



## **A Study on Secure Query Processing Technique for Efficient XML Resource Access**

**Sun-Moon Jo<sup>1</sup>, Won-Keun Choi<sup>2</sup>**

*<sup>1</sup>Department of Computer Information Technology Education, Paichai University*

*<sup>2</sup>Department of Information & Communication Engineering, Inha Technical College*

---

### **A B S T R A C T**

With the development of the mobile environment, it has become more common to access dynamic XML data regardless of location and time. As the application areas of XML are gradually expanding, the security issue of XML has become a major concern. XML is an important tool for storing and exchanging data. It also plays an important role in systems and web applications on the Internet. However, XML is just a language, so the security of the application can not be guaranteed. There are also problems such as permission to access resources, authentication, security enhancement and privacy protection. XML should be used to support access because protection can not be guaranteed due to some functions of the data while using the existing access uniquely. As this makes XML data increasingly complex, there is a growing demand for a secure access policy for data. Therefore, it is difficult to apply the existing access policy. The requirements of access in XML need to be integrated with Web technology support, transparency, fine access control, and existing user authorization techniques. In this paper, we propose a secure query processing technique for efficiently accessing large capacity XML data resources. We also analyze the existing problems and present experimental results through practical and important techniques and performance evaluation. Finally, we describe the direction of future research through secure XML access policy.

© 2017 KKITS All rights reserved

---

**KEYWORDS :** Access control, Policy, Security, Mobile computing, XML, XPath

---

**ARTICLE INFO:** Received 29 June 2017, Revised 2 August 2017, Accepted 11 August 2017.

---

---

\*Corresponding author is with the Department of Information & Communication Engineering, Inha Technical College, 100 Inha-ro, Nam-gu, Incheon, 22212,

KOREA.

*E-mail address:* wkchoi@inhate.ac.kr

## 1. 서론

네트워크상에서 정보는 분산되고 공유되기 때문에 권한이 없는 사용자가 정보에 대한 접근, 위조로부터 XML은 안전하지 못하다[1, 2]. 모바일 환경에서 기존의 데이터베이스에서 정보를 사용자에게 접근을 부여하는 것처럼 대용량 XML 데이터를 대상으로 사용자가 XML 데이터의 특정 항목에만 접근하여 이용할 수 있도록 권한을 부여한다. 이를 위해서는 사용자의 접근 권한을 관리할 수 있어야 한다. 사용자가 XML 데이터에 접근할 때 안전한 권한에 따라 제어할 수 있어야 한다. 간단한 방법은 권한에 따라 별도의 문서를 보유하는 것이다. 그러나 이는 기억 장소의 낭비와 문서의 중복으로 데이터 변경의 어려움이 있다[3, 4].

본 연구에서는 대용량 XML 데이터 접근을 위한 안전한 질의 처리 정책을 제안한다. 웹에서 접근 제어는 문서 교환이 빈번할 수 있으므로 상황에 적절히 대처해야 한다. 이것은 데이터에 대한 접근의 명세를 중요하게 만들어 접근 보호 수준의 기술이 필요로 한다[5-7]. 첫 번째는 대용량 XML 데이터는 다양한 정보를 포함하므로 여러 가지 안전한 보호 수준을 지원해야 한다. 어떤 경우에는 여러 데이터에 같은 접근 정책이 적용될 수 있고, 같은 데이터의 부분마다 다른 접근 정책이 적용될 수 있다. 두 번째는 데이터가 항상 사전에 정의된 유형에 맞는 것은 아니다. 정책은 데이터 유형과 관련하여 자세한 내용이 필요하므로 기존의 접근 정책에 의해 다루어지지 않는 상황을 잘 관리해야 한다.

본 논문은 다음과 같이 구성한다. 2장에서는 관련 연구에 관하여 기술한다. 3장에서는 웹 환경에서 대용량 XML 데이터를 위한 효율적이고 안전한 질의 처리 정책 시스템에 관하여 기술한다. 추가로 기존의 연구와 제안하는 정책이 어떤 특징이

있는지를 비교를 통해 기술한다. 끝으로 4장에서 결론을 맺고 향후 연구를 기술한다.

## 2. 관련 연구

본 장에서는 접근 제어를 통한 이전의 질의 처리 연구를 살펴보고 문제점에 대하여 설명한다.

