공동 작업을 지원하는 XML 데이터의 접근 권한 메커니즘

이제희, 박성은, 이용규
동국대학교 컴퓨터공학과
e-mail : bongjava@dongguk.edu

An Authorization Mechanism for XML Data Supporting Cooperative Work

Je Hee Lee, Sung Eun Park, Yong Kyu Lee
Dept. of Computer Engineering, Dongguk University

요 약

최근에 웹 기반의 공동 작업에 대한 연구가 활발히 진행되고 있으며, 웹 표준 언어인 XML 데이터에 대한 접근 제어 및 관리에 대한 필요성이 점차 중요시되고 있다. 이에 접근 제어 표준인 XACML이 제안되었지만, 공동 작업에 대한 정의가 없는 문제가 있다. 본 논문은 이러한 문제를 해결하기 위하여 공동 작업에 관한 기능을 기존의 XACML 스키마에 추가하여 확장하였으며, 이를 통해 기존의 공동 작업을 위한 XML 데이터에서 원하지 않는 권한 모두를 위임하는 경우를 방지하고, 권한의 오·남용을 줄일 수 있게 되었다. 또한 본 논문에서는 이러한 공동 작업을 관리하기 위한 접근 권한 메커니즘을 설계하고 구현한다.

1. 서론

인터넷의 급속한 성장과 네트워크의 발전으로 공유 데이터에 대한 공동 작업이 점차 활발해지고 있다. 이처럼 공동 작업의 중요성이 증가함에 따라 공유 데이터를 작업할 다양한 공동 작업 플랫폼이 개발되고 있으며, 그 중에서도 최근에는 웹 기반의 공동 작업에 대한 연구가 활발히 진행되고 있다.

공동 작업을 위해서는 데이터에 대한 접근 제어 관리가 필요한데, 최근에 XML 데이터의 접근 제어를 위한 접근 제어 정책으로 OASIS(the Organization for the Advancement of Structured Information Standards)에서 XACML(eXtensible Access Control Markup Language)[5]을 제안하였다. 그러나 이는 XML 기술을 사용하여 호환성과 표준성을 최대한으로 살린다는 장점이 있지만, XML 데이터의 공동 작업에 대해서는 명시하지 않아 공동 작업에 대한 접근 제어를 적용하는데 어려움이 있다.

이러한 문제를 해결하고자 본 논문에서는 XACML의 스키마에 공동 작업을 지원하기 위한 권한 수정, 위임, 이양에 관한 기능을 추가하고, XML 데이터의 생성, 추가, 수정, 삭제에 관한 접근 제어 기능을 자세히 기술한다. 그리고 공동 작업을 위해 기능을 추가한 XACML 확장 스키마를 이용하여 공동 작업을 위한 XML 데이터의 권한 관리 메커니즘과 접근 제어 메커니즘을 설계 및 구현한다.

본 논문의 구성은 다음과 같다. 먼저 2장에서는 관련 연구로 공동 작업시스템과 기존의 접근 제어 메커니즘에 대해 소개하고, XML 기반의 접근제어 기술인 XACML을 살펴본다. 3장에서는 공동 작업을 지원하기 위한 XACML의 확장 스키마를 정의하고, 스키마를 기반으로 권한 관리 메커니즘과 접근 제어 메커니즘을 설계한다. 4장에서는 설계한 공동 작업을 위한 권한 관리 메커니즘과 접근 제어 메커니즘 구현에 대해서 설명하고, 5장에서는 결론 및 향후 연구에 대해 기술한다.

2. 관련 연구

본 장에서는 최근에 활발히 진행되고 있는 웹기반의 공동 작업 시스템과 기존의 접근 제어 메커니즘과 XACML에 대한 내용을 소개한다.

2.1 공동 작업 시스템

최근에 웹 기반으로 공동 작업의 효율을 높이기 위한 플랫폼이 소개되고 있으며, 이러한 대표적인 시스템으로는 기존의 유즈넷 서비스에서 제공한 공동작업 기능을 WWW으로 변형한 동기/비동기식 시스템인 HyperNews, 분산된 데이터에 대한 원격 접근을 제공하는 시스템으로 데이터 저장 관리의 기능들을 지원하는 Alliance, 웹을 기반으로 한 사용자들 간의 상호 작용 및 공동 작업을 위해 설계된 시스템인 Mushroom 등이 있다.

