情報保護學會論文誌
第15卷 第6號, 2005. 12

역할 계층과 암호학적인 키 할당 기법을 이용한 XML 객체의 접근제어*

반 용 호,†‡ 배 경 만, 김 종 훈
동아대학교

Access Control of XML Object Using Role Hierarchy and Cryptographic Key Assignment Scheme*

Yong-Ho Ban,†‡ Kyoung-Man Bae, Jong-Hoon Kim
Dong-A University

요 약

XML에 대한 사용의 증가와 함께, XML 객체에 대한 보안의 필요성이 계속해서 증가하고 있다. 특히, 다양한 사용자가 서로 결합되어 있는 환경에서 공유되는 XML 객체에 대한 접근제어 문제의 해결은 매우 중요하다. 본 논문에서는 XML 객체에 대한 접근제어를 위하여 RBAC의 역할 계층과 계층적 키 유도/할당 기법을 결합한 접근제어 모델을 제안한다. RBAC는 자체적으로 주체에 대한 키 할당 기법은 지원하지 않으므로 계층적 키 분배 기법을 도입하여 접근제어 메커니즘이 실현되도록 하였다. 본 논문에서 제안된 방식은 XML 객체를 위한 접근제어에서 RBAC이 제공하는 관리상의 이점뿐만 아니라, 상위 계층의 사용자가 하위 계층의 키를 유도하여 사용할 수 있게 지원하므로 각 역할 계층에서 관리하는 키의 수가 기존 방식에 비하여 줄어드는 특징을 제공한다.

ABSTRACT

As the usage of XML documents increases the requirement of security for XML documents is growing. Especially it is very important to solve the problem of access control to XML object which shares in the environment where various users connect to each others. In this paper, we propose the access control model and mechanism which is combined with role hierarchy in the RBAC and hierarchical key derivation/assign method for the access to XML object. So we implement the access control mechanism by including hierarchical key derivation method. The technique, we proposed, gives not only the benefit in management which RBAC provides in access control to XML objects, but also it can help derive a lower layer key from the higher layer user's. This feature decrease the number of keys managed in each role hierarchy in comparison with previous methods.

Keywords : *access control, RBAC, XML security, hierarchical key derivation*

Ⅰ. 서 론

W3C의 지원 아래 구성된 XML 작업 그룹에 의하여 1996년 제안된 XML은 HTML을 대신하는 차세대 웹 문서의 표준으로 자리 잡았다[13]. XML

접수일 : 2005년 9월 15일 ; 채택일 : 2005년 11월 29일
* 본 연구는 2003학년도 동아대학교 학술연구비(공모과제) 지원에 의해 수행하였습니다.
† 주저자, ‡ 교신저자 : idpass@paran.com

은 단순한 프로그래밍 언어로 인식되기 보다는 분산 컴퓨터 환경에서 네트워크 통신 프로토콜, 클라이언트-서버 시스템, 데이터베이스 시스템 등에서 응용 프로그램 간 정보교환을 제공하는 기반기술로 인식이 확대되고 있으며, 현재 관심을 모으고 있는 웹 서비스, 전자상거래, 기업응용시스템통합(EAI) 그리고 유비쿼터스 컴퓨팅 분야에서 기반 기술의 하나로 XML을 채택하게 될 것이다. 그러나 이러한 환경에서 XML을 일정한 보안상의 제약 없이 사용할 경우, 사용자의 권한에 상관없이 해당 XML 객체에 접근할 수 있는 상황이 발생할 수 있으므로 XML 객체에 대한 기밀성이나 무결성이 훼손되는 상황이 발생할 수 있다. 따라서 XML에 대한 접근제어 방법, 특히 다양한 사용자가 서로 결합되어 있는 환경에서 공유되는 XML 객체에 대한 접근제어 문제의 해결은 매우 중요하다. XML에 관련된 보안 기법에 대한 연구 중 대표적인 것은 W3C를 중심으로 수행된 XML전자서명, XML암호화 등을 예로 들 수 있다.[14,15] 그러나, XML 전자서명과 암호화는 단순한 통신상의 기밀성과 무결성을 제공할 뿐 관리적 요소인 다양한 사용자와 다양한 접근권한 정책을 반영하지 못하고 있다. XML 객체를 이용하는 환경에서의 접근제어를 위한 연구가 OASIS XACML 표준에서 제시되었다.[16] 본 논문에서는 XML 객체에 대한 접근제어를 위하여 RBAC의 역할 계층과 계층적 키 유도/할당 기법을 결합한 접근제어 모델과 메커니즘을 제안한다. RBAC 모델은 계층적 접근제어와 접근 권한 관리를 쉽게 사용할 수 있도록 해주며, 이러한 특징은 XML 문서의 특징과 잘 부합한다. 그러나 RBAC는 자체적으로 주체에 대한 키 할당 기법은 지원하지 않으므로 계층적 키 분배 기법을 도입하여 접근제어 메커니즘이 실현되도록 하였다. 본 논문에서 제안된 방식은 XML 객체를 위한 접근제어에서 RBAC가 제공하는 관리상의 이점뿐만 아니라, 상위 계층의 사용자가 하위 계층의 키를 유도하여 사용할 수 있게 지원하므로 각 역할 계층에서 관리하는 키의 수가 기존 방식에 비하여 줄어드는 특징을 제공한다. 또한 보안 계층이 추가 되거나 삭제되는 경우에 해당 보안 계층 간의 관계만을 갱신하므로 전체 암호화에 사용된 전체키를 갱신할 필요가 없다. 본 논문은 다음과 같이 전개된다. 논문의 2장에서 접근제어와 관련된 이전의 연구들에 대하여 살펴본다. 3장에서는 역할 계층과 계층적 키 할당 방법을 기반으로 하는 새로운 방식의 XML 객체에 대한 접근제어 모델을 제안하고, 제안된 모델이 가지고 있는 주요 특징들을 기술한다. 4장에서는 제안된 접근제어 모델을 기반으로 XML 문서를 권한에 따라 관리하는 접근제어 메커니즘에 대하여 설명하고, 제안된 메커니즘이 실제 환경에서 어떻게 적용될 수 있을지를 기술한다. 5장에서는 본 논문에서 제안된 모델의 보안성과 본 논문에서 제안된 방식을 기존의 연구들과 비교를 통하여 제안된 방식이 가지는 특징과 차이점에 대하여 설명하고, 6장에서는 결론과 향후에 진행되어야 할 연구 과제를 제시한다.

II. 관련 연구

본 장에서는 접근제어를 위한 기존의 모델과 구성요소에 대한 이전의 연구들을 살펴본다.

