XML 문서를 위한 인덱스 기반의 명세/속성 기반 접근 제어

최남규°, Van-Trang-Nguyen, 차효성, 구미숙, 황정희, 류근호
충북대학교 데이터베이스 연구실
{cnam9°,nvtrang,kkido,gumisug,jhhwang,khryu}@dblab.chungbuk.ac.kr

Specification / Attribute based access control based on Index for XML Document

Nam Kyu Choi°, Van Trang Nguyen, Cha hyo soung, Gu Mi Sug, Jeong Hee Hwang, Keun Ho Ryu
Database Laboratory, Chungbuk National University

요 약

최근 연구되고 있는 XML 문서를 위한 접근 제어에 관한 연구는 간접적으로 접근 권한을 표현하는 명세 기반 접근 제어 방법과 각 객체에 직접적인 접근 권한을 표현하는 속성 기반 접근 제어 방법으로 구분할 수 있는데, 명세 기반 접근 제어 방법은 공간 효율적이며, 속도 비효율적인 특성을 갖으며, 속성 기반 접근 제어 방법은 속도 효율적이며, 공간 비효율적인 특성을 갖는다. 또한 이러한 연구의 초점은 안전한 접근 제어를 보장하면서, 부가적인 비용 증가를 줄이고자 하지만, 대부분의 연구에서는 인덱스 기법에 기반 하지 않고 문서 전체 또는 일부를 액세스 하므로 탐색 비용 또는 데이터 처리 비용이 증가하고, 특정 기법에 국한 하여 적용하기 때문에 각 기법이 갖는 근본적인 문제점을 해결 할 수 없다. 따라서 이러한 문제점을 해결하기 위해 인덱스 기반의 전역 접근 제어와 지역 접근 제어 메커니즘 제안하고, 이를 기반으로 명세/속성 기반 접근 제어를 연계하여 강제 접근 제어(MAC)의 최소 접근 권한 정책을 지원하는 역할 기반 다중 레벨 접근 제어 모델에 적용하였다.

1. 서 론

XML이 인터넷상의 데이터 표현 및 교환의 실질적인 표준으로 인식되면서 XML에 대한 연구의 중요성이 높아지고 있는 가운데, XML을 기존의 데이터베이스를 활용하여 관리 하거나 또는 기존의 시스템과 통합하고자 하는 연구가 진행되고 있다. 즉, 서로 다른 구조를 갖는 관계형 데이터베이스와 XML의 이질적 구조에 대한 맵핑이나 변환 문제, 그리고 XML 문서의 계층적 구조와 순서화 된 특성을 효율적으로 지원하기 위한 인덱싱 기법에 대한 연구도 함께 이루어지고 있다[1][2]. 이와 더불어 최근 정보 유출의 심각성이 높아지면서 XML문서에 대한 접근 제어에 관한 연구가 부각되고 있다[3][4][5][6][7][8].

XML문서에 대한 접근 제어 방법은 직접적인 접근 표현 또는 간접적인 접근 표현 접근 방식에 따라 각각 저장 공간과 실행 시간 비용의 관점에 따라 상반되는 특성을 갖지만[5], 기존의 연구들은 대부분 두 기법의 연계 또는 통합을 통한 근본적인 문제 해결보다는 한 가지 기법에 편향적인 방법이나 메커니즘을 제시하고 있으며 이러한 연구들의 초점은 안전한 접근 제어 보장과 비용 최소화를 목적으로 하지만, XML 문서를 위한 효율적인 인덱스 구조를 고려하지 않기 때문에 불필요한 탐색은 물론 데이터 증가에 따른 엄청난 탐색 비용의 증가를 직면하고 있다[9].

따라서 이 논문에서는 이러한 기존 연구들의 문제점을 해결하기 위해 인덱스 기반의 전역 접근 제어와 지역 접근 제어 메커니즘 제안하고, 이를 기반으로 명세/속성 기반 접근 제어를 연계하여 강제 접근 제어(MAC)의 최소 접근 권한 정책을 지원하는 역할 기반 다중 레벨 접근 제어 모델에 적용 한다.

이 논문의 구성은 다음과 같다. 2장에서는 XML 인덱스에 대해 설명하고, 3장에서는 명세 기반 접근 제어와 속성 기반 접근 제어의 특성에 대해 살펴본다. 그리고 4장에서는 전역 접근 제어와 지역 접근 제어 메커니즘을 이용한 명세/속성 기반 접근 제어의 연계 방법 및 적용 예에 대해 기술하고, 5장에서 결론을 맺는다.

