XACML기반 자원 접근제어 시스템 모델 연구

송준홍*°,이형석* ,김동수**, 신동규*

*세종대학교 컴퓨터공학과, **한국전산원

A Study on XACML based Resource Access Control System

Song, Jun-Hong Lee, Hyoung-Suk Kim, Dong-Soo Shin, Dong-Kyoo

Sejong University, National Computerization Agency

E-mail : {song0424, bestehen, shindk}@gce.sejong.ac.kr, kimdsoo@nca.or.kr

요 약

웹 서비스의 등장으로 XML이 기반 기술로서 자리 매김하고 있는 현재, XML을 이용하여 여러 표준기술을 제정하려는 움직임이 많아지고 있다. XACML은 접근제어 리스트(access control list)를 통해 보안이 요구되는 자원에 대해 미세한 접근 제어 서비스를 제공할 수 있는 XML 기반의 언어이다. XACML은 SAML PDP(Policy Decision Point)의 일부로서 역할을 수행 할 수 있으며 각 정의에 따라 각각의 사용자 별 XML 문서 접근 정책을 수립하고 적용 할 수 있다. 본 논문에서는 XML기반의 Access Control 표준인 XACML에 대하여 분석하고 적용 방법에 대하여 연구하였다.

1. 서론

특정 업체별로 상이했던 어플리케이션 프로토콜은 현재 XML을 기반으로 단일화되어 가고 있다. 또한 웹 서비스 및 XML 기반 전자상거래 프레임워크 등에서 기반 기술 언어로 활용되고 있으며 다양한 적용 연구 및 표준 기술 개발 또한 한창 진행 중 이다. 비즈니스에서도 ebXML을 중심으로 XML기술이 빠르게 도입되고 있으며 보안 기술의 적용이 중요하게 다루어지고 있다. XML보안 기술로 XML 전자서명[1], XML 암호화[2], 인증 서비스인 SAML[3], XML기반 PKI 표준 기술인 XKMS[4]와 더불어 XACML[5] 등을 대표적인 기술로 들 수 있다. SAML은 인증과 승인 서비스 프레임워크를 제시하고 있고 XML기반 공개키 서비스를 위해 XKMS의 개발이 진행되고 있다. 특히 데이터의 활용에 XML을 이용하는 비중이 커지면서 데이터에 대한 섬세하고 정확한 접근이 필요하게 되었고, 이에 대한 정책 수립이 중요한 문제로 제기되면서 XACML이 제안되었다.

XACML은 접근제어 리스트(access control list)를 통해 보안이 요구되는 자원에 대해 미세한 접근 제어 서비스를 제공 할 수 있는 XML 기반의 언어로서 인증 서비스인 SAML의 PDP(Policy Decision Point)의 일부로서 역할을 수행 할 수 있고 PDP에서는 제정된 정책에 따라 자원 접근 권한 리스트로 각각의 사용자 별 XML 문서 접근 정책을 수립하고 적용 할 수 있다. XACML은 웹 서비스와 ebXML에서 접근제어 표준기술로 활용될 전망이다. 이 논문에서는 XML 접근제어 표준안인 XACML기술을 분석하고 적용방안에 대하여 논할 것이다.

2. XACML 기술 분석

2.1 XACML 개요

XACML(eXtensible Access Control Markup Language)은 XML문서에 대한 미세한 접근을 정책리스트를 이용하여 제어할 수 있는 XML기반의