2.1 역할기반 접근제어(RBAC)

역할기반 접근제어(RBAC)는 역할을 기반으로 접근제어 정책을 표현하는 접근제어 모델이다. RBAC의 핵심 개념은 사용자가 기업이나 조직의 정보 자원을 임의로 접근할 수 없도록 하는 대신에, 접근권한이 역할(role)에 부여되고 사용자는 적절한 역할에 소속되어 역할의 수행에 필요한 최소 자원만을 접근할 수 있도록 하는 것이다. 이러한 개념은 권한 관리를 매우 단순화 시켜주고 기업의 특정한 보안정책 구현에서 유연성을 제공하는 장점을 가진다. 그림 1에서 RBAC 기본 모델을 보여준다. 기본 모델은 사용자(U), 역할(R), 인가권한(P), 세션(S)으로 구성된다.[1] 기본적인 RBAC 모델에 역할계층구조, 제약조건이라는 특성이 추가될 수 있는데 역할계층(Role Hierarchy)은 권한과 책임에 대한 조직 내의 순서를 나타낼 수 있는 가장 일반적인 방법으로 트리구조로 나타내며 상위역할의 권한은 하위역할에 상속될 수 있다. 제약조건은 접근제어 정책이 실제 시스템 환경에 적용 가능하도록 하는 사전 규약들로 사용자 할당, 권한 할당, 그리고 접근제어 세션에 적용된다.

2.2 키 유도 기법에 의한 계층적 접근제어

컴퓨터 통신시스템에서의 키 관리 문제는 사용자 계층으로부터 만들어진다. 이러한 계층에서 사용자와

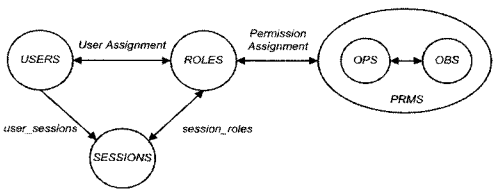


그림 1. RBAC 모델의 기본 구조

사용자가 가진 정보들은 분리된 몇 개의 집합으로 나누어지고, 각 사용자는 사용자 보안 등급(Security Clearance) 이라 부르는 보안 계층에 할당된다. 예를 들어, $SC_1, SC_2, ... SC_n$ 을 서로 독립된 보안 계층이라 두고 기호 $\leq$를 집합 $SC=\{SC_1, SC_2, ... SC_n\}$ 상의 순서 관계라고 가정할 때, 순서 집합 $SC_j \leq SC_i$는 보안 계층 SC_i의 사용자가 보안 계층 SC_j의 사용자에 비해 보안 등급이 높거나 동등하다는 것을 의미한다. 이 경우 보안 계층 SC_i의 사용자는 보안 계층 SC_j의 사용자가 소유하고 있는 정보를 읽거나 저장할 수 있지만, SC_j는 SC_i가 소유한 정보를 읽거나 저장할 수 없다. 이러한 접근 방법에서 핵심 문제는 특정 보안 계층의 사용자가 낮은 보안 계층의 사용자에 대하여 키를 유도하는 방법이다. 계층에서의 키 관리 문제를 위하여 Alk 등은(이하, AT) 대칭키 암호화방식의 키 할당 기법을 제안했다.[2] 이 기법의 특징은 사용자 u가 보안 계층 m에 할당되었다면, 사용자 u는 보안 계층 $m' \leq m$이 되는 모든 계층을 복호화 할 수 있도록 해준다. AT 방식은 다음과 같이 요약된다. 먼저, 각 보안 계층 SC_i는 공개된 정수 t_i를 선택한다. SC_i의 비밀키 SK_i는 $SK_i = SK_0^{t_i} (\mathrm{mod} m)$에 따라 계산된다. 여기서, SK_0는 CA의 비밀키 이고, m은 두 소수 p, q의 곱이다. 만약, $SC_j \leq SC_i$가 유지된다면, t_j / t_i는 정수이고, 추론에 의하여 SC_i는 SK_j를 유도할 수 있다.

$SK_j = SK_0^{t_j} = SK_0^{t_i * (t_j / t_i)} = SK_i^{(t_j / t_i)} (\mathrm{mod} m)$. 이에 반하여 $\neg(SC_j \leq SC_i)$인 경우, t_j / t_i의 결과는 정수가 될 수 없으므로 키 유도는 불가능하다. 이후의 연구들에서 계층적 구조에서의 키 관리 문제는 정규 할당 방법을 이용하여 t_i의 값을 줄이기 위한 개선된 방법, bottom-up 키 생성 체계를 이용하는 또 다른 방법들과 함께 동적으로 보안 계층을 추가하거나 삭제하고, 공개된 정보의 크기를 줄이기 위한 해결책들이 제안되었다.[3-5] 결론적으로, 계층적 키 관리 기법은 자신이 소유한 정보로부터 하위 계층의 키 유도를 허용하고, 상위 계층의 키를 유도하기 위해 하위 계층 사용자들에 의한 다양한 협업 공격의 가능성을 피할 수 있는 특징을 제공한다.

2.3 XML 객체의 접근제어

지난 몇 년 동안 XML을 기반으로 하는 응용 애플리케이션의 증가와 함께 XML 객체에 대한 접근제어 방법론 및 접근제어 기법들에 대한 다양한 연구가 진행되었다.[6-8] Damiani 등은 사용자의 접근 요청에 대해 해당 XML 객체를 이용하여 DOM 트리를 생성한 후에 XML 접근제어 목록을 검색하여 사용자의 접근 권한이 없는 노드들을 DOM 트리에서 삭제한 뒤 제공하는 접근제어 방식을 제안했다. 즉, DOM 트리를 이용하여 XML 객체와 DTD의 엘리먼트에 접근권한을 설정하고, 설정된 접근권한 정보에 의해 사용자의 XML 객체의 접근을 제어는 방식이다.[6] 그러나 접근 요청에 대하여 각각 DOM 트리를 생성하므로 다수의 사용자가 동시에 동일한 객체에 접근을 시도할 때, 사용자가 요구하는 객체에 대해 매번 DOM 트리를 생성해야 하는 단점이 존재한다. Christian 등은 XML 객체의 암호화에 접근제어 개념을 도입하여 다른 권한을 가진 다양한 사용자를 위한 암호화 기법을 제안하였다.[7] 이러한 방법은 XML 객체의 각 노드 중에서 기밀정보를 가진 노드를 서로 다른 키로 암호화하여 암호화 풀에 저장하고, 접근 요구가 발생하면 기밀 노드 중에서 사용자에게 권한이 있는 노드만 선별하여 키와 함께 전달하는 기법이다. 그러나 이러한 기법은 접근을 요청한 사용자에게 권한이 존재 하는 노드들만을 전달하기 위해 각 노드마다 권한이 존재하는 사용자들의 집합을 유지해야 한다는 단점을 가진다.