2. XML 인덱스

XML 문서를 관계형 데이터베이스에 저장하고, XML의 정규 경로 표현 또는 질의를 만족하기 위해서는 XML 각 문서에 대한 경로와 위치정보가 유지되어야 하고, 필요한 자료에 대해 보다 빨리 접근하기 위해서는 탐색영역을 최소화해야 한다[10]. 이 연구에서는 이러한 요구 사항을 충족시키기 위해 XPath (XML Path Language) 원리를 기반하는, [10]에서 제안 되었던 인덱스 구조를 이용하고, 추가적으로 정규 경로 표현 식을 위한 추가적인 XML문서의 계층적 구조 정보를 함께 유지한다.

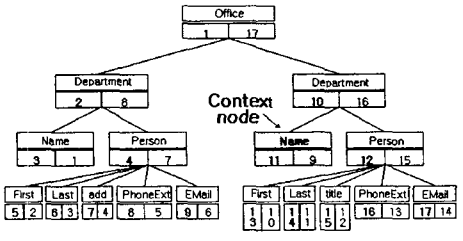

그림 1 XML 인덱스 트리[9][10]

그림1과 같이 탐색 영역 축소를 위한 문서 분할하기 위해서는 XML 문서를 트리로 표현할 preorder과 postorder 번호를 각

노드의 ID로 부여함으로 XML 문서 전체의 순서와 위치를 유지하면서 동시에 부여된 ID의 간단한 비교를 통하여 문서를 4개의 축으로 분할 할 수 있고[10], 추가적인 계층적 구조에 대한 정보를 유지함으로 경로와 위치(position)질의를 요구하는 XML의 표준 경로식 표현을 지원한다.

3. 명세 기반 접근 제어와 속성 기반 접근 제어

3.1 명세 기반 접근 제어

명세 기반 접근 제어는 간접적으로 접근 권한을 명세함으로 접근 권한 또는 정책을 표현하는 방식으로, 접근 제어를 할 대상(target) 파일에 대한 접근 권한에 대한 명시를 정책 파일 또는 규칙 파일을 통해 간접적으로 하고, 사용자가 요구가 발생하면 명시된 부분과 대상 파일을 맵핑 또는 비교를 통해 접근을 제어하기 때문에 미세한 접근 제어의 경우 빈번한 맵핑과 디스크 액세스가 발생하는 단점을 갖지만, 접근 권한에 대한 주체(subject)와 객체(object) 등의 관계 등의 복잡한 접근 제어 정책 또는 규칙에 대해 표현이 가능하다[5][11]

이러한 특징 때문에 이 기법은 수행 시간 비효율적, 저장 공간 효율적 특성을 갖으며[5], 대상 객체와의 매핑의 경우에도 문서 전체를 파싱하거나 DOM등의 API를 통해 적제하기 때문에 수행비용에 대해 더욱 비효율적이다[9].

명세 기반 접근 제어에 대한 연구는 공통의 산업 명세를 만드는 국제적인 컨소시엄인 OASIS의 XACML(extensible Access Control Markup Language) 기술 위원회 중심으로 연구되고 있으며, 이러한 연구는 XACL(extensible Access Control Language)의 기술을 갖은 IBM Tokyo 연구실과 XML의 세부적 접근 제어에 대해 연구를 하고 있는 이탈리아의 Milan 대학을 포함하여, Baltimore Technologies, CrossLogix, Hewlett-Packard, IBM, Jamcracker, Oblix, Reuters, Sun Microsystems와 WebMethod 등의 기업들로 구성 되어 있다[12][13][14].

3.2 속성 기반 접근 제어

속성 기반 접근제어는 각 객체에 직접적인 접근 권한을 표현하는 속성 기반 접근 제어 방식으로, 접근 제어를 할 대상(target) 파일 내의 각 엘리먼트에 접근 권한에 대한 실제 값 또는 표현을 첨가한다. 이러한 특성으로 이 기법은 수행 속도 관점에서는 효율적이며, 저장 공간 관점에서는 비효율적이다. 그러므로 이러한 저장 공간 비효율적 특성을 보완하기 위해 [4][5]연구에서는 수행 시간 비용을 증가시키지 않으면서 저장 공간을 줄이는 연구에 초점을 맞추어, 최소의 노드에 접근 권한을 부여하고 제안된 알고리즘을 이용하여 권한을 상속 또는 전파하는 기법을 제안하였으나, 인덱스에 기반 하지 않았기 때문에, 데이터의 증가에 따른 근본적인 탐색 영역 축소를 통한 탐색 비용에 대한 문제를 해결할 수 없었다. 따라서 [9]에서는 탐색 영역 축소와 필터링을 지원함으로 탐색 비용 문제를 해결하기 위해 인덱스 기반의 접근 제어 맵을 제안하였는데, 구축 방법은 먼저 XML 트리의 표현은 각 엘리먼트 노드에 부여된 preorder과 postorder번호를 좌표로 적용하여 인덱스 맵으로 구성하고[10], 동시에 각 엘리먼트 노드 즉 각 좌표마다 보안 등급 정보를 속성처럼 저장 및 유지함으로 가능케 된다. 즉 인덱스 맵에 인덱스 기반의 접근 제어 맵으로 확장 적용한다.