XML의 이점으로 인해 XML은 데이터 교환 및 일반 표현 매체로 자리 잡아 널리 사용되며 웹 서비스를 구축하는 동안 핵심이 되었다. 그러나 이러한 애플리케이션은 특정 레벨에 대한 안전한 요구 사항을 필요로 했지만 XML을 기본으로 사용하는 애플리케이션의 안전을 보장할 수 없는 마크업 언어이다[8]. XACL에서 접근 평가 모듈은 해당 접근 요구에 적합한 정책을 찾고 조건부 실행뿐 아니라 접근 결정을 한다[9, 10]. 이 연구는 XML 데이터 등을 상세하게 속성을 정의할 수 없다. Gabillon에서는 XML 데이터를 트리로 표현하였다[11]. 이 기술은 모든 종류의 노드를 안전하게 보호할 수 없다. 더구나 복사 정책과 충돌 해결 정책은 복잡하다. 흘 필러는 조각 간의 관계를 표현하여 질의 처리를 수행하는 기술을 제시하였다[12]. XFRag는 질의 처리 시간을 개선한 XFPro를 제시하였다[13]. 그러나 부가 정보로 인하여 처리 시간과 메모리 낭비 등의 문제점이 발생 한다. Damiani는 모바일 환경에서 요소를 보호할 수 있는 가능성이 없다 [14]. 더구나 XML 데이터의 접근은 읽기 연산만을 제공한다. 또한 요소에 대한 접근을 거부하는 레이블링 기술을 적용하는 것은 거부된 요소의 하위 요소 역시 접근을 거부하게 된다. 그러므로 데이터의 활용에 한계가 있다. [15, 16]은 공간 사용량 측면에서 다른 레이블링 보다는 좋으나 Dewey 레이블링 방식과 XML 문서의 깊이에 따라서 성능에 문제점이 있다.

### 3. 안전한 질의 처리 정책 설계

#### 3.1 접근 제어 정책(ACP)

본 연구에서 사용할 접근 제어 정책의 요구 사항을 기술한다. 첫째, 웹 사이트를 사용하면 XML 문서를 항상 사용할 수 있어야 한다. 둘째, 접근 제어 동작은 요청자에게 가능한 투명해야 한다. 요청자는 문서의 접근 제어 정책에 의해 숨겨진 메시지를 알 수 없어야 한다. 셋째, 접근 제어는 다른 사용자 권한부여 기법을 쉽게 통합해야 한다. 넷째, 좋은 접근 제어는 문서 집합, 단일 문서, 요소 집합, 단일 요소, 콘텐츠에 이르기까지 다양하고 세밀하게 지원해야 한다. 또한 DTD에 대한 문서의 보장도 지원해야 한다[17].

본 연구에서는 대용량 XML 데이터의 내부 구성 요소 식별을 위해 W3C에서 제안한 XPath를 사용한다[18]. XPath는 문서의 트리 구조상에서 슬래시(/)로 구별하여 요소 이름이나 미리 정의된 함수들의 나열이다. 트리에서 XPath  $l_1/l_2/\dots/l_n$ 은  $l_n$ 이라고 명명된 모든 속성이나 요소를 나타낸다.

