자를 막지 못하였을 경우 막대한 피해를 입을 수 있다. 이러한

*조선대학교 컴퓨터공학과

접수일자 : 2002. 6. 17

침입자로부터 정보를 보호하고 데이터의 흐름에 안전성을 더하기 위해 암호화 기술이 쓰여지고 있다. 그러나 지금까지의 암호화 기법은 데이터의 사이즈가 커질 경우 암호화 자체의 연산 시간으로 인하여 시스템에 접근하는데는 상당한 시간이 지연된다. 멀티미디어 데이터의 경우 기존의 암호화 방식으로 연산 시간은 물론 시스템 자체에 상당한 부하를 주게되며 실시간 데이터의 전송이 필요할 경우에도 기존의 시스템에서는 부적절할 수밖에 없다. 특히 최근의 암호화 시스템은 하드웨어보다는 소프트웨어적으로 구현되고 있는 추세이므로 기존 정보 보호의 모델링에서 보다 더 빠른 접근제어 모델링이 요구되고 있다.

본 연구는 이러한 보안 문제점을 해결하기 위하여 기존의 보안 시스템을 충분히 살펴보고 기본시스템 구조에 RBAC(Role-Based Access Control)기법을 접목시켜 새로운 접근제어 설계 모델링을 제시한다.

II. 정보보안의 접근제어 모델링

보안은 크게 물리적 보호와 논리적 보호의 두 가지 범주로 나눌 수 있다. 물리적 보호는 우리가 흔히 생각하는 강도, 도난 등으로부터 개인이나 기업의 재산과 생명 등을 보호하는 것이고 논리적 보호는 그 개념 면에서는 물리적 보호와 비슷하지만 적용범위가 크게 다르다. 논리적 보호는 네트워크 보안 또는 정보 보안이란 환경적인 재난이나 정보 통신망의 오류, 컴퓨터의 악용으로부터 정보 통신망의 자원을 보호하는 것이며, 또한 정보의 수집, 가공, 저장, 검색, 송신, 수신 중에 정보의 훼손 변조, 유출 등을 방지하기 위한 관리적, 기술적 정보보호 시스템을 말한다. 다시 말하면, 정보보안이란 정보의 무결성, 비밀성, 가용성을 보장하고 정보의 정상적인 유지를 위하여 인위적, 물리적, 기술적, 자연적인 장애 기능을 사전에 예방 조치하고, 사후 회복 조치하는 일련의 과정을 말한다[2][3].

1. 정보 보안 모델링의 필요성

첫째, 정상적인 정보의 기능 유지 측면에서 정보는 고유한 사용 목적과 기능을 유지해야 하고 필요한 장소, 사람, 시점에 정확히 전달되어야 한다. 그러나, 정보 자체가 무결성이나 비밀성 등이 보장되지 못하면 무용지물이 될 소지가 많으므로 정상적인 정보의 기능 유지를 위하여 필요하다. 둘째, 자산의 보호 측면에서 정보는 정보와 관련된 모든 자산, H/W, S/W, 데이터 등의 손실과 왜곡으로 막대한 재정적인 손실을 가져올 수 있으므로 정상적인 통신망 운영과 재산권 보호를 위하여 필요하다. 셋째로, 통신망의 확대와 컴퓨터의 보급으로 정보의 집중화를 가져왔고, 정보 수집과 이용이 활성화, 다양화 되어감에 따라, 개인의 프라이버시 보호를 위해서 필요하다. 넷째, 기업이나 조직의 안전에 관한 측면에서 정보 통신망을 이용한 기업 비밀 정보의 유출, 파괴, 훼손으로 기업 조직의 안전 보장을 위해서 필요하다.

2. 정보 보안 모델링 설계의 기본

정보 보안을 달성하기 위해서는 무엇보다도 DBMS에서 발생할 수 있는 여러 형태의 보안 위협 요소들의 식별이 필요하다. 우발적으로 혹은 특별한 기술을 사용하여 시스템에서 관리하는 정보를 부적절하게 노출시키거나, 변경하는 악의가 있는 행위 모두가 위협 요소가 된다. 따라서 시스템의 보호는 저장된 자원을 우발적 또는 의도적으로 권한이 없는 사용자가 판독, 그리고 갱신하는 것을 방지하는 동시에 정당한 권리를 갖는 사용자가 부당하게 서비스의 거부를 당하지 않도록 함을 의미한다[6].