XML 객체에 대한 접근제어에서 RBAC 모델을 반영한 연구들도 수행되었다.[9-12] Hao 등이 제안한 논문은 레퍼지토리에 저장된 XML 객체에 대하여 RBAC 모델을 적용하여 접근제어를 수행하는 초기의 모델이다.[5] 그러나 이 모델은 인스턴스 객체 내부의 엘리먼트에 대한 접근을 위한 연산만을 제공하고 있으며, 역할을 부여 받는 사용자에 대한 정의와 역할 정보, 역할 계층 등이 하나의 설정 파일에 모두 포함되어 사용자에 대한 변경이나 역할 정보에 대한 변경이 발생 시 설정 파일을 일일이 재구성하여야 한다는 단점을 가지고 있다. Jingzhu 등은 XML Database에 대한 접근제어를 위하여 역할

그래프 모델과 객체지향 DB의 설계 기법을 이용하여 접근제어를 수행하는 기법을 제시하였다.[10] 그러나 해당 논문에서는 역할 계층이나 키를 이용한 계층적 구조에서의 접근제어를 제시하지 못하고 있다. Jason Crampton은 역할 계층과 키 계층을 이용한 접근제어 기법을 제시하고 있다.[11] 기본적인 개념은 본 논문에서 제안한 방식과 유사하나 역할 계층과 키 계층에 대한 동적인 관리 방법을 제시하지 않는다는 단점을 가지고 있다.

Ⅲ. 제안된 모델의 구성 요소

본 장에서는 계층적 키 할당 기법을 이용한 XML 문서의 접근제어 모델에서 사용되는 주체와 객체 그리고 이들 사이에서 수행되는 연산에 대하여 설명한다.

3.1 객체(Object)

접근제어 정책에서 접근제어의 대상이 되는 자원들의 집합을 객체라고 정의한다. 본 논문에서는 접근제어 객체를 특정 Schema나 DTD를 따르는 XML 문서의 엘리먼트와 속성으로 정의한다. 엘리먼트와 속성은 XPath나 XPath Filter에 의해 구분된다. 만약 사용자가 그림 2에 있는 환자의 정보 중에서 환자의 담당의사 정보를 알고 싶다고 요청을

```
<? XML Version="1.0" encoding="euc-kr" ?>
<PRs>
 <PaNa="Alice">
 <Personal>
 <RRN> 801225-1234567 </RRN>
 <YMD>
 <Year>1980</Year>
 <Month>12</Month>
 <Date>25</Date>
 </YMD>
 </Personal>
 <Medical>
 <Doctor>KimCH</Doctor>
 <Nurse> MoonJS</Nurse>
 <Diagnosis> Insulin </Diagnosis>
 <Prescription> Chemo medicine </Prescription>
 <Bill> 500,000 </Bill>
 </Medical>
 </Patient>
 <PaNa="Bob">
 .......
 </Patient>
 </PRs>
```

그림 2. 객체 정보를 포함하는 XML 문서의 예

한다면 Medical/Doctor가 객체에 해당된다. 각각의 객체는 보안 등급(Security Clearance)을 부여받게 되는데, 보안 등급은 객체에 대한 접근제어의 수준을 나타내며, 해당 객체를 제공한 제공자나, 객체를 관리하는 보안 정책 및 이를 관리하는 보안 관리자에 의해 결정된다. 보안등급의 결정은 다음과 같은 과정을 통해 이루어진다. 먼저 XML 객체 작성을 위한 Schema 작성 시 사용된 엘리먼트와 속성에 정의된 모든 요소에 대한 보안 등급 참조 사전(Security Clearance Reference Dictionary)을 작성한다. SCRD를 기반으로 XML 객체의 작성에 사용된 엘리먼트 및 속성에 대한 보안 등급 정보를 가진 파일을 작성한다. 만약, Schema를 따르지 않는 객체인 경우 실제 XML 객체의 각 엘리먼트로부터 직접 보안 등급 정보를 추출할 수 있다. 객체에 대한 접근제어 요구 수준은 각 애플리케이션에 따라 각각 다를 수 있고, 엘리먼트나 속성에 대한 접근제어 요구 수준 역시 해당 정책에 따라 달라진다. 예를 들어, 환자의 정보에 대한 보안 수준이 높은 보안등급 수준으로 할 수도 있고 보안 수준이 상대적으로 낮은 수준으로 설정될 수도 있다는 의미이다. 즉, 보안 등급은 항상 같은 것이 아니라 문서가 이용되는 상황에 따라 다르게 설정되어 질 수 있다.

3.2 주체 (Subject)

접근제어 정책은 사용자가 유효한 어떤 정보를 소유하고 있다는 개념을 기반으로 정의된다. 사용자가 소유한 정보는 보안 목표를 위해 요구되는 주체의 속성들로 구성된다. 각각의 사용자는 하나 혹은 그 이상의 유효한 정보와 연결된다. 이 유효 정보는 사용자가 시스템에 등록되거나 동의하였을 때 할당된다. 본 논문에서는 사용자가 가진 유효정보를 다음과 같이 정의한다. S = (user_id, password, [purpose]) or (certificate, certificate_password, [purpose]). 주체는 시스템에 의해 미리 배포된 사용자 ID와 패스워드, 그리고 접근 목적으로 이루어진다. 여기서 '[]'는 생략될 수 있음을 나타낸다. 각각의 주체는 보안 계층(Security Class)이라고 하는 속성을 부여받게 되는데, 보안 계층은 2절에서 언급된 RBAC의 역할 계층과 동일한 의미를 가진다. 즉 각각의 사용자는 각 역할 계층에 할당되고, 역할 계층은 접근 가능한 객체를 배정 받는다. 보안 계층들은 순서집합 $S=\{u_1, u_2 \cdots u_n\}$으로 나타낼 수 있으며 각 계층은

```
<Staff>
 <Employee Name="KimCH">
 <Personal> <RRN> 760407-2345678 </RRN>
 </Personal>
 <StaffInfo>
         <Position> Doctor </Position>
         <AccountableTo/>
 </StaffInfo>
 </Employee>
 <Employee Name="MoonJS">
 <Personal> <RRN> 800722-1901234 </RRN>
 </Personal>
 <StaffInfo>
         <Position> Nurse </Position>
         <AccountableTo>
                 <Doctor>KimJH</Doctor>
         </AccountableTo>
 </StaffInfo>
 </Employee>
 <Employee Name="HanHD">
 <Personal> <RRN> 780509-1432567 </RRN>
 </Personal>
 <StaffInfo>
         <Position> Staff </Position>
         <AccountableTo/>
 </StaffInfo>
 </Employee>
</Staff>
```

그림 3. 주체 정보를 표현한 XML 문서

기호 '≤'를 이용해서 서로의 관계를 나타낼 수 있다. 만약 $u_1 \leq u_2$인 경우, u_2는 u_1의 상위 계층 또는 같은 계층이며, u_2는 u_1이 가지는 정보에 접근할 수 있지만 반대의 경우는 허용되지 않는다.