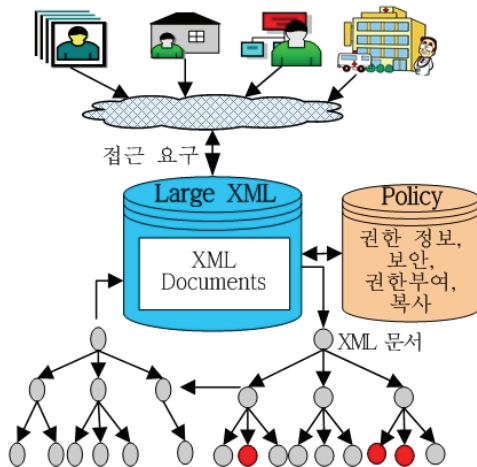


그림 1. 모바일 환경에서 접근 정책  
Figure 1. Access Policy in Mobile Environment

<그림 1>은 제안하는 권한 정보, 보안, 권한부여, 복사 정책에 XML 데이터의 자원 접근 정책의 구조를 설명하고 있다. 권한 정보는 주체가 접근할 수 있는 혹은 접근할 수 없는 객체에 대한 정보이다. 주체는 식별 번호나 요청이 나온 위치를 토대로 언급할 수 있다. 본 연구에서는 주체는 사용자 ID(패스워드), IP 주소, 그리고 접근 목적으로 이루어진 집합을 가진 사용자로 이루어진다. 또한 객체는 접근 제어의 대상이 되는 자원들의 집합을 정의한다. 보안 정책은 접근을 허가하고 거부할 것인가에 대한 원칙을 정의하고 있다. 접근을 허가하는 조건이나 방법을 사용자의 접근 요청의 부분적인 허가나 권한이 없는 데이터의 여과에 대한 내용도 포함하고 있다. 권한부여 정책은 작은 단위의 XML 데이터에 대한 보안의 기술이다. 작은 단위의 권한부여 정책은 사용자나 객체에 대한 권한을 부여할 때 이용된다. 추가로 객체에 관하여 여러 사용자들의 권한 충돌이 발생할 때도 사용된다. 전파 정책은 동일한 요소에 서로 다른 권한이 설정되어 있는 경우에 충돌 시 권한들 사이의 우선순위를 결정하기 위한 방법으로 사용한다. 권한 충돌 우선순위 규칙을 정의한다. 첫째, 가장 자세히 기술한 주체에 권한이 우선순위가 높다. 둘째, 전파에서 발생한 권한보다는 자세히 명시한 권한이 높다. 셋째, DTD에 기술한 권한보다는 직접 XML 문서에 권한이 우선순위가 높다.

<그림 2>는 충돌 해결 정책에 관한 알고리즘이다. AP로부터 aut.dtd와 xml.xas의 교집합 값이 공집합인 경우는 c의 부모의 레이블 정보를 c의 레이블에 설정한다. aut.dtd와 xml.xas의 교집합 값이 공집합이 아닌 경우는 결정 규칙에 동일한 모드에서 충돌이 발생한 경우는 충돌 해결 우선순위를 이용한다. ap에 존재하는 ap.aut.dtd와 ap.xml.xas의 교집합 값이 공집합인 경우는 미리 정해진 접근 권한 값을 설정한다. default()는 기본 접근 문서만

제공한다.

```

입력: DOM Tree, RQ: User_requester,
      AP: Authorization Policy
출력: DOM Tree
for each c ∈ children(T.root) do
  if c.parent.type in(L, R, LDH, LD) then
    /* L: 권한부여, R: 재귀 권한부여, LDH: 로컬
      하드 권한부여, LD: 스키마 수준에서 상세 */
    if Aut.dtd ∩ xml.xas == ∅ then
      /* xas(xml access sheet) */
      c.label←c.parent.label
    else
      c.label←decision_rule
        (c.p.label, ap.auth.dtd, ap.xml.xas)
    fi
  else if ap.aut.dtd ∩ ap.xml.xas == ∅ then
    c.label←default()
  else
    c.label←decision_rule(ap.auth.dtd, ap.xml.xas)
  fi
fi od
    
```

그림 2. 충돌 해결 알고리즘  
Figure 2. Conflict Resolution Algorithm

### 3.2 성능 평가

본 연구에서는 대용량 XML에 대한 안전한 질의 처리 정책에 대해서 몇 가지 제안을 하였다. 기존의 연구(HADA)와 제안한 ACP의 주요 기능에 관하여 비교하였다. 비교의 기준은 대용량 XML 데이터의 보안 요구사항의 만족여부와 접근 주체, 주체 단위, 접근 객체, 권한 방식이다. 제안된 ACP는 아주 작은 단위 접근 정책을 대상 문서에 대한 접근 가능 영역을 요소 단위로 정의함으로써 작은 단위로 지원한다. 기존에 연구에서 가지는 공통적인 단점은 XML 데이터에 대한 접근 수행 주체를 개별 사용자로 이용하고 있다. 사용자와 접근 대상 객체의 관계를 HADA에서는 1대 1의 접근은 가능하지만 대규모의 사용자 또는 대용량 데이터와 이를 따르는 인스턴스 문서를 가지는 환경에서는 적용이 불가능하다.

본 연구에서 시뮬레이션은 다음과 같은 환경에서 수행되었다. Intel Core(TM)2 Duo 3.0GHz CPU, 8GB 메모리, Windows 7 운영 체제이고 Java 1.8.0을 이용하였다. 성능 평가는 HADA와 ACP에 대하여 XML 데이터 접근을 비교하였다. XMark 벤치마크 프로젝트[19, 20]로부터 DTD와 XML 데이터를 이용하여 질의 처리를 실행하여 시간의 차이를 비교하였다.