3. 접근제어 모델링

모델링의 목적은 시스템의 보안 요구를 나타내는 요구 명세를 효과적으로 명시하고 설계할 특정 시스템의 소프트웨어와 독립적인 개념 모델을 만드는데 있다. 보안 모델은 명시된 보안 시스템의 기능적 구조에 관한 성질을 정의하는 표현 수단을 제공함으로 목표하는 시스템의 보안 요구 사항을 간결하고 정확하게 제공하는 것, 뿐만 아니라 궁극적인 시스템 구현의 기본 정책이 된다. 접근제어에서 기본이 되는 정책은 크게 3가지 범주로 나눌 수 있다.

1) 신분 · 기반 정책: 주체나 또는 그들이 속해 있는 그룹들의 신분에 근거하여 객체에 대한 접근을 제한할 뿐 접근되는 객체 정보의 중요성에는 아무런 지식을 가지고 있지 않으므로 단순한 신분 위장에 의해서 접근제어가 파괴될 수 있다.

2) 규칙·기반 정책: 주체가 객체들간의 관계를 정의하고 정보의 흐름이 일어났을 때 정보가 소유한 제한 규칙을 상속하며, 각 주체와 객체에 대해서 규칙·기반 정책이 일정하므로 단순한 신분 위장으로 접근제어를 파괴할 수 없다.

3) 직무·기반 정책: 신분기반 정책과 규칙기반 정책의 특성을 모두 가진 상업용 환경에 적합한 정책으로서, 개별적 신분이 아닌 자신의 직무에 따라 접근할 수 있는 정보가 결정되고, 사용할 수 있는 정보의 한계가 정해진다[10].

공개키 기반구조는 공개키 인증 문제를 해결하기 위한 것이며, 그림 1은 공개키 기반구조 모델링을 LDAP, SFCA, SSL등의 몇 개의 모듈로 구분하여 설계하였다.

LDAP(Lightweight Directory Access Protocol)는 접근하는데 사용되는 프로토콜인데, Directory 라는 것은 트리 구조를 가지고 정보를 저장하는 특별한 종류의 Database라고 할 수 있다. 기본 개념은 하드디스크의 디렉토리 구조와 비슷하다. 다른 점은 root 디렉토리가 "world(지구 전체)"이고, 첫 번째 레벨이 "국가들", 그 이하의 레벨이 회사나, 각종 조직, 장소 등이 된다는 점이다. 그 이하로 계속 내려가다 보면 특정인이나 설비, 문서 등의 항목까지도 내려갈 수 있도록 제공한다.

SFCA(Softforum Certification Authority)는 인증기관의 솔루션으로서 사용자에게 디지털 인증서를 발급하여 사용자 자신의 신원을 보다 강력하게 증명하고, 인증서에 기반한 전자서명을 구현함으로써 데이터 무결성 확인, 거래사실 부인 봉쇄 등을 가능하게 하여 인터넷기반의 전자상거래에 확고한 신뢰성을 제공한다. 특히 신뢰성 있고 안전한 전자상거래 서비스의 근간이 되는 국가 PKI(Public Key Infrastructure)를 만들어 가는 전자서명 공인 인증 체계는 통신서비스에서 통신망 인프라만큼 중요하다고 할 수 있다[2].

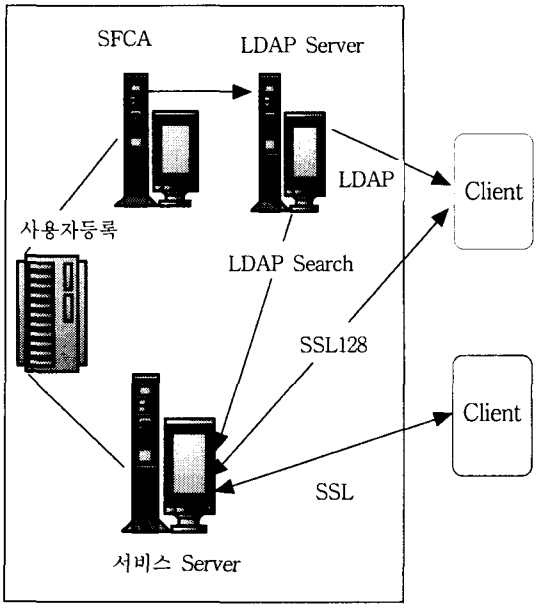

그림 1. 공개키 기반 접근제어
Fig. 1. Access Control of PKI

SSL(Secure Socket Layer)은 네트워크 또는 인터넷상에서 데이터나 메시지 전송의 안전을 관리하기 위해 넷스케이프사에 의해 만들어진 보안 프로그램이다. 넷스케이프의 SSL은 디지털 서명의 사용에도 포함되는 RSA의 공개/개인키 암호화 시스템을 사용한다. SSL은 TCP/IP 위에서 동작하도록 설계되었으며, SSL은 응용계층과 전송계층 사이에서 클라이언트와 서버간의 안전한 채널을 형성해 주는 역할을 수행한다.