예를 들어, 그림 3에서와 같이 사용자 KimCH, MoonJS, Alice는 각각의 역할에 할당될 수 있다. KimCH, MoonJS는 각각 의사와 간호사의 역할을 가지고 있고, Alice는 환자의 역할을 자동으로 할당받는다. 각각의 역할 계층은 XPath형식으로 나타낼 수 있다. 표 1에서 각 사용자에 대하여 부여된 역할과 사용자의 표현, 역할 계층을 표현한 XPath 표현식을 볼 수 있다. KimCH, MoonJS는 그림 3에 나타나 있는 position과 같은 역할을 할당 받았고 Alice는 그림 2에 나타나 있는 Patient[@Name]에서 환자라는 역할을 할당받았음을 알 수 있다.

표 1. 사용자에 대한 역할 계층 할당

사용자	역할	역할 계층 표현
u_1	D	//StaffInfo/Position="Doctor"
u_2	N	//StaffInfo/Position="Nurse"
u_3	S	//StaffInfo/Position="Staff"
u_4	P	//Patient[@Name]

3.3 연산 (Operation)

접근제어 모델에서 연산은 권한부여 과정을 통하여 접근 가능한 객체에 대하여 수행가능 한 동작(action)들의 집합으로 정의할 수 있다. 즉 수행 가능한 동작을 a라 하고, 대상 객체 집합을 O, 연산을 P라고 할 때, $P=(O,A)$로 나타 낼 수 있다. 접근제어 모델에서의 연산 유형은 사용되는 모델의 형태에 따라 다양하게 정의될 수 있지만, 일반적으로 R(*Read*), W(*Write*), U(*Update*), D(*Delete*)의 유형을 허용할 수 있다. 그러나 본 논문에서는 읽기 연산인 R(*Read*)에만 그 초점을 두고 논의를 진행한다. 즉, 본 논문에서 연산 $P=(O,R)$로 고정하여 논의한다.

Ⅳ. 역할 계층과 계층적 키 할당 기법을 이용한 XML 객체의 접근제어

4.1 접근제어 시스템의 구조

그림 4는 XML 문서의 접근제어를 위한 접근제어 모델의 구조를 보여준다. 제안된 모델은 사용자 인증 부분과 역할관리 부분, 보안 계층 관리 부분, 정책관리 서버, CA, XML 질의 처리기, XML 객체 저장 DB 등으로 구성된다. 역할 관리 모듈은 각 사용자에 대한 역할의 생성 및 삭제, 새로운 역할의 추가, 각 역할간의 계층 관계 등을 정의하고 관리하는 일을 담당한다. 또한 미리 정의된 보안 정책에 따라 XML 객체에 대한 암호화를 위하여 역할 계층과 키 계층을 서로 연결하고, 이에 관련된 정보를 관리한다. 보안 계층 관리 모듈은 XML 객체 DB에 저장된 전체 객체들에 대한 보안 등급 생성 및 삭제, 수정하는 일을 담당한다. 정책관리 서버는 기본 보안 정책을 정의하고, 이를 모듈 전체에 적용하는 역할을 담당한다. CA는 문서의 암호화에 사용되는 키를 생성하고 분배하는 역할과 계층 관계 목록을 생성하는 기능을 가진다. 계층 관계 목록은 계층의 모든 사용자에게 공개된다. 그러나 오직 CA만이 관계 목록의 내용을 수정할 수 있는 권한을 가진다. 암호화 모듈은 주어진 XML 객체에 대하여 접근 가능한 영역에 대한 암호화(XML 객체 DB 측) 및 복호화(사용자 측)를 수행한다.

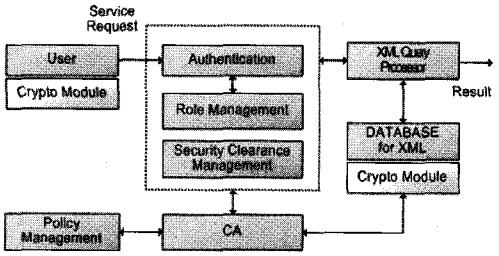


그림 4. XML 객체의 접근제어를 위한 시스템 구성

4.2 보안 정책(Security Policy)

보안 정책은 객체와 사용자 계층에 대하여 정의된다. 객체에 대한 정책은 접근제어가 요구되는 객체의 보안등급을 지정하는 과정이다. 즉, 대상 객체에 포함된 모든 엘리먼트 및 속성에 대하여 일정한 규칙에 따라 보안 등급이 부여된다. 주체에 대한 보안 정책은 주어진 객체에 대하여 접근 가능한 역할 계층을 정의하는 과정이다. 그림 3의 문서에 대하여 접근 가능한 역할 계층은 다음과 같다. (P): 주어진 문서에서 환자 이름이 동일한 Patient 항목을 볼 수 있는 계층으로 정의 한다. (D): 주어진 문서에서 Medical 부분만 볼 수 있는 계층으로 정의한다. (N): 환자의 현재 상태만 볼 수 있는 계층이다. (S): 환자의 이름과 기타정보를 조회 할 수 있는 계층으로 정의한다. 표 2와 표 3에서 보안 등급 테이블과 역할 계층의 예를 보여준다.

표 2. 객체에 대한 보안 등급 테이블

보안 등급	해당 요소
E	RRN
D	Diagnosis/ Prescription
C	Medical/ Doctor/ Nurse
B	Bill
A	Patient@Name/ Personal /..

표 3. 주체의 역할 계층(RC) 정보

역할 계층	접근가능 항목
P	ABCDE
D	ACD
N	ACD
S_2	AB
S_1	A

4.3 접근제어 정책(Access Control Policy)

문서에 대한 접근제어 정책은 다음과 같이 정의한다. 정책을 P라 할 때, $P = (Sc, O, Ac, Op)$. 여기서 Sc는 보안 계층, 즉 사용자에게 할당된 역할, O는 Sc가 접근할 수 있는 객체, Ac는 접근 가능한 보안, Op는 가능한 연산을 의미한다. Sc와 O는 XPath 식으로 표현된다. 접근제어 정책의 간단한 예를 표 4에서 보여준다. P_1의 의미는 doctor의 역할을 가진 사용자는 PatientRecord 문서의 Pataient 에 포함된 element 중에서 보안등급이 A, C, D를 만족하는 요소들에 Read 연산이 가능하다는 것을 나타낸다. 다른 접근제어 정책 역시 비슷한 의미를 가진다. 다시 말하면 사용자 KimJH는 D(doctor)의 역할을 할당 받게 되고 할당받은 D역할은 Patient 요소에 포함되고 보안등급이 A, C, D를 만족하는 요소들에 대해 read연산이 가능하다. 즉, KimJH 사용자는 표 2에 제시된 보안등급 A, C, D에 포함되는 요소들에 접근이 가능하다는 것을 나타낸다.