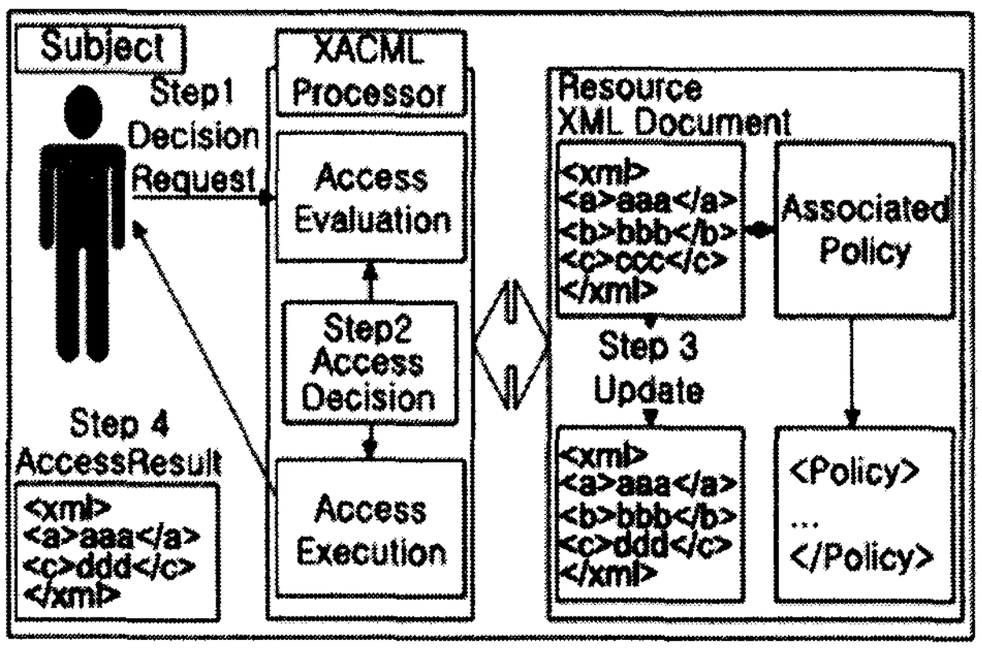
언어이다. XACML TC(Technical Commitee)에서는 XACML로 정의된 기술로 정책과 인증을 표현하기 위한 XML 스키마를 제정하고 있다. 이 정책에서의 리소스는 XML을 사용하여 표현되는 어떠한 객체도 될 수 있으며 XACML은 XPath[6]나 LDAP 등 다양한 프로토콜과 함께 바인딩하여 사용될 수 있으며 필요하다면 어떠한 새로운 프로토콜과도 함께 사용될 수 있다. XACML은 인증시스템의 섬세한 접근과 접근자 요청의 특징적인 역할에 대한 제어를 할 것으로 기대된다.

XACML은 크게 resource, subject, action의 3가지 요소로 구성되는데 subject는 접근 주체, 역할 등을 나타내는 사용자의 ID 나 그룹이 될 수 있고, resource는 subject가 접근할 데이터를 의미하며 그 데이터의 참조로서 단일 XML 문서에서 개별 요소 수준까지 지정 할 수 있다. action은 resource에 대한 수행 가능 동작으로 구성되며 각각은 읽기, 쓰기, 생성 등의 작업이 될 수 있다.

XACML은 공통의 산업 명세를 만드는 국제적인 컴소시엄인 OASIS(the Organization for the Advancement of Structured Information Standards)에 의해 표준화되고 있으며 현재 Working Draft 상태이다.

2.2 XACML 명세서

XACML명세서(eXtensible Access Control Markup Language)[7]는 XML문서에 대해 접근 제어 데이터 구조를 위한 문법과 의미를 정의하고 있으며 접근 제어에 대한 기술 요소들을 포함하고 있다. 그림1은 XACML프로세스의 개념도이다.



[그림 1] XACML 프로세스 개념도

Subject인 접근 주체는 XML문서 자원에 접근하기 위하여 접근하려는 자원의 요청정보가 담긴 Decision Request를 제출한다. XACML프로세서는 인증 정보를 바탕으로 정책(Policy)에 따라 접근권한평가 후 권한에 따른 자원의 접근을 허가한다. 접근 주체는 권한에 따른 적절한 실행 결과를 알 수 있다.