Query	XPath[18]
Q1	/site/people/person/homepage
Q2	/site/increase
Q3	/site/people/person/phone
Q4	/site/emailaddress
Q5	/site/people/person/education

그림 3. 질의 예  
Figure 3. Query Example

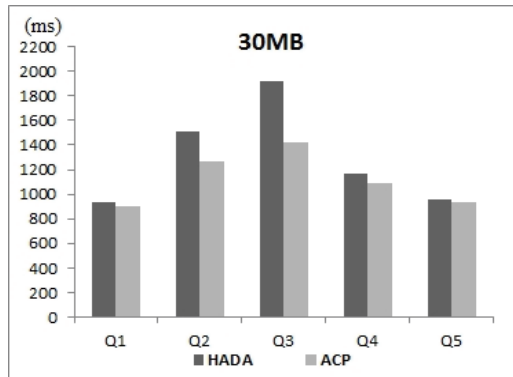


그림 4. 처리 시간  
Figure 4. Processing Time

본 실험에서는 질의 처리 시간을 측정하였다. 데이터양은 30MB으로 질의는 5가지 유형으로 그림 3에 기술하였다. <그림 4>는 질의 처리에 걸린 시간을 나타낸 그래프이다. 실험 결과를 보면 ACP와 HADA는 Q1, Q4, Q5는 비슷하고 Q2, Q3 질의 처리 시간 대해서는 성능 차이를 보이고 있다. 데이터양

이 크기가 커지면 쿼리 시간도 늘어난다.

#### 4. 결 론

본 연구에서는 대용량 XML 접근을 위한 안전한 자원 질의 처리 정책을 제안하고 효율적인 문서 관리를 위한 권한부여와 알고리즘을 기술하여 실험을 실시하였다. 최근 XML 문서들은 수천 수백만 개의 원소들을 포함하고 있는 경우가 많이 있다. XML을 사용하는 가장 큰 이점은 미세하게 문서의 요소 및 속성 수준으로 동일한 문서의 다른 부분에 적용될 수 있다. 본 연구에서 정책은 일반적인 사용자나 객체에 대한 권한을 부여한다. 동일한 객체에 대한 여러 주체들의 권한 충돌이 발생할 때도 활용된다. 기존의 제시된 연구는 XML 데이터 고유의 접근 모드를 제공하지 않는다. 본 연구는 모바일 환경에서 브라우징과 사용자를 위한 효율적이고 안전한 접근 제어 정책을 제공하였다. 이를 바탕으로 관리자는 사용자가 요소에 있는 특정한 정보를 읽거나, 요소 링크를 추가 및 수정, 삭제할 권한을 부여받는다. 향후 연구는 대용량 XML 데이터를 이용하여 여러 응용 프로그램에 적용하는 연구가 더욱 필요하다.

#### References

[1] S. Mohan, A. Sengupta, and Y. Wu, *A framework for access control for xml*, ACM Journal, Vol. 5. No. N, pp. 1-38, 2006.

[2] K. Y. Chung, *Recent trends on convergence and ubiquitous computing*. Personal and Ubiquitous Computing, doi:10.1007/s00779-013-0743-2, 2013.

[3] R. S. Sandhu, E. J. Coyne, H. L. Feinstein, and C. E. Youman, *Role-based access*

*control models*, IEEE Computer, Vol. 29, No. 2. pp. 38-47, 1996.

[4] R. Wonohoesodo, and Z. Tari, *A role based access control for web services*, Services Computing, Proceedings, IEEE International Conference, pp. 49-56. 2004.

[5] L. Li, Y. Z. He, and D. G. Feng, *A fine-grained mandatory access control model for xml documents*, Journal of Software, vol. 10, 2004.

[6] Z. M. Wang, and D. W. Cui, *Access control strategy based on RBAC for xml security*, Computer Engineering and Applications, vol. 43, No. 17, 2007.

[7] S. D. Vimercati<sup>1</sup>, S. Foresti<sup>1</sup>, and S. Paraboschi, *Access control models for xml*, <http://www.springerlink.com/content/j8353g682562qk1k/fulltext.pdf>, 2007.

[8] A. D. Algarin, T. B. Ziminski, and S. A. Demurjian, *Generating XACML enforcement policies for role-based access control of xml documents*, Web Information Systems and Technologies. Springer Berlin Heidelberg, pp. 21-36, 2014.

[9] M. Kudo, and S. Hada, *XML document security based on provisional authorization*, Proceedings of the 7<sup>th</sup> ACM conference on Computer and communications security, Athens, Greece, pp. 87-96, 2000.

[10] S. Hada, and M. Kudo, *XML access control language: provisional authorization for xml documents*, <http://www.trl.ibm.com/projects/xml/xss4j/docs/xacl-spec>, pp. 1-28, 2002.