V. 접근제어 수행 메커니즘

본 장에서는 접근제어 수행 메커니즘과 역할 계층 관리에 대하여 설명한다. 5.1절에서는 각 사용자 계층에 사용되는 키의 생성과 유도에 대하여 설명한다. 본 절에서 사용된 키 생성과 키 유도 기법은 Chen 등이 제안한 방법을 기반으로 하고 있다.[5] 5.2절에서는 역할 계층의 동적인 관리 기법에 대해 설명 한다.

5.1 계층키 생성과 유도 방법

계층키 생성과 유도 기법에서 다음과 같은 조건이 필요하다. 1.키 생성에 사용되는 대칭형 암호시스템 $E_K(x)$와 $D_K(x)$는 키 K를 이용하여 임의의 입력 값 x에 대하여 암호화 및 복호화를 안전하게 수행한다.

표 4. 접근 제어 정책

ID	정책의 표기
P1	(D, //Patient, ACD , r)
P2	(N, //Patient, ACD, r)
P3	(S1, //Patient, AB, r)
P4	(S2, //Patient, A, r)
P5	(P[@Name], //Patient, ABCDE , r)
P6	(P[@Name],//Medical/Diagnosis= "AIDS" or "Cancer", ABCE , r)

표 5. 키 생성의 예

SC	ID	SK	RelationInfo
P	$P(P)$	$K(N)$	R_{PD}, R_{PN}, R_{PS_1}
D	$P(D)$	$K(N)$	R_{DS_1}, R_{DN}
N	$P(N)$	$K(N)$	-
S_1	$P(S_1)$	$K(S_1)$	-
S_2	$P(S_2)$	$K(S_2)$	-

2. 사용되는 해쉬 함수 $H(x)$는 기존에 알려진 공격에 안전하다.

5.1.1 관계 설정 및 키 생성 단계

관계 설정단계에서는 사용자간의 관계를 고려한 정보를 저장하기 위한 관계 목록을 구성한다. 관계 목록은 사용자의 키 유도에 대한 정보를 제공한다. 관계 목록은 계층의 모든 사용자에게 공개된다. 그러나 CA만이 관계 목록의 내용을 수정할 수 있는 권한을 가진다. 역할 계층에서 서로 독립된 n개의 보안 계층 $SC_1, ..., SC_n$이 존재한다고 가정할 때, CA는 보안 계층 SC_i에 대한 비밀키 SK_i를 유도하기 위하여 다음의 과정을 수행한다. 1.계층의 모든 보안 계층 SC_i에 대하여, CA는 임의의 두 정수 P_i와 sk_i를 선택하고, 안전한 방법으로 각 계층에 sk_i를 전송하고, P_i는 공개한다. 2.전위 순환을 통해 계층으로부터 보안 계층 SC_i를 획득한다. 3.관계 $SC_j \leq SC_i$를 유지하는 보안 계층 SC_i에 대하여, SC_j의 비밀키를 유도하기 위한 공개변수 R_{ij}를 계산한다. 여기서 $R_{ij} = E_{H(P_j \oplus SK_i)}(sk_j)$가 된다. 4.각 보안 계층이 역할 계층에 포함되도록 과정을 반복한다. 위의 모든 과정이 끝나면 표 5와 같은 결과를 얻을 수 있다. 표 5는 과정 1-2에서 각각의 보안계층의 식별자인 ID와 비밀키 SK가 할당되고 과정 3에서 할당된 2개의 요소들을 사용하여 보안계층 사이의 관계를 만든다. 키 생성단계는 키 생성을 위한 것보다는 관계설정을 위한 과정이라고 할 수 있다. 즉, 관계를 만들기 위해 필요한 2개의 요소인 식별자 ID와 비밀키 SK를 각 역할(보안 계층)에 할당하고 2개의 요소를 이용해서 각 역할간의 관계를 만드는 것이다. 과정1-2가 수행되고 나면 그림 5-a에서와 같이 각 역할에 ID와 SK가 할당된 것을 볼 수가 있다. 과정 3에서 만든 관계들을 할당하면 그림 5-b에서와 같은 각 역할 간의 순서관계를 만들 수 있다.

5.1.2 키 유도 단계

관계 $SC_j \leq SC_i$가 성립하는 두 계층 SC_i와 SC_j가

표 6. 관계설정

$R_{PD} = E_{H(P(D) \oplus K(P))}(K(D))$
$R_{PS_2} = E_{H(P(S_2) \oplus K(P))}(K(S_2))$
$R_{DS_1} = E_{H(P(S_1) \oplus K(P))}(K(S_1))$
$R_{DN} = E_{H(P(N) \oplus K(P))}(K(N))$
$R_{PN} = E_{H(P(N) \oplus K(P))}(K(N))$
$R_{PS_1} = E_{H(P(S_1) \oplus K(P))}(K(S_1))$

존재한다고 가정하자. SC_j의 등급에 해당하는 영역에 접근하기 위해서 SC_i는 SC_j의 비밀키를 유도해야 한다. 비밀키 sk_j를 유도하기 위해 보안 계층 SC_i에 속한 사용자는 다음의 과정을 수행해야 한다. 1. SC_i 자신의 비밀키 sk_i와 SC_j의 공개 매개변수 P_j를 이용해 해쉬값 $H(P_j \oplus sk_i)$ 를 계산한다. 2. SC_i와 SC_j의 공개변수 R_{ij}를 이용해 sk_j를 유도한다.

$sk_j = D_{H(P_j \oplus SK_i)}(R_{ij}) = D_{H(P_j \oplus SK_i)}(E_{H(P_k \oplus SK_i)}(sk_k))$ 예를 들어 환자의 정보를 나타는 XML 객체에서 S_1에 해당하는 데이터 영역에 D가 접근하기 위해서는 보안 등급 D는 S_1의 비밀 키를 유도해야 한다. S_1의 비밀키 SK_{S_1}을 유도하기 위해서 보안계층 D는 과정 1에서와 같이 자신의 비밀키 SK_D와 S_1의 공개 정보 $P(S_1)$을 이용해 복호화에 쓰일 해쉬값 $H(P(S_1) \oplus SK_D)$을 계산하고 과정 2와 같이 $H(P(S_1) \oplus SK_D)$를 키로 사용하고 R_{DS_1}을 인수로 가지는 복호화 과정을 거쳐 S_1의 비밀키 SK_{S_1}을 유도한다.

$$SK_{S_1} = D_{H(P(S_1) \oplus SK_D)}(R_{ij}) = D_{H(P(S_1) \oplus SK_D)}(E_{H(P(S_1) \oplus SK_D}(SK_{S_1}))$$

5.2 역할 계층의 관리

본 절에서는 제안된 모델에서의 역할 계층 관리 기법에 대하여 설명한다.