그림3은 현재노드 (preorder=11, post order=9)를 기준으로 3등급이고, preceding 영역을 질의하는 인덱스 기반의 접근 제어 맵의 예이다.

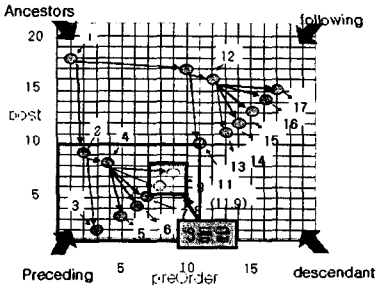

그림 3 인덱스 기반의 접근 제어 맵(Map) [9]

3.3 기존 연구의 문제점

XML 구조를 유지하는 인덱스를 이용하여 각 엘리먼트 또는 데이터 값을 읽지 않고, 최소의 데이터를 이용하여 접근 제어를 할 수 있지만, 많은 연구에서는 인덱스 구조에 기반하지 않고 DOM 등의 API를 통해 문서를 전체 또는 일부를 적제하여 접근 권한 정책을 적용함으로써 연산 비용을 증가 시킨다는 문제점이 있다[14]. 그리고 명세 또는 속성 기반 접근 제어는 각 기법에 따라 공간 또는 시간 효율적 또는 비효율적 특성을 갖지만 기존의 대부분 접근 제어 연구에서는 특정 기법에 국한 하여 적용 가능하다는 문제점이 있다. 따라서 이 논문에서는 이러한 문제점을 해결하고자 인덱스 기반의 명세/속성 기반 접근 제어 연계 메커니즘을 적용한다.

4. 인덱스 기반의 명세 / 속성 기반 접근 제어 연계

4.1 전역 / 지역 접근 제어 메커니즘

XML 인덱스는 탐색 시간 축소뿐만 아니라 최소의 데이터를 이용하여 XML의 계층적 구조를 유지하는 목적을 갖는다. 이러한 인덱스의 원리를 이용하여 [9]에서 제안한 XML 인덱스 접근 제어 트리를 이용하여 각 노드에 preorder과 postorder 값과 접근 권한에 대한 속성 값을 첨부한다. 이러한 원리를 이용하여 속성 기반 접근 제어뿐만 아니라 명세 기반 접근 제어 또한 그림 3 의 좌측 트리와 같이 접근 제어 트리로 구성할 수 있다.

기존의 명세/속성 기반 접근 제어에서 각 기법의 특성에 의해 명세 기반 접근 제어는 간접적인 접근 제어 전략 또는 규칙의 정의에 적합하고, 속성 기반 접근 제어는 각 노드에 직접적으로 미세한 접근 권한 부여에 적합하기 때문에 이 두 기법의 연계를 위해서는 이러한 특성을 이용하여 명세 기반 접근 제어 기법에 기반하여 대상 문서(target)에 대한 대략적 또는 전역적 접근 권한을 정책 파일을 통해 간접적으로 부여하고, 속성 기반 접근 제어 기법에 기반하여 대상 문서에 직접적으로 세부적이고 지역적인 접근

권한을 부여하는 메커니즘을 따른다. 즉 그림 3와 같이 명세 기반의 전역 접근 제어 트리로부터 속성 기반의 지역 접근 제어 트리로 호출한다.