2.2 접근 제어 메커니즘

접근 제어 메커니즘으로는 권한 주체와 권한 객체 사이의 권한 관계를 매트릭스로 표현한 접근 제어 매트릭스(Access Control Matrix), 권한 주체에 대한 권한이 부여된 객체들의 리스트로 표현하는 접근 제어 리스트(Access Control List), 그리고 권한 객체에 대해 접근이 허용된 주체들의 리스트로 표현하는 자격 리스트(Capability List) 등이 있다.

2.3 XACML

XACML은 2003년 2월 OASIS에서 표준화한 것으로 XML 문서에 대한 접근을 정책리스트를 사용하여 제어하는 XML 기반 언어이다. 이는 정책 언어와 요청/응답 언어로 구성되어 있으며, 정책 언어는 가장 기본이 되는 규칙(Rule), 여러 규칙들을 포함하는 정책(Policy), 정책들의 집합인 정책집합(PolicySet)으로 구성되고, 요청/응답 언어는 사용자가 특정 자원에 대한 접근을 요청(Request)과 요청한 내용에 대한 결과를 사용자에게 전달하는 응답(Response) 등으로 구성된다.

3. 공동 작업을 지원하는 접근 권한 메커니즘 설계

본 장에서는 공동 작업을 지원하는 XACML 확장 스키마를 정의한다. 또한, 작성한 스키마를 통해 권한 관리 메커니즘과 접근 제어 메커니즘을 설계한다.

3.1 XACML 확장 스키마

3.1.1 정책 확장 스키마

기존의 XACML 정책 스키마는 공동 작업을 위한 데이터의 정책을 정의하는데 복잡하고, 정책에 대한 제약이 많았다. 따라서 본 논문에서 확장한 정책 스키마는 기존의 정책 스키마에 공동 작업을 지원하기 위한 몇 가지 엘리먼트를 추가했으며, 중요 엘리먼트는 다음 [표 1]과 같다.

[표 1] 정책 확장 스키마의 중요 엘리먼트

엘리먼트	설명
Co-workPolicy	최상위 엘리먼트
Resources	공동 작업 데이터 명
Co-Subject	권한 소유자
Co-Action	소유자들의 권한 명
PreviousAction	권한의 위임, 이양 이전의 권한
EntrustedTimeValue	권한의 위임, 이양 적용 날짜
ExpirationTimeValue	권한의 만기 날짜

3.1.2 요청 문맥 확장 스키마

기존의 XACML의 요청 문맥 스키마에서 공동 작업을 지원하기 위한 몇 가지 엘리먼트를 추가했으며, 중요 엘리먼트는 다음 [표 2]와 같다.

[표 2] 요청 문맥 확장 스키마의 중요 엘리먼트

엘리먼트	설명
Request	최상위 엘리먼트
EntrustedSubject	위임 및 이양 요청자
EntrustedTime	위임 기간
PermanentEntrust	영구적인 위임 및 이양
LimitedEntrust	일시적인 위임 및 이양
Resource	공동 작업 데이터 명
Action	요청 행위

3.1.3 응답 문맥 확장 스키마

기존의 XACML의 응답 문맥 스키마에서 공동 작업을 지원하기 위한 몇 가지 엘리먼트를 추가했으며, 중요 엘리먼트는 다음 [표 3]과 같다.