5.2.1 역할 계층의 관리

기존의 역할 계층 구조에서, 새로운 역할 계층 SC_k가 SC_i의 하위 계층으로 추가 된다고 가정하자.

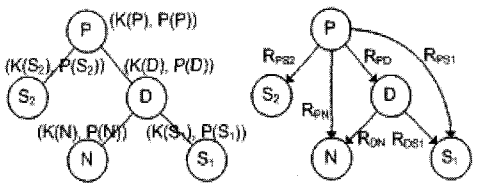


그림 5. (a) ID + 계층 키 (b) 관계 계층

새로운 계층의 추가를 위해서 다음과 과정을 수행한다. 1. CA는 두개의 큰 양의 정수 P_k와 S_k를 선택하여, 보안 계층 SC_k에게 S_k를 안전한 방식으로 전송하고 P_k를 공개한다. 2. 관계 $SC_k \leq SC_i$를 유지하는 보안 계층 SC_i에 대하여, CA는 공개변수 R_{ik}를 계산한다. $R_{ik}=E_{H(P_k \oplus SK_i)}(sk_k)$. 3. 관계 $SC_j \leq SC_k$를 유지하는 보안 계층 SC_j에 대하여, CA는 공개변수 R_{kj}를 계산한다. $R_{kj}=E_{H(P_j \oplus SK_i)}(sk_j)$. 4. 관계 $SC_k \leq SC_i$와 $SC_j \leq SC_k$를 유지하는 보안 계층 SC_i와 SC_j에 대하여, CA는 공개변수 R_{ij}를 계산한다. 단, $R_{ij}=E_{H(P_j \oplus SK_i)}(sk_j)$ 그림5-b에서 역할 D_1이 역할 P의 하위 계층으로 추가 된다고 가정했을 때, 역할D_1의 ID와 SK_{D_1}가 CA에 의해 할당되고, 순서 관계에 따라 관계들이 계산된다. D_1은 P의 하위 계층이고 N의 상위 계층이므로, 관계 $R_{D_1N}=E_{H(P(N) \oplus K(D_1))}(K(N))$과 $R_{PD}=E_{H(P(D_1) \oplus K(P))}(K(D_1))$를 추가 한다.

기존의 역할 계층 구조에서, 역할 계층 SC_k가 삭제되는 경우 공개 디렉토리의 갱신을 통해서 CA는 계층 SC_k와 연관된 모든 공개 파라미터를 삭제할 수 있다. 1. CA는 P_k와 sk_k를 삭제한다. 2. CA는 관계 $SC_k \leq SC_i$를 유지하는 보안 계층 SC_i에 대하여 R_{ik}를 삭제한다. 3. CA는 관계 $SC_j \leq SC_k$를 유지하는 보안 계층 SC_j에 대하여 R_{kj}를 삭제한다. 4. CA는 관계 $SC_j \leq SC_k$를 유지하는 보안 계층 $SC_k \leq SC_i$와 $SC_j \leq SC_k$에 대하여 R_{ij}를 삭제한다. 그림 5-b에서 역할 D가 취소된다고 가정하면, 역할 D의 ID와 SK를 삭제한다. 그리고 순서관계에 따라 연관된 관계들을 삭제한다. 그림 5-b에서는 관계 R_{PD}와 R_{DN} 을 삭제한다.

5.2.2 역할 관계의 관리

보안 계층 SC_p가 보안 계층 SC_q에 대하여 접근이 승인되었다고 가정하자. 이 경우, SC_p와SC_q 사이에 새로운 관계가 $SC_q \leq SC_p$를 만족하도록 계층에 추가되어야 한다. 새로운 역할 관계의 추가를 위하여 CA는 새로운 관계변수 R_{pq}를 계산한다. SC_q의 모든 하위 역할은 SC_q가 SC_p에 종속되는 것과 마찬가지로 SC_p의 하위 역할이 된다. 따라서 CA는 SC_q의 모든 하위 역할에 대한 관계변수를 계산한다. SC_p의 상위 역할에게 승인된 동일한 관계가 SC_q에게도 설정되어야 하므로 CA는 SC_p의 상위 역할을 갱신하고, 해당되는 관계변수를 계산한다. 최종적으로, SC_q의 하위 계층과 SC_p의 상위 계층 사이의 관계를 구성하고 해당되는 관계변수를 계산한다. 이 과정을 정리하면 다음과 같다. 1. 추가되는 관계 $SC_q \leq SC_p$에 대하여, CA는 $R_{pq}=E_{H(P_j) \oplus (sk_p)}(sk_q)$ 를 계산한다. 2. 관계 $SC_j \leq SC_q$를 가지는 임의의 보안 계층 SC_j에 대하여, 새로운 관계 $SC_q \leq SC_p$가 추가된 후에 SC_j는 SC_p에 대하여 새로운 자손이 된다. CA는 SC_p와 SC_j에 대하여 관계변수 R_{pj}를 계산한다. 단, $R_{pj}=E_{H(P_j) \oplus (sk_p)}(sk_j)$가 된다. 3. 관계 $SC_p \leq SC_i$인 임의의 보안 계층 SC_i에 대하여, 새로운 관계 $SC_q \leq SC_p$가 추가된 후에, SC_i와 SC_q 사이의 새로운 관계를 위하여 CA는 R_{iq}를 계산한다. 단, $R_{iq}=E_{H(P_j) \oplus (sk_i)}(sk_q)$ 4. $SC_j \leq SC_q$와 $SC_p \leq SC_i$에 대하여, CA는 $R_{ij}=E_{H(P_j) \oplus (sk_i)}(sk_j)$ 를 계산한다. R_{ij}는 새로운 관계가 추가되기 전까지 존재하지 않은 관계변수이다. 예를 들어, 그림 5-b에서 역할 S_2와 역할 N사이의 역할 관계가 생긴다면 키 생성 단계의 과정 3을 통해 관계 R_{S_2N} 을 추가 해주면 된다. 그리고 표 6의 역할 S_2의 RelationInfo에 R_{S_2N}만 추가하면 역할 S_2와 역할 N사이에 관계가 새로 생성된다.