① Decision Request

접근자가 XML자원에 접근하려는 목적으로 제출하는 요청서로 PDP에서 수신하는 문서이다. 접근하려는 주체가 <Subject>엘리먼트에 명시되고, <Resource>는 접근하려는 자원, <Action>엘리먼트는 자원에 대한 접근자의 실행을 명시하며 read, write 등의 값을 갖는다. 표1은 Decision Request 문서의 기본 구조를 보여준다. SAML의 인증, 승인, 역할 정보와 함께 subject, resource, action정보를 가지고 있다.

```
<?xml version="1.0" encoding="UTF-8"?>
<Request>
<Subject>...</Subject>
<Resource>…</Resource>
<Action >...</Action>
<saml:Assertion>
   <saml:AuthenticationStatement>
   <saml:Subject> … </saml:Subject>
   </saml:AuthenticationStatement>
</saml:Assertion>
<saml:Assertion>
   <saml:AttributeStatement>
   <saml:Subject> ... </saml:Subject>
   <saml:Attribute AttributeName="role">...
   </saml:Attribute>
   </saml:AttributeStatement>
</saml:Assertion>
</Request>
```

[그림 2] Decisioin Request의 기본 구조

② Rule

Rule은 접근 주체별로 특정 resource에 대하여 어떤 동작을 허용하는 지에 대하여 정의하는 문서

이다.

```
<?xml version="1.0" encoding="UTF-8"?>
<Rule Effect="Permit">
<Description>...</Description>
<Target>
    <Subjects>...
    </Subjects>
    <Resources>...
    </Resources>
    <Actions>...
    </Actions>
</Target>
<Condition>...
</Condition>
</Rule>
```

[그림 3] Rule의 기본 구조

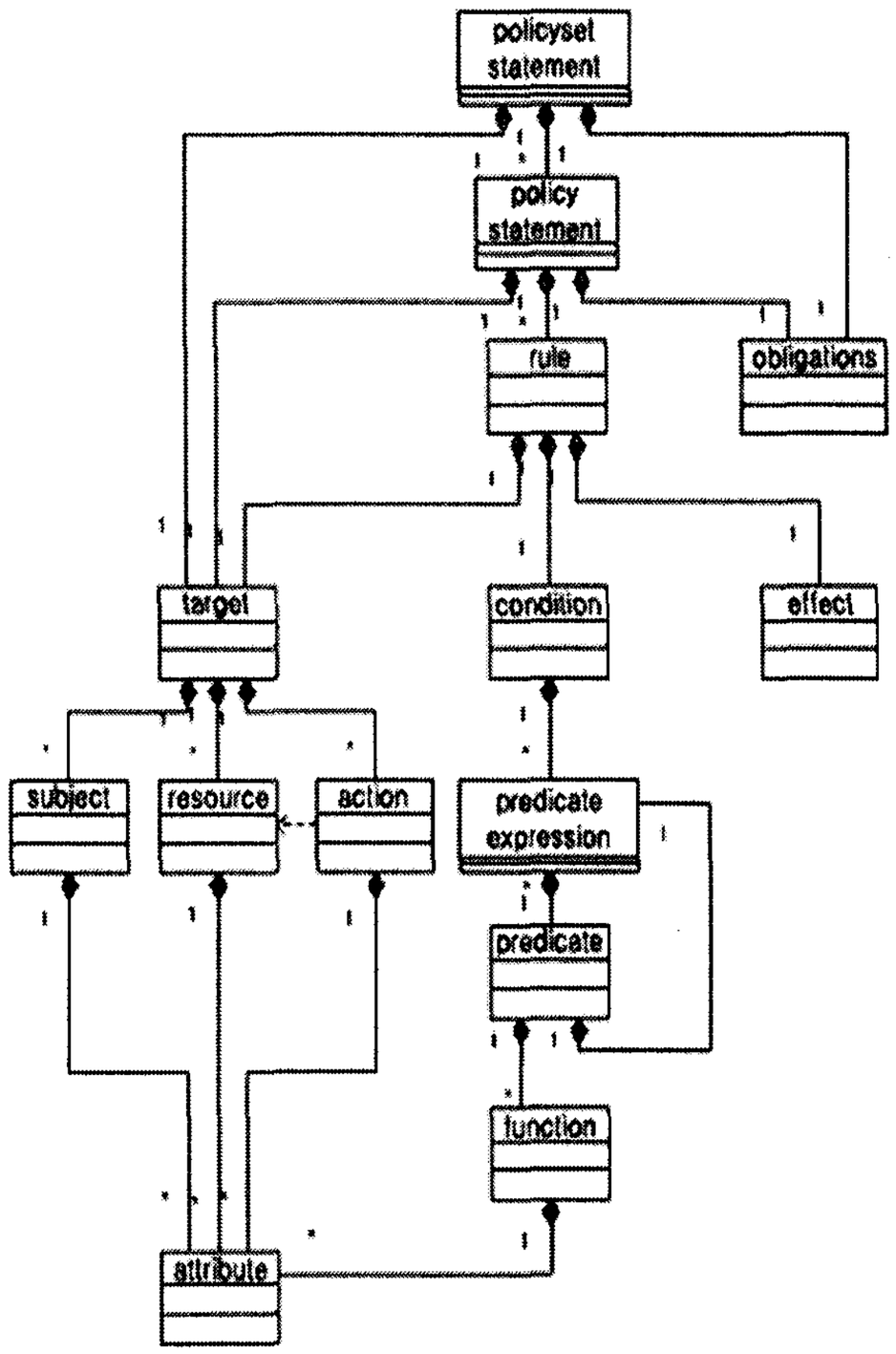
<Rule>엘리먼트는 effect속성에서 'permit', 'deny' 값을 가지며 해당 resource에 대한 정책의 허용, 거부를 명시하여 적용된다. <Subject>, <Resource>, <Action>은 Decision Request에서의 역할과 같으며 <Condition>엘리먼트는 조건을 나타내는 엘리먼트로 이 조건이 만족되면 자원접근 또는 거부가 가능하다. 정책은 이러한 Rule이 여러 개가 모여 수립된다. 정책 모델은 [그림 4]와 같은 구조를 가진다.