[표 3] 응답 문맥 확장 스키마의 중요 엘리먼트

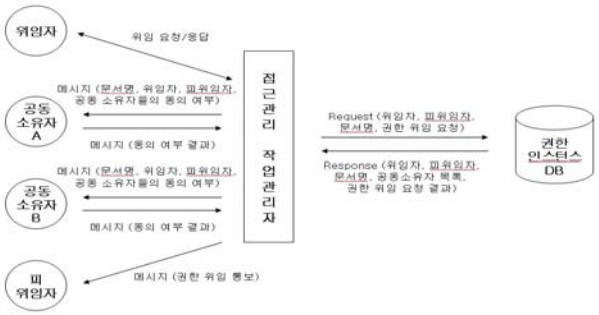
엘리먼트	설명
Response	최상위 엘리먼트
EntrustInfo	위임 및 이양에 대한 정보
AgreementInfo	공동 소유자들의 동의 여부
Result	응답 결과

3.2 권한 관리 메커니즘 설계

3.2.1 권한 관리 메커니즘

권한을 위임받기 위해서 'Manage'의 권한을 가진

사용자들의 동의가 필요하다. 위임은 단기 위임과 영구 위임으로 나눈다. 단기 위임은 일정기간을 정해 그 기간 동안은 위임받은 권한을 사용할 수 있지만, 기간 만료 시에는 권한이 소멸된다. 권한 위임은 메시지를 통해 'Manage'의 권한을 가진 사용자들이 동의를 통해서 이루어진다. [그림 1]은 권한 위임 및 이양에 사용한 메시지 기능에 대한 흐름도이다.

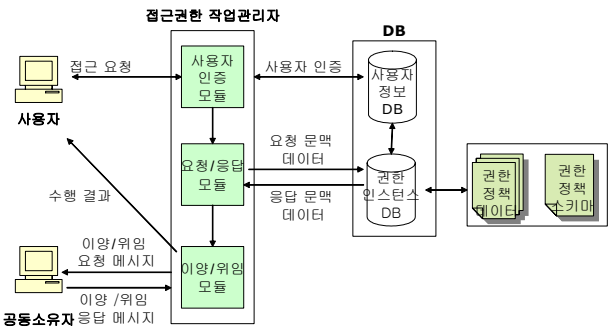


[그림 1] 메시지 기능의 흐름도

권한 이양은 이양자의 권한을 이양 받을 사용자에게 양도하는 기능으로 'Manage'의 권한을 가진 사용자만 사용할 수 있다. 권한 위임과 같이 메시지를 통해 데이터의 'Manage'의 권한을 가진 사용자들의 동의를 얻는다. 여기서 이양을 한 경우에는 기본 권한인 'Read' 권한을 갖는다.

3.2.2 권한 관리 메커니즘에 대한 시스템 설계

'Manage' 권한을 가진 사용자가 요청하는 권한 관리 기능을 접근 권한 관리자가 요청/응답 문맥 스키마를 적용한 XML 문서로 작성한다. 이를 요청/응답 모듈로 전달하게 되고, 요청한 문서의 권한 정보와 비교한다. 요청한 작업이 권한 정보의 범주에 속해 있는 경우에는 요청/응답 모듈은 접근 권한 관리자로 응답 문서를 전달하게 된다. 그리고 동시에 이양/위임 모듈을 통해 작업하려는 XML 데이터의 공동 소유자에게 메시지를 전달한다. [그림 2]는 권한 관리 메커니즘에 대한 시스템 구조도이다.

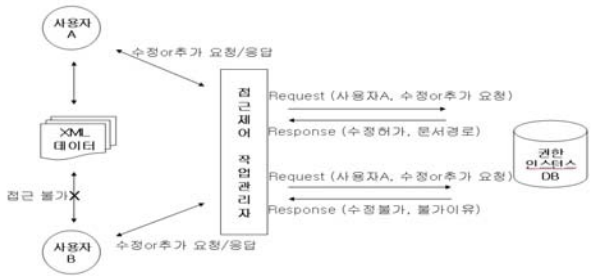


[그림 2] 권한 관리 메커니즘의 시스템 구조도

3.3 접근 제어 메커니즘 설계

3.3.1 접근 제어 메커니즘

데이터를 추가 또는 수정할 때에 실제 저장되어 있는 데이터와 현재 사용자가 작업하려는 데이터와 차이가 발생할 수 있다. 본 논문에서는 이와 같은 데이터의 불일치를 해결하기 위해 데이터의 동시성 제어 기능을 제공한다. [그림 3]은 동시성 제어 기능에 대한 흐름도이다.