역할 관계 $SC_q \leq SC_p$가 계층에서 삭제되는 경우 CA는 다음과 같이 공개 디렉토리의 갱신을 수행한다. 1. CA는 관계 $SC_q \leq SC_p$를 취소하기 위해 R_{pq}을 삭제한다. 2. 관계 $SC_j \leq SC_q$와 $SC_q \leq SC_p$ 를 만족하는 임의의 보안 계층 SC_j에 대하여, CA는 R_{pj}을 삭제한다. 3. $SC_p \leq SC_i$와 $SC_q \leq SC_p$ 를 가지는 임의의 보안계층 SC_i에 대하여 CA는 R_{iq}을 삭제한다. 4. $SC_j \leq SC_q$와 $SC_p \leq SC_i$에 대하여 CA는 R_{ij}를 삭제한다. 그림 5-b의 관계들 중에서 역할 D와 역할 N사이의 관계 R_{DN}을 삭제하는 경우에 표 6에서 관계 R_{DN}을 삭제하고, 표 5에서 역할 D의 RelationInfo에서 R_{DN}을 삭제하면 된다.

Ⅵ. 제안된 방식의 평가

6.1 보안성 평가

· 공개변수를 이용한 상위계층 비밀키 유도 공격

고려할 수 있는 첫 번째 공격 유형은 하위 계층의 사용자가 공개된 파라미터와 자신이 소유한 비밀키를 통하여 자신과 이웃한 계층 또는 상위 계층의 비

표 7. 제안된 모델의 기능적 특성 비교

비교 항목	Damiani [6]	Cristian [7]	Jeon [8]	Jason [12]	제안된 모델
기반 모델	DAC	없음	없음	RBAC	RBAC
접근제어 수행 주체	개별사용자	개별사용자	개별사용자	역할이 부여된 사용자	역할을 부여받은 사용자
접근제어 대상 객체	인스턴스 문서	엘리먼트	엘리먼트	엘리먼트	인스턴스, 엘리먼트
메커니즘 적용 방식	노드 필터링	암호기술 적용	XPath 필터링	암호기술 적용	해쉬함수/대칭형 암호화
영역분할 방식	레이블링	엘리먼트 지정	엘리먼트 지정	엘리먼트 지정	객체의 보안등급에 따라
레이블링 과정	필요	필요	필요	불필요	불필요
엘리먼트 표현	XPath 사용	엘리먼트 이름	XPath사용	XPath사용	XPath 사용
전체 키의 수	지원되지 않음	노드의 수와 동일	지원되지 않음	역할 수 +1	역할 수와 동일
역할의 동적 관리	불가능	불가능	불가능	불가능	가능
주체 관리 키 수	지원되지 않음	접근하고자 하는 노드 수와 동일	지원되지 않음	1개	1개
동적 키 관리 지원	불가능	불가능	불가능	불가능	가능
역할 관리의 방법	정적	정적	정적	정적	동적

밀키를 유도할 수 있는가의 여부이다. 즉, $SC_j \le SC_i$로 구성된 계층구조에서 계층 SC_j에 속한 사용자가 R_{ij}와 sk_j를 이용하여 SC_i의 비밀키를 얻을 수 있는가? 이러한 공격 방식은 승인되지 않은 공격자가 알려진 평문을 통해 문제를 해결하고자 것과 동일하다.

· 협업에 의한 공격

상위 계층에서의 비밀키를 유도하기 위한 시스템의 하위 계층에서의 둘 이상의 사용자에 의한 협업 공격에 대한 문제를 생각해보자. SC_i의 하위 계층인 SC_j와 SC_k가 SC_i의 비밀키를 얻기 위하여 협업공격을 시도하는 경우, 공격자는 $R_{ij}=E_{H(P_j)\oplus(sk_j)}(sk_j)$, $R_{ik}=E_{H(P_i)\oplus(sk_j)}(sk_k)$ 와 자신의 비밀키를 이용해 공격을 시도해야 한다. 그러나 해쉬 함수의 특성상 $sk_j, sk_k, R_{ij}, R_{ik}$를 이용하여 공격자는 sk_i를 역으로 유도할 수 있는 방법이 없다. 따라서 하위 계층이 상위 계층의 비밀 키를 얻기 위한 방법은 존재하지 않음을 알 수 있다.

· 내부 정보 수집에 의한 공격

$SC_i, SC_{i+1}, \cdots SC_{i+m}$으로 구성된, m개의 부모 노드를 가지는 계층 S_j에 속한 사용자가 존재하는 시스템을 생각해보자. 공개인수 $R_{ij}, R_{(i+1)}, \cdots R_{(i+m)j}$,의 수집에 의하여 공격자는 그의 부모중 하나에 대한 비밀키를 유도하기 위한 시도를 할 수 있다. 이러한 공격 방식은 승인되지 않은 공격자가 알려진 평문을 통해 문제를 해결하고자 것과 동일하다.

· 공격 4. 외부 정보 수집에 의한 공격

공격 3의 경우와 마찬가지로, 공격자가 시스템의 외부로부터 접근을 시도하는 경우, 대칭키 암호시스템에 대한 암호문 공격을 해결해야 한다. 일반적으로 암호문을 이용한 대칭키 암호시스템에 대한 공격은 평문을 이용한 공격보다 어렵다고 알려져 있으므로, 공격자는 외부 수집을 통한 공격을 성공시킬 수 없다.

6.2 기능성 평가

본 절에서는 본 논문에서 제안된 방식이 가지는 주요 특징을 이전 방식들과 비교하여 본 논문에서 제안된 모델의 기능적 특징에 대하여 평가한다. 평가의 기준은 접근제어 수행의 주체, 접근제어의 단위, 메커니즘 구현 방식, 역할의 동적 관리, 사용된 키의 수 등이다.

· 접근제어 주체

최근까지 XML 문서의 접근제어를 위한 다양한 기법들이 제안되었다.[11-14] 그러나 기존 기법들의 공통적인 단점은 접근제어 수행 주체를 개별 사용자로 정의하고 있다는 점에 있다. 사용자와 접근제어 대상 객체의 관계를 1대1로 지정하는 형태로 접근제어 규칙을 정의하고 적용함으로써 사용자와 대상 객체 사이에서 1대1의 접근제어는 가능하지만, 대규모의 사용자 또는 대규모의 스키마 문서와 이를 따르는 인스턴스 문서를 가지는 환경에서는 적용에 한계가 존재한다. 본 논문에서 제안된 방식은 접근제어 수행 주체를 사전에 부여된 역할 그룹으로 정의하고, 역할 계층에 대하여 명시적으로 접근 가능한 접근제어 목

록을 정의함으로써 대규모의 사용자 또는 대규모의 스키마 문서와 이를 따르는 인스턴스 문서를 가지는 환경에서 보다 효율적으로 적용할 수 있다.