3-1. 공개키(PKI)의 기본 모델

인터넷이라는 신뢰할 수 없는 공간을 통해 커뮤니케이션이 이루어지는 한 각각의 서비스 형태나 어플리케이션에 따라 적절한 정보보호 체계를 구축해야 하는 현실에서 필수적으로 요구되는 정보보호기술은 공개키 기반 구조(PKI Public Key Infrastructure)라고 할 수가 있다. PKI는 본래 공개키를 이용해 인증 체계를 구축해 가는 전체 인프라로서 정의되지만 이제는 그 자체가 하나의 독립적인 서비스이며 상품적 개념으로 발전했다[7][10].

1) 인증기관

인증기관은 사용자에게 디지털 인증서를 발급하여 주어 사용자가 인증서에 기반하여 자신의 명칭을 증명할 수 있도록 함으로써 기존의 패스워드에 기반한 인증에 비해 강력한 인증기능을 수행할 수 있도록 한다. 또한 인증서에 기반한 전자 서명을 수행할 수 있다[6].

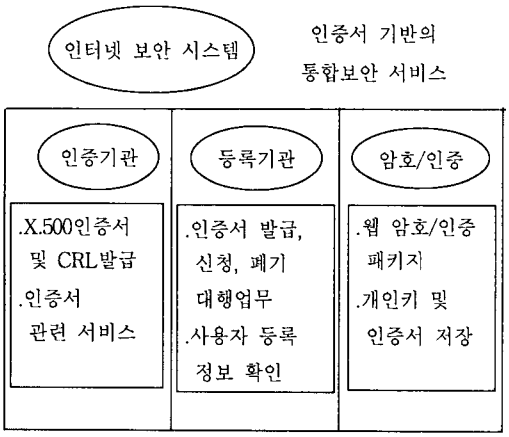

그림 2. 보안 시스템의 구조

Fig. 2. Structure of Security System

2) 등록 기관

사용자로부터 얻은 등록 정보를 확인하고 인증기관에게 인증서 요청을 수행한다. 웹 응용 서비스 보안을 위한 암호 패키지 및 해당 서비스 서버와 사용자 클라이언트간에서 암호화에 기반한 강력한 사용자 인증과 전송되는 데이터 암호화 및 통신 내역 부인 봉쇄를 위한 전자 서명 기능을 구현할 수 있도록 지원한다.

3) 암호/인증

일반 C/S Application을 이용하여 전달되는 데이터의 암호화 및 전자 서명을 지원하고 웹 암호/인증 패키지 · 개인키 및 인증서를 저장한다.

3-2. 암호화 알고리즘

암호 알고리즘은 크게 대칭키 알고리즘과 비대칭키 알고리즘으로 나뉘어 진다. 대칭키 알고리즘이란 암호화에 사용된 Key와 복호화에 사용된 Key가 동일한 알고리즘을 말하며, 비대칭키 알고리즘이란 암호화에 사용된 Key와 복호화에 사용된 Key가 서로 상이한 알고리즘을 말한다[1].

3-2-1. 대칭키 알고리즘

인증자는 인증을 원하는 정보를 비밀키로 암호화 하고 암호문과 평문을 검증자에게 전송한다. 검증 자는 자신의 비밀키로 암호문을 복호화하여 인증자가 제공한 암호문과 일치하는지를 확인하여 인증한다.