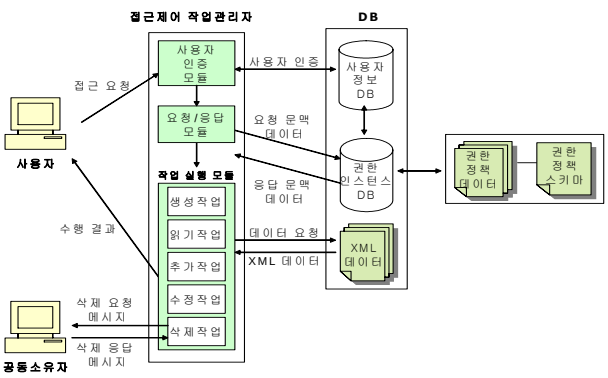


[그림 3] 동시성 제어 기능의 흐름도

데이터의 삭제는 'Manage' 권한을 가진 사용자가 한 명일 경우에는 요청 즉시 처리되지만, 여럿일 경우에는 다른 'Manage' 권한을 가진 사용자의 삭제 동의를 얻어야한다. 삭제 동의는 본 논문에서 제공하는 메시지 기능을 사용하며, 모든 사용자들의 동의를 얻은 후에, 삭제를 수행한다.

3.3.2 접근 제어 메커니즘에 대한 시스템 설계

접근 제어 관리자는 사용자의 요청을 XACML의 요청 문맥 스키마를 적용한 XML 문서로 작성하고, 요청/응답 모듈로 전달한다. 요청한 작업이 권한 정보의 범주에 속해 있는 경우에는 요청/응답 모듈은 접근 제어 관리자로 응답 데이터를 전달한다. 접근 제어 관리자는 사용자에게 요청한 데이터의 내용을 인터페이스로 출력한다. [그림 4]는 접근 제어 메커니즘에 대한 시스템 구조도이다.



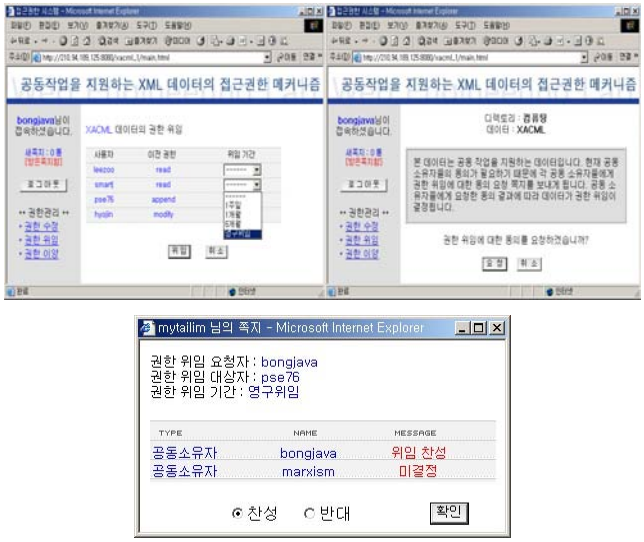
[그림 4] 접근 제어 메커니즘의 시스템 구조도

4. 공동 작업을 지원하는 권한 관리 메커니즘 구현

본 장에서는 앞 절에서 설계한 권한 관리 메커니즘과 접근 제어 메커니즘을 구현한다.

4.1 권한 관리 메커니즘 구현

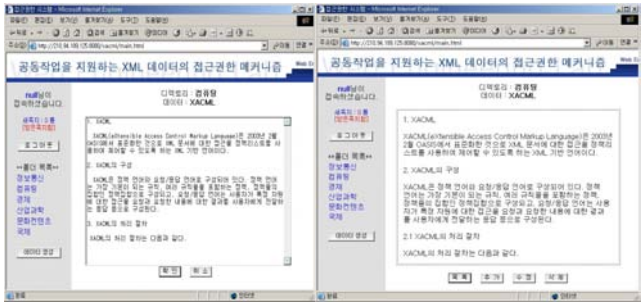
권한 관리 메커니즘은 사용자들의 동의 여부를 물어보는 메시지 기능을 제공한다. [그림 5]는 공동 작업 데이터에 대해서 권한 위임을 하는 화면으로 공동 작업 데이터에 대해서 접근할 수 있는 사용자들의 권한을 나타낸다. 본 화면은 권한이 'Manage'인 경우에만 참여할 수 있다