[11] A. Gabillon, and E. Bruno, *Regulating access to xml documents*, In Proceedings of the Fifteenth Annual IFIP WG 11.3 Working Conference on Database Security, 2001.

[12] S. Bose, and L. Fegaras, *XFrag: A query*

*processing framework for fragmented xml data*, WebDB, pp. 97-102, 2005.

- [13] H. Huo, G. Wang, X. Hui, R. Zhou, B. Ning, and C. Xiao, *Efficient query processing for streamed xml fragments*, Lecture Notes in Computer Science(LNCS) 3882, DASFAA, pp. 468-482, 2006.
- [14] E. Damiani, S. Vimercati, S. Paraboschi, and P. Samarati, *Design and implementation of an access control processor for xml documents*, In proceedings of the 9th International WWW Conference, Amsterdam, pp. 59-75, 2002.
- [15] D-H. Sun, and S-C. Hwang, *A labeling methods for keyword search over large xml documents*, Journal of The Korean Institute of Information Scientists and Engineers, Vol. 41, No. 9, pp. 699-706, 2014.
- [16] G. Qadah, *Indexing techniques for processing generalized xml documents*, Computer Standards & Interfaces, Vol. 49, pp. 34-43, 2016.
- [17] L. Sun, and H. Wang, *A purpose-based access control in native xml databases*, Concurrency and Computation: Practice & Experience, Vol. 24, No. 10, pp. 1154-1166, 2012.
- [18] World Wide Web Consortium(W3C), *XML path language(XPath) 2.0*, Available at <http://www.w3.org/TR/xpath20>, 2003.
- [19] The XML benchmark project, Available form: <http://www.xml-benchmark.org>. Jan. 2017.
- [20] A. Schmidt, and F. Waas, *XMark: a benchmark for xml data managemen*, Proceedi ngs of the 28th VLDB Conference, 2004.

---

## 효율적인 XML 자원 접근을 위한 안전한 질의 처리 기법에 관한 연구

조선문<sup>1</sup>, 최원근<sup>2</sup>

<sup>1</sup>배재대학교 교양학부(IT)

<sup>2</sup>인하공업전문대학 정보통신과

---

### 요 약

XML의 적용 영역이 점차 확대되면서 XML의 보안 문제가 주요 관심사가 되었다. XML은 데이터 저장 및 교환에 중요한 도구이다. 그러나 XML은 단지 언어 일뿐이므로 응용 프로그램의 보안을 보장할 수 없다. 또한 자원들을 접근하기 위한 권한의 허가, 인증, 보안의 강화와 사생활 보호와 같은 문제들이 발생한다. 데이터의 일부 기능으로 인해 기존 접근을 고유하게 사용하는 동안 보호가 보장될 수 없으므로 XML을 사용하여 접근을 지원해야 한다. 최근 XML 문서들은 수천 수백만 개의 원소들을 포함하고 있다. 이로 인하여 XML 데이터가 점차 복잡해지면서 데이터에 관한 안전한 접근 정책에 대한 요구가 증가하고 있다. 그러므로 기존의 접근 정책을 적용하기에는 어려운 점이 있다. XML에서 접근의 요구 사항은 웹 기술 지원, 호환성, 투명성, 미세한 접근 제어, 기존 사용자 권한부여 기법과 통합이 필요하다. 본 논문에서는 효율적인 대용량 XML 데이터 자원 접근을 위한 안전한 질의 처리 기법을 제안한다. 기존의 문제점을 분석하여 실제적이고 중요한 기법과 성능 평가를 통하여 실험 결과도 제시한다.

---



**Sun-Moon Jo** received the M.S., and Ph.D. degrees in the Department of Computer Information Engineering from Inha University in 2002 and 2007, respectively.

He is currently a professor in the Department of Computer Information Technology Education, Paichai University. His research interests include XML, Security, Knowledge System, Healthcare,

Deep learning, and Recommendation. He is an editorial board member of several International Journals. Also, He is a life member of the KKITS.

*E-mail address:* sunmoon@pcu.ac.kr



**Won-Keun Choi** received the bachelor's degree in the Department of Electronic Engineering from the Ajou University in 1982. He received the M.S. degree and the Ph.D. degree in the Department of Electronic Engineering from Korea University in 1986 and 1999, respectively. From 1986 to 1991, he was a researcher at LG Information & Communication Network Lab. He is a professor in the Department of Information & Communication Engineering at Inha Technical College from 1991 to Now. His current research interests include High Speed Network, QoS, Protocols. He is a life member of the KICS, IEEK, KITS.

*E-mail address:* wkchoi@inhac.ac.kr