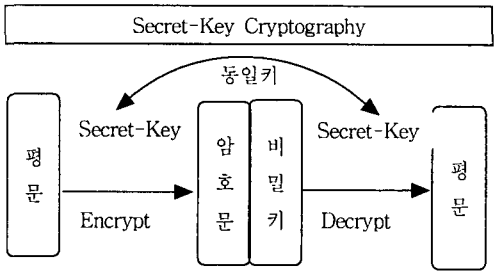

그림 3. 대칭키 인증

Fig. 3. symmetric key authenticity

가령 송신자 S가 전송문 M을 수신자 R에게 하려는 경우 두 사람 사이에 공유되는 비밀키를 K라 하고 암호화 함수를 E, 그리고 복호화 함수를 D라 할 때, 전송문 M이 송신자 S로 부터의 것인가를 확인하는 인증 절차는 다음과 같이 이루어진다.

```
S                    : C = E(M)K
S ----------> R : M,C
R                    : M' = D(C)K
                     : 만약 M = M'이면 인증 성공
                       M ≠ M'이면 인증거부
```

이런 인증절차는 외부 침입자에 의하여 쉽게 침입당할 수 있다. 외부 침입자는 송신자가 수신자에게 전송하는 내용을 도청하여 저장하였다가, 그대로 저장한 내용 M,C를 수신자에게 재 전송함으로써 정당한 송신자 S로부터의 전송문인 것처럼 위장이 가능하기 때문이다. 이러한 단점을 보안하기 위하여 송 · 수신자는 매번 통신 때마다 다른 임의의 정보 T를 이용함으로 가능해진다.

S ---------- R : user name
R ---------- S : 임의의 정보 T
S : X = E(T)K
S -----> R : M,X
: Y = D(X)K
: T = Y 이면 인증 성공
: T ≠ Y 이면 인증 거부

송신자 S는 수신자 R에게 자신의 식별 이름을 전송하고, 이를 수신한 R의 수 T를 생성하여 송신자 S에 전송한다. 송신자 S는 이제 수신자로부터 받은 T를 비밀키 K로 암호화하여 암호문 X를 생성한 후, 전송문 M과 X를 수신자에게 전송한다. 수신자 R은 암호문 X를 역시 비밀키 K로 복호화하여 자신이 생성한 임의의 수 T와 비교하여 일치하면 송신자로부터 받은 전송문 M을 인증한다. 만약 T와 일치하지 않으면 전송문 M이 송신자 S로부터의 것이라는 것을 인증하지 않는다.

3-2-2. 비대칭키 알고리즘

비대칭키 암호화 알고리즘은 공개키 암호화 알고리즘 이라고도 하며, 암호화에 사용된 키와 복호화에 사용되는 키가 서로 다르다는 특징을 가지고 있다. 공개키는 키 소유자가 대외적으로 공개를 해서, 공개키를 획득한 사람이 그 키를 이용하여 메세지를 암호화하고, 공개키의 소유자에게 전송하면, 공개키 소유자는 개인키로 암호화된 메세지를 복호화하여 이용하게 된다. 이러한 절차를 SET Protocol에서는 전자봉투 (Digital Envelope)라 하는데 반해, 개인키로 암호화를 하면, 그 사람의 공개키를 가지고 있는 사람

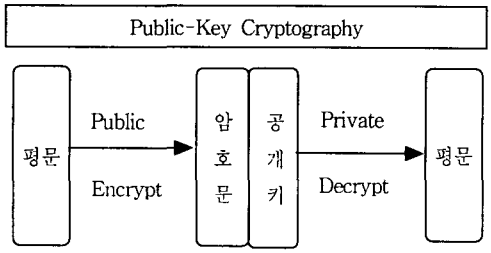

그림 4. 비대칭키 인증
Fig. 4. Asymmetric Key Authenticity

은 누구나 그 암호화된 메세지를 풀어볼 수 있다. 이는 특정한 개인키를 가지고 있는 사람이 유일하기 때문에 개인키 소유자만이 암호화를 할 수 있고, 이는 그 사람이 서명한 것과 동일한 효과를 발휘하기 때문에 전자서명(Digital Signature)이라고 한다.

비 대칭키의 인증절차는 송신 S는 자신의 공개키 KU를 수신자 R에게 공개하고 자신의 개인키 KR는 비밀로 유지한다. 역시 수신자 R도 자신의 공개키 KU을 송신자에게 공개하고 자신의 개인키 KR는 비밀로 유지하며, 역시 암·복호화 함수 E와 D가 존재한다. 이때 송신자S와 수신자 R사이의 인증 절차는 다음과 같다

S -------- R : user name
R -------- S : 임의의 정보 T
S : C = E(M,T)KR
S -------> R : C
: C′ = D(C)KU
: C = T이면 인증 성공
: C≠T이면 인증 거부

송신자 S는 수신자 R에게 자신의 식별 이름을 전송하면 수신자는 임의정보 T를 생성하여 송신자에게 이를 전송한다. 송신자 S는 전송문 M과 수신자R로부터 받은 임의의 정보 T를 자신의 개인키 KR로 암호화하여 암호 C를 생성하여 수신자에게 전송한다. 다음에 수신자는 암호는 C를 송신자 S의 공개키 KU로 복호화 하여 임의의 정보 T가 자신이 생성한 값과 일치하는가를 확인하여 인증한다. 위와 같은 인증 절차에서는 송수신자는 각각 자신의 개인키 및 상대방의 공개키를 모두 유지하는 단점이 있다.