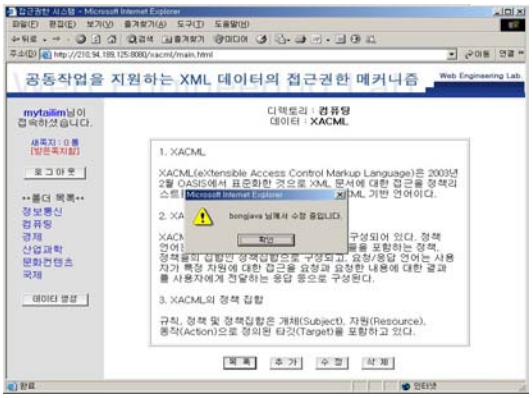


[그림 5] 공동 작업 데이터에 대한 권한 위임 화면

4.2 접근 제어 메커니즘 구현

접근 제어 메커니즘에서는 동시성 제어 기능을 제공한다. [그림 6]은 공동 작업 데이터에 대해서 수정 작업을 하는 화면으로 'Modify' 이상의 권한을 가진 사용자만 수행할 수 있다. 먼저, 데이터베이스에 저장되어 있는 정책 스키마를 기반으로 한 공동 작업 데이터의 권한 인스턴스를 통해 작업할 데이터의 권한 유무를 판별한다. 기존에 수정을 요청한 사용자가 데이터의 수정을 잠금을 설정했기 때문에 타 사용자들의 수정 작업을 차단한다.





[그림 6] 공동 작업 데이터에 대한 수정 작업 화면

5. 결론 및 향후 연구

기존의 XML 데이터의 접근제어 기술인 XACML은 공동 작업에 관한 접근 권한 기능이 명시되어 있지 않고, 권한 이양 및 위임 시에 권한의 오·남용 등의 보안 문제를 갖고 있다.

이러한 문제를 해결하고자 본 논문에서 최근에 표준화된 XML 데이터의 접근제어 기술인 XACML의 기능을 확장하였다. 우선 권한 관리에 관한 기능으로 권한 수정, 위임, 이양에 대해 기술하였고, 접근 제어에 관한 기능으로 공동 작업을 지원하는 XML 데이터의 생성, 추가, 수정, 삭제에 대해 추가하였다. 또한 이러한 기능들을 포함하는 공동 작업을 위한 XML 데이터의 접근 권한 메커니즘을 설계 및 구현하였다.

향후에는 본 논문에서 사용자 인증부분의 부족함을 보완하고자 XML 기반의 인증과 권한 정보 교환에 관한 표준인 SAML(Security Assertion Markup Language)을 공동 작업에 적용하기 위한 기능을 추가할 것이다.

참고문헌

[1] D. A. Black, "Introducing HyperNews : Combining the functions of Usenet and the WWW," Linux Journal, Vol. 1996, No. 10, 1996.
[2] E. Damiani, S. D. C di Vimercati, and S. Paraboschi, P. Samarati, "Controlling access to xml documents," Proc. of the IEEE Internet Computing, Vol.5, No.6, pp.18-28, 2001.
[3] D. Decouchant, M. R. Salcedo, "Alliance: A Structured Cooperative Editor on the Web," http://orgwis.gmd.de/projects/W4G/proceedings/alliance.html, 1996.
[4] T. Kindberg, "Mushroom-A framework for ollaboration and interaction across the Internet," http://orgwis.gmd.de/projects/W4G/proceedings/mushroom.html, 1996.
[5] eXtensible Access Control Markup Language, http://www.oasis-open.org/committees/xacml/repository/draft-xacml-schema-policy-15.doc, 2004.