③ 데이터 흐름도

XACML의 데이터 흐름 모델은 [그림 5]와 같다. 다이어그램에서 보여주는 데이터 흐름은 저장소에서 유용하게 사용될 수 있는데 예를 들어 PDP와 PIP(Policy Information Point), PDP와 PRP(Policy Retrieval Point) 혹은 PAP(Policy Administrator Point)와 PRP사이의 통신이 적절하게 이용 될 수 있다. 그러나 XACML 명세서는 저장소에서의 사용이나 특정한 통신 프로토콜에서의 활용에 제한을 두고 설계되지는 않았다. 모델에서 보여주는 데이터의 흐름은 다음과 같은 순서를 따른다.

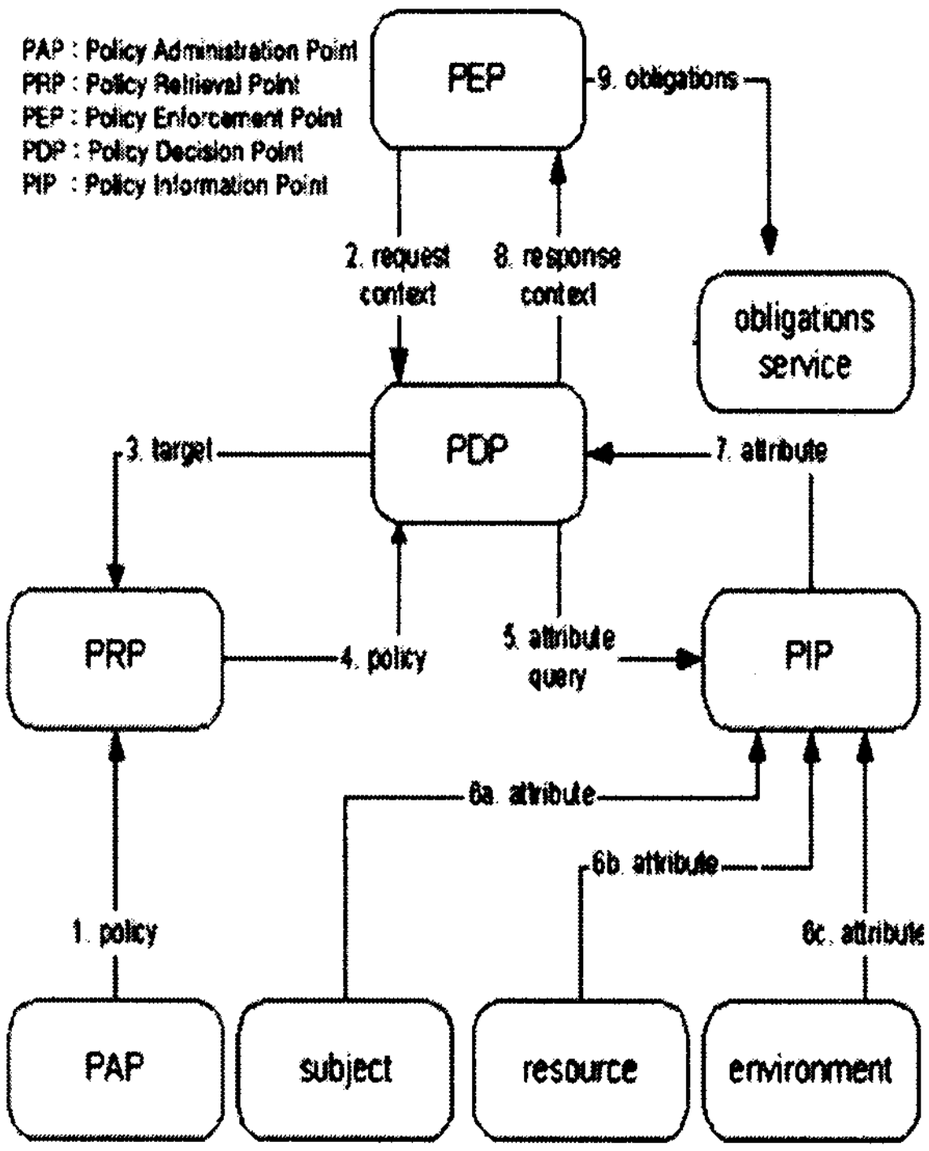
(1) PAP는 policy statements를 만들어서 PRP에서 사용가능 하도록 한다.

(2) PEP가 PDP에게 SAML형식의 인증과 함께 요청을 한다.



[그림 4] 정책 언어 모델

(3) PDP는 PRP로부터 decision request를 통해 policy statement의 위치를 파악하고 검색한다.
(4) PRP는 적절한 policy를 PDP에게 XACML policy statement 혹은 policyset statement 형식으로 반환한다.
(5) PDP 인증 접근 요청과 policy statement을 살펴본다.
(6) PIP는 특정방법을 사용하는 다른 시스템에 의해 attributes를 위치시키고 파악 할 수 있다.
(7) PIP는 PDP로부터 요청받은 SAML의 형식으로 된 attributes를 반환한다.