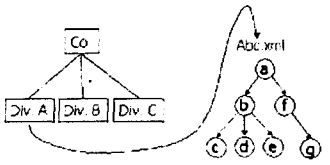

그림3 2단계 접근 제어 모델

4.2 적용 : 역할 기반 다중 레벨 접근 제어

명세 기반의 접근 제어는 정책 기반의 접근 제어를 적용에 적합하고 속성 기반의 접근 제어는 문서의 세부적인 부분에 대한 접근 권한 부여에 적합한데, 이러한 특성을 기반으로 명세/속성 기반 접근 제어 연계 메커니즘을 이용하여 다중 레벨 접근 제어에서 최소 권한 정책을 지원하는 역할 기반 다중 레벨 접근 제어 모델[8][15]을 효율적으로 구현할 수 있는데, 먼저, 역할 기반 정책을 명세 기반 접근 제어 방식으로 표현하고, 두 번째로, 문서에 대한 다중 레벨 접근 제어를 속성 기반 접근 제어 방식으로 표현한다. 그림 4는 위의 모델을 적용한 예인데, 보안 등급이 "2"이고, "role A"를 갖는 사용자가 객체(object) "abc.xml" 문서를 호출 하여(그림 4), 문서의 엘리먼트가 "2등급"으로 설정된 부분에 대해 속성 기반 접근 제어를 적용한다.

```
<?xml version="1.0" encoding="UTF-8"?>
<subject level="2">
  <role name="roleA">
    <object href="roleA/abc.xml"/>
  </role>
</subject>
```

그림 4 역할 기반 다단계 접근 제어

5. 결론

접근 제어 연구의 초점은 안전한 접근 제어를 보장하면서 부가적인 비용 증가를 줄이는데 있지만, 대부분의 연구에서는 근본적인 접근을 통한 문제 해결 보다는 특정 기법에 의존적인 메커니즘에 기반하고 있으므로 각 기법이 갖는 근본적인 문제를 해결하지 못하고 있으며 접근 권한을 부여하기 위해 실제 데이터 전체 또는 일부를 적재하는 방법을 적용함으로써 데이터 처리의 효율성을 저하되었다. 따라서 이 연구에서는 이러한 문제를 해결하기 위한 인덱스 기반의 전역 접근 제어와 지역 접근 제어 메커니즘에 기반한 명세/속성 기반 접근 제어를 연계하고, 이를 역할 기반 다중 레벨 접근 제어 모델에 적용한 예를 보였다.

향후 연구로는 보다 실질적인 검증을 위해서는 실제 접근 제어 모델을 이용한 세부적인 접근 제어 메커니즘의 구현이 요구된다.

참고 문헌

[1] Igor Tatarinov, Stratis D. Viglas, Kevin Beyer,Jayavel Shanmugasundaram, Eugene Shekita, Chun Zhang. Storing and Querying Ordered XML using a Relational Databases System, In SIGMOD Conference, 2002

[2] Quanzhong Li, Bongki Moon, Indexing and Querying XML Data for Regular Path Expressions, VLDB2001

[3] OASIS,"eXtensible Access Control Markup Language (XACML) 1.0", http://www.oasis-open.org/committees/download.php/2406/oasis-xacml-1.0.pdf

[4] SungRan Cho, Sihem Amer-Yahia, Lakes V.S. Lakshmanan, Divesh Srivastava, Optimizing the Secure Evaluation of Twig Queries , VLDB, 2002

[5] Ting Yu, Divesh Srivastava, Lakes V.S. Lakshmanan, H.V. Jagadish, comparessed Accessibility Map: Efficient Access Control for XML, VLDB2002

[6] 반용호,심효영,김종훈, "XML 문서 보호를 위한 접근제어 메커니즘 연구", 정보과학회 2003년 춘계학술대회, 제 30권 제 01호, 2003 . 04

[7]이형석,성백호,차석일,김현희,신동일,신동규,"XML기반 Access Control 기술의 분석과 적용", 제 29권 제 02호, pp.0000~0000, 2002.10

[8]신휴근,이원석,김동규, "XML 문서를 위한 역할 기반 접근 제어, 정보과학회 2003년 춘계학술대회, 제 30권 제 01호, pp. 0000~0000, 2003.04

[9] 최남규, 황정희, 류근호, 박진수, "XML문서를 위한 인덱스기반의 다중 접근 제어", 정보처리 학회 10권 1호, pp1599-1602, 2003.3

[10] Torsten Grust. Accelerating Xpath Location Steps, In SIGMOD Conference, 2002

[11] IBM Tokyo Research Laboratory, "XML Access Control Language: Provisional Authorization for XML Documents.", http://www.trl.ibm.co.jp/projects/xml/xacl/xacl-spec.html

[12] Cover Pages hosted by OASIS, "OASIS Forms Technical Committee to Standardize Security Access Control with XML. Interoperability Consortium to Develop XACML", http://xml.coverpages.org/XACML-PR20010424.html

[13] Cover Pages hosted by OASIS, "XACL *Technology* Reports", http://xml.coverpages.org/xacl.html, May 04, 2001

[14] E.Bertino, S. Castano, and E. Ferrari. Securing XML documents with Author-X. IEEE Internet Computing, 5(3) : pp21-31, 2001

[15] 조준호, 김응모, "다단계 데이터베이스 역할기반 제어 보안 모델", 정보처리학회 2000년 추계학술대회, 제 7권, 제 02호, pp.0113~0116, 2000.10