· 접근제어 단위

XML 인스턴스 문서는 보안 민감성의 수준이 다른 각각의 요소를 포함할 수 있으므로 다양한 접근제어 계층이 지원되어야 한다. 이러한 요구사항을 만족시키기 위해서는 접근제어 메커니즘이 최소한의 단위로 보안 정책을 적용할 수 있는 충분한 유연성을 제공해야 하는데, 본 논문에서 제안된 모델은 대상 문서에 대한 최소 접근 가능 영역을 엘리먼트 단위로 정의하여 접근제어를 수행할 수 있다.

· 접근제어 영역의 분할

기존의 연구에서는 접근제어 영역을 정의하기 위하여 해당 문서를 트리화하고, 모든 노드에 접근제어 정책을 기술하는 방법(접근제어 정책의 레이블링 과정)을 수행하여 접근제어 영역을 분할한다. 그러나 본 논문에서는 각 엘리먼트에 대한 보안 등급을 정의하고 보안등급에 따라 접근제어 영역을 정의한다. 이러한 방식의 장점은 접근 제어가 반드시 필요한 영역은 한정되어 있으므로, 접근 제어가 필요한 노드들에 대해서만 보안 등급을 지정하여 요구되는 보안정책의 수를 줄일 수 있다.

Ⅶ. 결 론

본 논문에서는 XML 객체에 대한 접근제어를 위하여 RBAC의 역할 계층과 계층적 키 유도/할당 기법을 결합한 접근제어 모델과 메커니즘을 제안하였다. 본 논문에서 제안된 방식은 XML 객체를 위한 접근제어에서 RBAC가 제공하는 관리상의 이점뿐만 아니라, 상위 계층의 사용자가 하위 계층의 키를 유도하여 사용할 수 있게 지원하므로 각 역할 계층에서 관리하는 키의 수가 기존 방식에 비하여 줄어드는 특징을 제공한다. 또한 보안 계층이 추가 되거나 삭제되는 경우에 해당 보안 계층 간의 관계만을 갱신함으로서 전체 암호화에 사용된 전체키를 갱신할 필요가 없다는 장점을 가진다. 이후 연구에서는 제안된 모델의 실제적인 구현을 통하여 제안된 모델의 효율성과 가용성에 대하여 평가하는 작업이 이루어질 예정이다. 또한 제안된 모델에서 고려되지 않은 부분인 상황 정보를 제안된 모델과 결합시키는 작업들도 이루어져야 한다.

참 고 문 헌

[1] R. Sandhu, E.J.Coyne, H.L. Feinstein, "Role-based Access Control Models," *IEEE Computer*, Vol.29(2), pp. 33-47, 1996.

[2] Selim G. Akl, Peter D. Taylor, "Cryptographic solution to a problem of access control in a hierarchy," *ACM Transactions on Computer Systems*, Vol.1(3), pp. 239-248, Aug 1983.

[3] Chang, C.C, Hwang, R.J, Wu,T.C, "Cryptographic Key assignment scheme for access control in a hierarchy," *Infromation System*, Vol.17(3), pp. 243-247, 1992.

[4] 박영희 외 5인,"Diffie-Hallman 키 교환을 이용한 확장성을 가진 계층적 그룹키 설정 프로토콜," 정보보호학회논문지, 13(5), pp. 3-15, 2003.

[5] T.S. Chen, J.Y. Huang, "A novel Key management scheme for dynamic access control in a user hierarchy," *Applied Mathematics and Computation*, Vol.162(1), pp.339-351, 2005.

[6] E. Damiani, C. Vimercati, S. Paraboshi, P. Samarati, "Securing XML Documents," EDBT 2000, Germany, pp. 27-31, June, 2000.

[7] C. G. Pollmann, "XML Pool Encryption," XMLSEC02, USA, pp.1-9, 22, Nov, 2002.

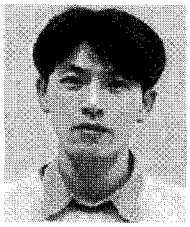
[8] J.M. Jeon, Y.D. Chung, M.H. Kim, Y.J Lee, "Filtering XPath expressions for XML access control", *Computers & Security*, Vol.23(7), pp. 591-605, 2004.

[9] Hao He, Raymond K. Wong, "A Role-Based Access Control Model for XML Repositories," 2001.

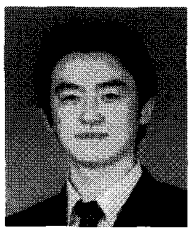
[10] J.Wang, S. Osborn, "A Role Based Approach to Access Control for XML

Databases," SACMAT'04, June, 2004.
[11] 최동희, 박석, 접근제어 정책구현을 위한 역할기반 XML 암호화," pp. 3-15, 정보보호학회논문지, 15(1), 2005.
[12] Jason Crampton, "Applying Hierarchical and Role-Based Access Control to XML Documents," *In Proc. of ACM Workshop on Secure Web Services 2004*. pp. 41-50, 2004.
[13] www.w3c.org, "eXtensible Markup Language1.0," W3C Recommendation, 04 February 2004.
[14] www.w3c.org, "XML-Signature Syntax and Processing," W3C Recommendation, 12 February 2002.
[15] www.w3c.org,"XML Encryption Syntax and Processing,"W3C Recommendation, 10 December 2002.
[16] http://docs.oasis-open.org/xacml/2.0/

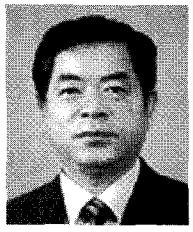
〈著者紹介〉



반 용 호 (Yong Ho Ban) 학생회원
1998년 2월: 동서대학교 전자공학과 졸업(학사)
2000년 8월: 동아대학교 대학원 컴퓨터공학과 졸업(석사)
2003년 2월: 동아대학교 컴퓨터공학과 박사과정 수료
〈관심분야〉 암호 프로토콜, 접근제어 모델 및 메커니즘 설계, 유비쿼터스 환경의 정보보호



배 경 만 (Kyoung Man Bae) 학생회원
2004년 2월: 동아대학교 컴퓨터공학과 졸업(학사)
2004년 3월~현재: 동아대학교 대학원 컴퓨터공학과 석사과정
〈관심분야〉 계층 키 분배, 접근제어, 유비쿼터스 환경의 정보보호



김 종 훈 (Jong Hoon Kim) 정회원
1974년 2월: 동아대학교 전자공학과 졸업(학사)
1977년 2월: 동아대학교 대학원 전자공학과 졸업(석사)
1986년 2월: 경북대학교 대학원 전자공학과 졸업(박사)
1986년 ~현재: 동아대학교 컴퓨터공학과 교수
〈관심분야〉 암호이론, 접근제어, 유비쿼터스, HW/SW 통합설계,