ACXESS - Access Control for XML with Enhanced Security Specifications

Sriram Mohan,Jonathan Klinginsmith
Department of Computer Science
Indiana University

Arijit Sengupta
Raj Soin College of Business
Wright State University

Yuqing Wu
School of Informatics
Indiana University

Abstract

We present **ACXESS** *(Access Control for XML with En-hanced Security Specifications), a system for specifying and enforcing enhanced security constraints on XML via virtual "security views" and query rewrites.* **ACXESS** *is the first system that bears the capability to specify and enforce com-plicated security policies on both subtrees and structural relationships.*

1 Introduction

Research on XML has mainly attempted to provide effi-cient storage and query processing techniques. Similar to most data management systems, securing data or in other words, making certain data invisible, is as important as (if not more than) making the data available in an efficient manner. Given the semi-structured nature of XML data, sensitive information is contained not just in the data val-ues themselves, but also in the tree structure. Any access control language for XML should provide the DBA with the ability to control access to both data as well as to struc-ture. None of the existing techniques support access control on structure without actually generating and materializing the "views". This approach is non-realistic given that the data may constantly change and that usually there are mul-tiple security levels in a system with each level containing at least one security view.

2 Our Contributions

ACXESS [2] provides an infrastructure for access control on XML documents by specifying access constraints in the form of virtual security views (an approach also used in [1]) and enforcing the access constraints via query rewrites. The main contributions of our work can be summarized as fol-lows:

- We introduce an algebraic security view specification language SSX, by adopting and modifying a graph editing language, to enable conditional hiding and re-organizing XML elements/subtrees.

- We propose SAS - an annotated schema to represent the security constraints internally.

- We propose SQR, a rule-based secure query rewrite algorithm for enforcing the security constraints, using only the information in the SAS.

- We conduct extensive experimental evaluation on var-ious benchmark databases and prove that our approach is both effective and efficient.

A complete discussion of SSX, SAS and query rewrite(SQR) in **ACXESS** is available at [3].

3 Demonstration Proposal

We will demonstrate **ACXESS** focusing on the three ma-jor components: security view specification, security con-straint representation and security constraint enforcement - via query rewrites.

- **Security View Specification:** Besides SSX, we will also demonstrate a graphical interface that assists the DBA in identifying the entities on which security con-straints are to be specified and to rearrange the schema using augmented graph editing operations.

- **Security Constraint Representation:** The specifica-tion tool will visually present the SAS associated with a security view. The DBA can use the SAS (and the se-curity view) to identify problems in their security pol-icy and detect and prevent information leakage.

- **Security Constraint Enforcement Via Reformula-tion:** Users can enter an XPath query which is rewrit-ten based on the user groups and then evaluated. The demonstration will display the rewritten XQuery ex-pression and the XML fragment obtained by evaluat-ing the rewritten XQuery expression.

References

[1] W. Fan, C.-Y. Chan, and M. Garofalakis. Secure XML query-ing with security views. In *SIGMOD*, 2004.
[2] S. Mohan, A. Sengupta, and Y. Wu. Access control for xml - a dynamic query rewriting approach. In *CIKM*, 2005.
[3] S.Mohan, A.Sengupta, Y.Wu, and J.Klinginsmith. Access control for XML, at http://www.cs.indiana.edu/~acxess/.