(8) 만약 policy statement가 TRUE를 반환하면 PDP는 PEP에 "permit" 이라는 decision attribute와 응답 값을 반환한다.
(9) PEP는 obligation을 제출한다.



[그림 5] 데이터 흐름 모델

PDP는 요청을 수신하고 정책에 따라 처리할 수 있도록 프로세스를 실행하여 결과를 접근자에게 돌려주는 역할을 하는 중요한 구성요소이며 obligation은 특정 프로세스 실행 시 요구가 없어도 필수적으로 같이 수행되어야 하는 실행에 대하여 기술한다.

3. XACML의 적용

앞에서 언급한 바와 같이 XACML은 특정 시스템에 적용되도록 제정된 것이 아니다. XML을 활용하는 어떠한 자원들에게 적용되어질 수 있다. 다음은 몇 가지 활용 예를 제시한 것이다.

3.1 온라인 접근제어

온라인 환경에서 사용자나 프로세스는 온라인 서버에 요청을 보낸다. 정책프로세서는 이를 평가하여 접근허가 여부를 응답 해 줄 수 있다. 서버 내의 엘리먼트는 PEP에 의해 접근을 허가 또는 거부한다. Java 애플리게이션, J2EE같은 HTTP상의 어떠한 온라인 애플리케이션도 적용 범주에 들 수 있으며 FTP, POP3와 같은 다른 인터넷 프로토콜에도 적용될 수 있다. 주요 데이터의 흐름은 그림3의 데이터 흐름 모델과 같다. 웹 환경에서는 다양한 목적을 위한 요청이 있을 수 있다. 따라서 다양한 접근 평가 기준이 존재 할 수 있는데, 회사의 구성원에 대한 접근이나 시간에 따른 접근, 날짜에 따른 접근, IP에 따른 접근, 인증정보에 따른 접근 등이 있을 수 있다.