III. 모델링의 통합 시스템 구성도

오늘날 데이터 베이스 시스템은 중앙집중식으로 관리할 수 있어야 하며 모든 면에서 정보보호 정책을 가능하게 하면서 동시에 통합된 정책 관리를 제공하여야 한다. 접근제어는 접근제어, 인증, 권한부여 그리고 위임 관리를 위한 정책을 관리한다. 소프트웨어는 네트워크와 컴퓨터시스템을 위해 웹과 네

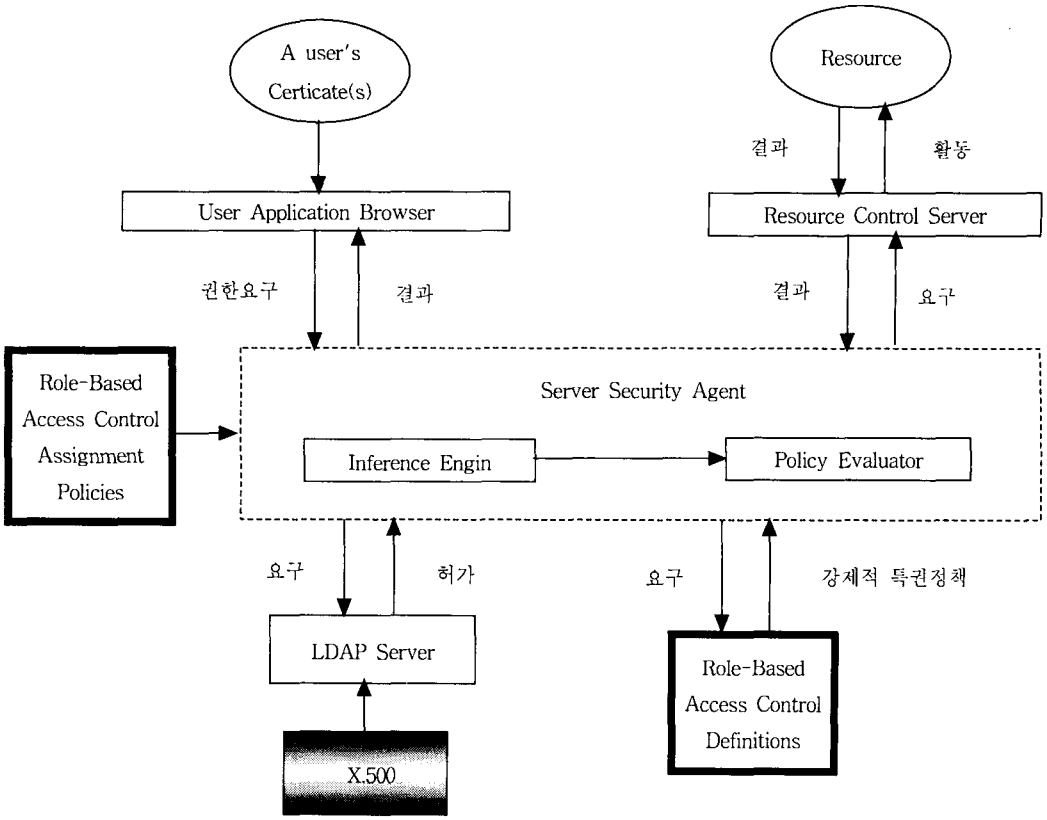

그림 5. 시스템 정책 구성
Fig. 5. Structure of System Policy

트워크 기반의 응용프로그램을 위한 공통된 관리 플랫폼을 제공한다. 접근제어는 인트라넷, 익스트라넷, 그리고 전자 상거래 환경에서 대용량적 설치에 적합하면서 관리가 쉽고 이상적인 보안 정책을 제공해야 한다.

