XACML을 이용한 클래스 간 접근제어

*송해선 **임경식

경북대학교

*hssong@ccmc.knu.ac.kr **kslim@knu.ac.kr

Access Control among Classes Using XACML

*Haesun Song **Kyungshik Lim

Kyungpook National University

요 약

접근제어 기술 중 하나인 XACML(eXtensible Access Control Markup Language)은 XML기반으로 다양한 시스템 사이에서 접근제어정책(Access Control Policy)을 기술하는 표준이다.[1] XACML은 정책을 설정하여 접근 권한을 제공하는 방법으로 시스템 환경에 적합한 접근제어가 가능하다. 본 논문에서는 클래스 간 참조 환경에서 XACML을 이용한 접근제어를 제안하여 정책을 이용한 접근제어 시스템을 구현한다. 그리고 OSGi(Open Service Gateway initiative) 기반의 OSEE(Overlay Service Execution Environment) 실행환경을 이용하여 오버레이 서비스의 클래스 간 접근제어를 실험하고 클래스 참조 환경과 상황에 따른 접근제어가 가능하도록 하였다.[2]

1. 서 론

XACML은 비즈니스 서비스를 고려한 다양한 접근제어 정책의 설정이 가능하고 EAM(Extranet Access Management)과 같은 차세대 서비스에서 통합 인증을 위한 SAML(Security Assertion Markup Language)과 연동되어 사용될 수 있다. 이는 접근제어 정책을 설정함에 있어서 확장성, 가독성, 상호 호환성을 제공하기 때문이다. 현재 홈 네트워크 및 e-비즈니스는 보안 인증을 위한 통합접근 관리 방안으로 XACML을 이용한 기술을 적용하고 있다.

자바언어는 응용 프로그램 및 서비스 개발을 위하여 클래스 참조를 제공한다. 이는 사용자들이 모든 속성과 기능을 구현할 필요 없이도 프로그램 개발이 가능하다. 그러나 시스템 상에서 허가되지 않은 사용자가 클래스를 참조 할 경우 서비스 수정 및 삭제와 같은 보안상의 문제가 발생한다. 따라서 사용자의 접근을 구별하고 제어할 수 있는 방안이 필요하다.

본 논문에서는 자바의 클래스 간 참조 환경에서 XACML을 이용하여 접근제어 할 수 있는 방안을 제시하고 구현한다. 그리고 OSGi 프레임워크 기반의 오버레이 서비스 실행환경인 OSEE에서 오버레이 서비스 클래스 간 접근제어에 적용하여 실험한다. 본 논문의 구성은 다음과 같다. 2장에서는 기존의 접근제어 기술에 대하여 소개하고 제한사항을 분석한다. 3장에서는 논문에서 제안하는 XACML 기반의 접근제어 모델 및 정책에 관하여 설명한다. 4장에서는 설계된 모델을 구현하고 클래스 간 참조를 제어하는 실험을 통하여 결과를 분석한다. 마지막으로 5장에서는 본 연구의 결론에 대해 서술한다.

본 연구는 한국과학재단 목적기초연구(R01-2003-000-10562-0)와 정보통신연구진흥원의 대학 IT연구센터 지원으로 수행되었음.

2. 관련 연구

2.1 접근제어 기법

접근제어 기법은 크게 임의적 접근 제어(Discretionary Access Control), 강제적 접근 제어(Mandatory Access Control)와 역할 기반 접근 제어(Role Based Access Control)가 있다. 임의적 접근제어는 접근하려는 주체 또는 그룹들의 신분에 근거하여 객체에 대한 접근을 제한하는 방법이다. 이는 접근을 요청하는 사용자의 식별을 통하여 접근제어를 수행하며 개체에 대한 권한을 가지고 있는 사용자가 접근 권한을 추가 및 제거할 수 있다는 의미에서 임의적 특성을 가지는 접근제어 정책이다. 강제적 접근제어는 객체에 대한 정보의 비밀성과 이러한 비밀성에 대한 접근 레벨을 정의하여 주체의 접근 권한에 이를 적용시키는 방법이다. 이는 접근 권한이 변경되지 않으며, 하위 레벨의 객체로 정보의 흐름을 허용하지 않기 때문에 흐름 제어 정책으로 정의될 수 있다. 역할 기반 접근제어는 역할을 중심으로 주체와 역할과의 상관관계와 객체의 접근 권한과 상관관계로 나누어진다. 즉, 객체에 접근하기 위해서는 해당 역할의 멤버가 되는 주체만이 접근할 수 있다. 본 논문에서는 참조를 제공하는 클래스가 접근하려는 클래스를 식별하고 권한을 설정하여 제어할 수 있도록 임의적 접근제어 모델을 기반으로 정책을 설