그러나 이러한 접근 제어를 위해 반드시 보안이 전제되어야 하는데 보호되지 않은 통신채널이나 미약한 인증정보를 사용한다면 접근제어에 신뢰성이 떨어진다. 그러므로 SAML, XKMS와 함께 인증과 승인 정보를 전제로 접근평가가 실행되는 것이 제안되고 있다.

3.2 ebXML 등록기/저장소

ebXML의 객체등록 저장소인 등록기/저장소의 접근 제어에 XACML을 적용할 수 있다. 다음과 같이 크게 3가지 용도를 적용시킬 수 있다.

- Restricting Read-Only Access

제출된 레지스트리 오브젝트에 대하여 거래파트너는 읽기만 가능하도록 한다. 레지스트리에 있는 모든 객체들은 UUID(Universally Unique Identifier)번호를 가지고 있고 UUID를 통해 URN의 형식을 확인해야만 한다.

- Write-Access

  객체를 레지스트리에 제출한 제출자는 레지스트리 오브젝트와 연관된 AccessControlPolicy를 제출하도록 한다. 이 AccessControlPolicy는 제출자의 파트너에게 write access를 허가한다. 이 객체 또한 UUID로 구별된다.

- Administrative Use case

  각 객체를 제출한 회사는 그 회사가 제출한 Access control policies의 관리자를 위한 관리자 access control policy를 제출한다[8].

특히 전자상거래를 위한 ebXML레지스트리 접근 제어는 인증과 승인, 보안이 필수적인 구성요소이다. 위의 적용 분야 외에도 DRM, EDI시스템, 금융, 정부행정기관, 의료분야의 리소스관리들에 활용될 수 있을 것이다.

4. 결론 및 향후 연구

XACML은 XML자원의 미세한 접근을 제어하며 접근자의 특징적인 행위에 대한 정책을 수립하고

실행함으로써 효율적인 자원 관리를 할 수 있는 접근제어 표준 기술이다. 본 논문에서는 이 XACML에 대하여 분석하고 그 적용 분야를 제시하였다.

기업들의 독립적인 전자상거래에서 기업 간의 협력에 의한 전자상거래와 데이터 이동으로 XML 데이터는 폭발적으로 증가하고 있으며 이에 따라 리소스의 효율적인 관리는 필수적이다. XACML은 XML로 표현되는 어떠한 객체에도 적용 될 수 있으며 활용분야도 대단히 광범위하다. 웹 서비스와 ebXML[9]에서도 접근제어 표준으로 활용될 전망이다. XACML기술을 바탕으로 XML 리소스의 접근제어 모델을 제시할 수 있는 시스템을 보다 앞서 실현하고 자원의 효율적인 관리를 위한 연구를 지속적으로 해야할 것이다.

5. 참고문헌

[1] XML-Signature Syntax and Processing, http://www.w3.org/TR/xmldsig-core/

[2] XML Encryption WG, http://www.w3.org/Encryption/2001

[3] Security Assertion Markup Language, http://www.oasis-open.org/committees/security/docs/cs-sstc-core-01.pdf

[4] XML Key Management Specification(XKMS), http://www.w3.org/TR/xkms/

[5] OASIS eXtensible Access Control Markup Language TC , http://www.oasis-open.org/committees/xacml/

[6] XML Path Language (XPath), http://www.w3.org/TR/xpath

[7] OASIS eXtensible Access Control Markup Language (XACML), http://www.oasis-open.org/committees/xacml/repository/draft-xacml-schema-policy-15.doc

[8] Use case, http://www.oasis-open.org/committees/xacml/repository/draft-xacml-usecase-01a.pdf

[9] ebXML, http://www.ebxml.org