그러므로 본 논문에서는 최종 사용자가 클라이언트 응용 프로그램으로 분석 서버에 연결된 상태에서 큐브 데이터 또는 데이터 마이닝 모델에 대한 최종 사용자 액세스를 제어하기 위해 사용되는 Role기능을 기본 시스템 구조에 응용하고, RBAC(Role- Based Access Control)을 포함, 확장하여 그림 5와 같이 통합 접근제어 모델링을 제시한다.

1. RBAC의 역할

Role은 유사한 작업을 수행하는 다수의 사용자를 하나의 그룹으로 묶어, 통합적인 접근제어를 수행하는 것으로 정의한다[7]. Role의 기능에는 여러 역할과 사용자를 묶어 새로운 역할을 지정하는 방법과, Role을 중첩하여 사용하는 방법 및 중첩 사용시 Primary Role을 지정하는 방법이 있는데, 본 논문에서는 Role을 데이터베이스, 큐브, 마이닝으로 구분하여 액세스 유형과 범위를 지정하고, 그림 6과 같이 Role의 새로운 모델링을 제안하였다.

㉮ 데이터베이스 역할

데이터베이스 역할은 Analysis Service 데이터베이스 수준에서 정의되어 데이터베이스의 여러 큐브에 할당될 수 있으므로, 역할의 사용자에게 이러한 큐브에 대한 액세스가 허용된다. 그러한 할당을 통해 데이터베이스 역할과 똑같은 이름의 큐브 역할이 만들어지고, 데이터베이스 역할은 같은 이름의 큐브 역할에 대

한 기본 값을 제공한다.

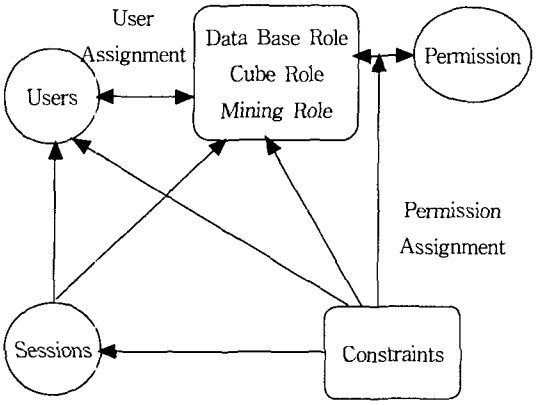

그림 6. RBAC 모델링
Fig. 6. Modeling of RBAC

㉯ 큐브 역할

큐브 역할은 데이터베이스 역할이 큐브에 할당될 때 큐브 수준에서 만들어지므로, 해당 큐브에만 적용된다. 큐브 역할의 기본 값은 같은 이름의 데이터베이스 역할에서 파생된 것이지만, 이 기본 값 중 일부는 큐브 역할에서 무시될 수 있다.

㉰ 마이닝 모델 역할

큐브 역할과 마찬가지로, 마이닝 모델 역할은 데이터베이스 역할이 마이닝 모델에 할당될 때 마이닝 모델 수준에서 만들어진다. 마이닝 모델 역할의 기본 값은 같은 이름의 데이터베이스 역할에서 파생되지만, 역할 구성원은 마이닝 모델 역할에서 무시될 수 있다.

㉱ 보안 및 인증

분석 서비스에서 관리하는 데이터에 대한 액세스를 제한하는 단계인데 분석 관리자를 통해 Analysis Service를 액세스하고 관리 기능을 수행하도록 허용되는 관리자를 제한하는 과정이고, 또한 클라이언트 응용 프로그램을 통해 분석 서버의 데이터를 액세스하는 최종 사용자를 제한할 수도 있으며, 데이터를 액세스할 수 있는 최종 사용자와 수행할 수 있는 작업의 종류를 지정할 수 있다. 뿐만 아니라, 큐브, 차원, 큐브 셀을 비롯하여 Analysis Service 데이터의 다양한 수준에서 최종 사용자 액세스를 제어 할 수 있다.

2. Role을 사용한 접근

Role은 하나의 문장으로 싱글유저에게 권한의 집합을 부여하고, 싱글유저에게 사용중인 권한의 집합을 활성화 또는 비활성화 하여 지원할 수 있도록 하며 이러한 경우 Role Password는 그 유저가 DB에 접속 되어 있는 동안 그 롤이 접속되어 있다면 즉시 Role이 활성화되기 위해 필요로 하는데 사용되어 진다.

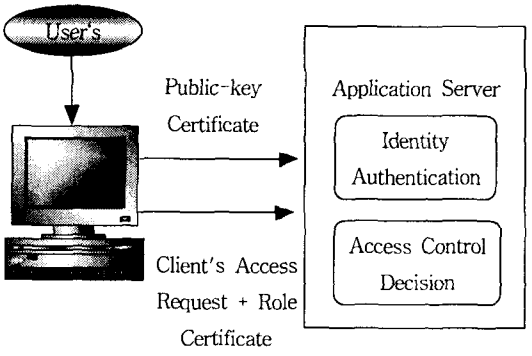

그림 7. Role 사용 접근제어
Fig. 7. Access Control of Role Use

하나의 유저에게 각각의 권한을 부여하는 것보다는 여러 개의 권한을 하나의 롤에 포함 시켜 그 롤을 정의하고 권한을 부여하는 것이 보다 더 편리하게 사용할 수 있을 것이다. 권한은 public에게 부여하여 데이터베이스 모든 유저에게 부여 할 수 있고 하나의 유저에게도 하나의 롤을 부여 할 수 있다. 이러한 메커니즘은 누군가가 몇 개의 Role로 접근할 때 예기치 않는 권한을 포함한 가상적인 Role로 부터 위험을 피할 수 있고, 유저소유의 보안을 실행할 수 있는 클라이언트 프로그램을 가지고 실행하는데 매우 유리할 것이다.

최종 사용자 보안은 그림 7과 같이 제어된다. 분석 서버에 연결된 동안 인증은 분석 관리자에 정의된 데이터베이스, 큐브, 마이닝 모델 역할의 기능은 각 역할에 사용자 집합과 이 사용자 집합이 모두 공유하는 액세스 권한을 정의하며, 역할은 분석 서비스 데이터베이스 수준에서 정의된 다음, 역할의 사용자에게 액세스가 허용된 큐브에 할당된다. 역할을 할당한 후에는 큐브 수준에서 역할에 대한 약간의 변경이 허용 가능하며, 이러한 변경은 데이터베이스 수준에서 역할에

영향을 주지 않는다. 따라서, 역할에는 역할이 할당되는 각 큐브에 대해 서로 다른 정의를 가질 수 있다.

3. Role의 통합 보안

전자서명 기술은 공개키 암호 시스템으로 비밀키와 공개키가 사용된다. 공개키는 공개된 정보이므로 어떻게 공개키의 위/변조 문제를 해결하는가 하는 공개키 인증 문제로 제기된다. 이러한 공개키 인증문제를 해결하기 위해 나온 것이 공개키 기반구조이다. 따라서 X.500을 기반으로한 PKI의 표준화가 IETF를 중심으로 이루어지고 있는데, 본 논문에서는 PKI의 기본 모델링을 이용하여 새로운 모델링을 제시했다. 그림 8은 PKI의 기본 시스템 모델링에 RBAC를 통합한 모델링이다. RBAC는 전통적인 명령 접근제어와 분산 접근제어 정책들의 하나인데 비해 본 시스템에서 제안된 Role을 적용하게 되면 어떤 사용자에 대해서 데이터베이스가 아닌 서버의 시스템적인 권한을 부여하는 방법으로 이루어진다. 그러므로 Role을 사용함으로써 서버에서는 사용자가 Public그룹 외에 한 그룹에만 속할 수 있었던 것을 한 사용자가 속할 수 있는 역할의 수는 제한이 없어졌다.

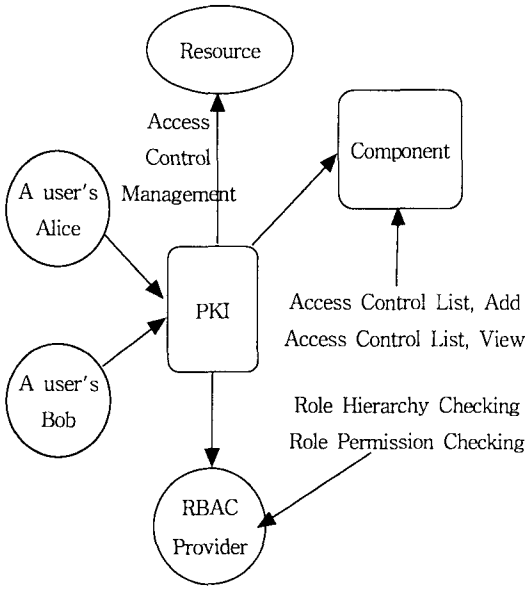

그림 8. RBAC의 혼합

Fig. 8. Mixing of RBAC

확장성에는 기존의 접근제어 운영체제에 Role을 적용함으로 상세한 접근권한을 설정 할 수 있게 되었고, 설계 기능을 통한 기능확장이 용이해지며, Role에 의한 접근제어 기능을 통한 손쉬운 통합 관리가 가능해졌다. 각 자원에 접근하고자 하는 접근자는 보안 관리자에 의해 지정된 Role에 의해서만 접근이 가능해지므로 내부정보 유출을 차단할 수 있고 시스템을 보다 안전하게 공유하여 사용할 수 있기 때문에 서버의 가용성을 증대시킬 수 있었다.

IV. 결 론

현대 사회는 정보통신 분야의 발전과 더불어 다양한 정보에 대한 관련 서비스 요구가 증대되고 있다. 그러나 서비스는 기본적으로 다자간 통신을 요구함으로써 안정성, 효율성 및 정보보안 부분에서 취약성을 드러내고 있다.

본 논문에서는 공개키의 기본 시스템 구조를 응용하고, RBAC를 포함, 확장하여 Role을 데이터베이스, 큐브, 마이닝으로 구분하여 엑세스 유형과 범위를 지정하고 Role의 새로운 모델링을 제시하여, 기존의 접근제어 운영체제에 Role을 적용함으로 상세한 접근권한을 설정 할 수 있게 되었다.

향후 연구 과제로 원격 사이트내의 정보 접근시 접근자의 신분을 판별 할 수 있는 종합시스템을 개발하여 해커나 정보 누출 및 외부의 공격으로부터 벗어 날 수 있어야 할 것이다. 그러기 위해서는 정보 보호 시스템과 접근 모델링의 메커니즘 및 암호 분류에 대한 판독 알고리즘에 대한 연구가 필요할 것으로 사료된다.

참 고 문 헌

[1] Jing-Jang, Kou-Chen and Duen-Ren, "Access control with role attribute certificates", *Computer Standards & Interfaces*, Vol. 22, pp.47-48, 2000.

[2] Edward C. Cheng, "An object-oriented organizational model to support dynamic role-based access control in electronic commerce", *Decision Support Systems*, Vol. 29, Issue 4, pp.362-363, 2000.

[3] Reinhardt A. Botha and Jan H. P. Eloff, "Access Control in Document-centric Workflow Systems An Agent-based Approach", *Computers & Security*, Vol. 20, Issue 6, pp.529-530, 2001.

[4] L. Labuschagne and J. H. P. Eloff, "Improved system-access control using complementary technologies", *Computers & Security*, Vol. 16, Issue 6, pp.545-547, 1997.

[5] Rayford B. Vaughn, Ronda Henning and Kevin Fox, "An empirical study of industrial security-engineering practices", *Journal of Systems and Software*, Vol. 61, Issue 3, pp.227, 2001.

[6] Sharman Lichtenstein, "Information Security Design Principles for Adaptive Organizations", *Computer Audit Update*, Issue 6, pp.8-9, 1996.

[7] 정원혁, 『Microsoft SQL Server』, 대림출판사, pp.480-492, 2001

[8] Chu-Hsing Lin, "Dynamic key management schemes for access control in a hierarchy", *Computer Communications*, Vol. 20, Issue 15, pp.338, 2000.

[9] Ahmed Patel, "Access control mechanisms in digital library services", *Computer Standards & Interfaces*, Vol. 23, Issue 1, pp.21-22, 2001.

[10] Marie A. Wright, "An Overview of PKI", *Computers & Security*, Vol. 15, Issue 4, pp.515-516, 1999.

자 기 소 개

방극인(Keug-In Bang)

1992년 광주대학교 전자계산학과 (공학사)

1994년 조선대학교 대학원 컴퓨터공학과(공학석사)

2002년 조선대학교 대학원 컴퓨터공학과 박사과정 수료

1996년~현재 나주대학 컴퓨터정보기술과 조교수

※주관심분야 : 객체지향 프로그래밍, 분산운영체제, 프로그래밍 환경, 정보보호

이 준(Joon Lee)

1979년 조선대학교 전자공학과 (공학사)

1981년 조선대학교 대학원 전자공학과(공학석사)

1997 숭실대학교 대학원 전자계산학과(공학박사)

1982년~현재 조선대학교 전자정보공과대학 컴퓨터공학부 교수

※주관심분야 : 분산 운영체제, 정보보호, 병렬처리, 프로그래밍환경.