

# Supporting XML Security Models using RDBMS: A Vision



Dongwon Lee  
Wang-Chien Lee  
Peng Liu

Penn State University



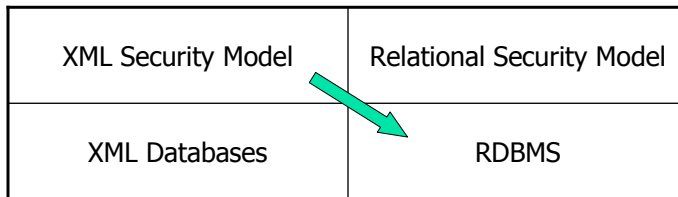
## Outline



- *Motivation*
- Related Work
- Framework and Issues
- Conclusion

# Motivation

- Needs for secure exchange and evaluation of XML data increase
- Still majority of XML data/documents are originally from RDBMS
- RDBMS has solid support for security already
- Many recent works re-invent the wheels
  - New XML Security Models, but
  - Since original data are from RDBMS, and RDBMS has a good support for security model, why don't we use it?



Dongwon Lee

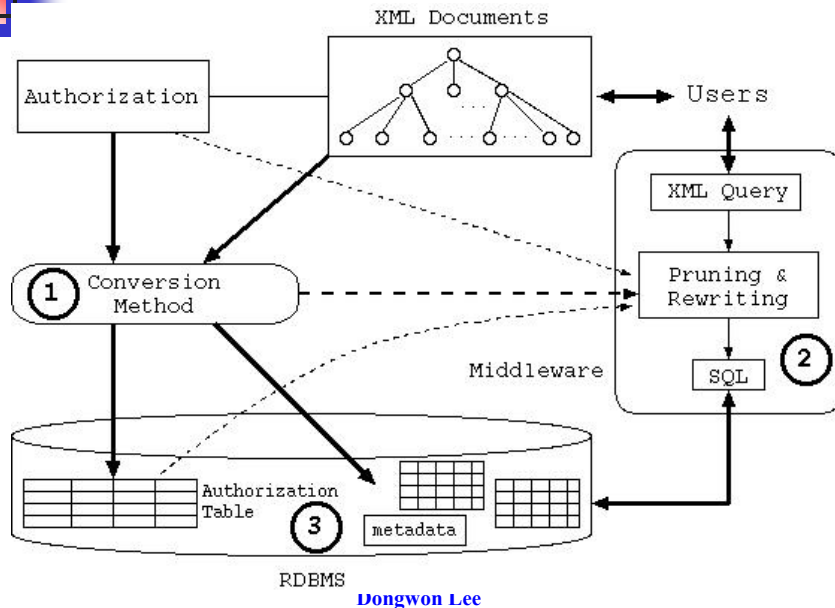
# Overview of Proposal

- XML data in RDBMS
  - Either XML documents are converted into RDBMS, or
  - They are originally stored there
- Security Admin specifies access controls in XML security model
- Users issue XML queries given XML view/schema
- Security check and query evaluation are done in RDBMS or Middleware atop RDBMS, not in XML side
- **Valid** and **secure** answers are returned to users

Dongwon Lee



# Architecture



# Outline

- Motivation
- *Related Work*
- Framework and Issues
- Conclusion



## Related Work I: Security Models

- Relational security model: Multilevel, Discretionary, etc
- Most RDBMS implements discretionary model
  - GRANT / REVOKE
  - Table or column level authorization
  - Views for indirectly supporting contents-based access control
  - Role-based access control
- XML security model: several proposed recently, no consensus or standard yet – active research area
  - We pick one by Samarati et al [TISSEC 02]
- No XML databases fully support the proposed XML security model – only research prototypes

Dongwon Lee



## Samarati's XML Security Model

- A Fine-Grained Access Control System for XML Documents
 

**Role**

**XML nodes**
- Model: 5-tuple (subject, object, action, sign, type)
- Users submit an XML query  $Q$  about an XML document  $D$
- DOM tree  $T$  is built from  $D$
- Access-denied nodes (based on the pre-defined policies) are removed from  $T$ , yielding to a refined DOM tree  $S$  (i.e., view)
- $Q$  is processed against  $S$  and answers are returned to users

Dongwon Lee



## Related Work II: Conversion

- See Sekar's Survey this morning [XSymp03]
- Conversion between XML documents and Relational data
  - Active research area
- Structure-based; use XML schema for conversion
  - STORED [SIGMOD 98], Inlining [VLDB 99], ...
- Data-based
  - Node/Edge [Data Eng. Bulletin 99], XRel [TOIT 01], ...
- We pick the [XRel](#) [TOIT 01]

Dongwon Lee



## XRel's Path-based Conversion

- View XML documents as a set of Paths
- Map such paths onto several tables in RDBMS
- Node information is captured via Root-to-leaf path
- Capture ancestor-descendent relationship via Region (ie, ordering scheme)

[Element\(docID, pathID, start, end, index, reindex\)](#)

[Attribute\(docID, pathID, start, end, value\)](#)

[Text\(docID, pathID, start, end, value\)](#)

[Path\(pathID, pathexp\).](#)

Dongwon Lee



## Related Work

---

- We use
  - XML security model – [Samarati's Model](#)
  - XML-RDBMS conversion method - [XRel](#)
- Our choice made at this point is arbitrary
- Finding which particular model or conversion methods are the best is one of the research issues

Dongwon Lee

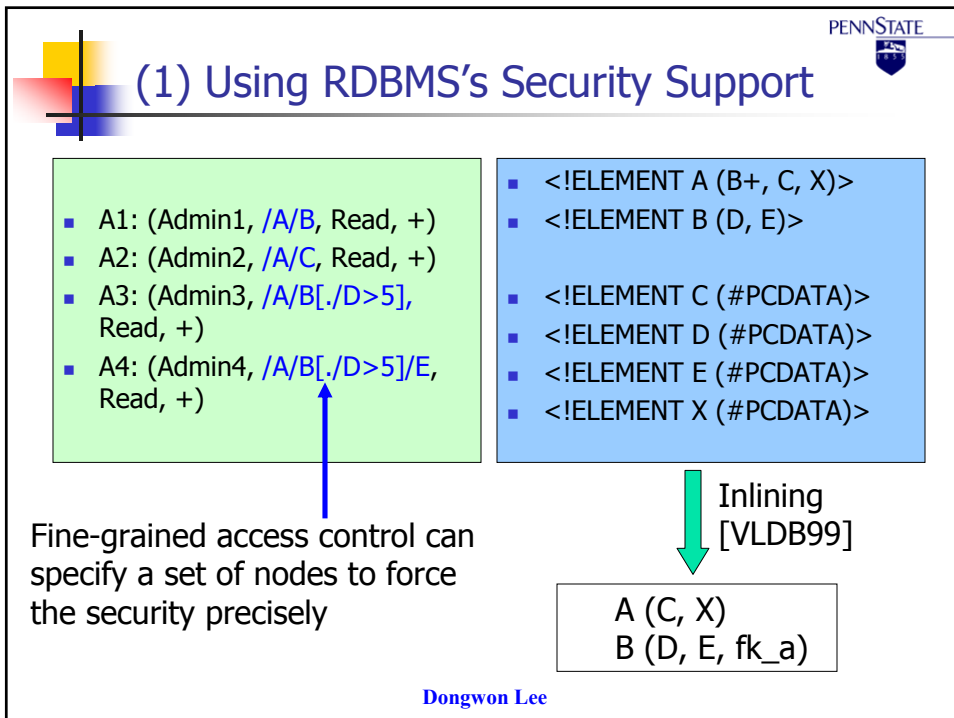
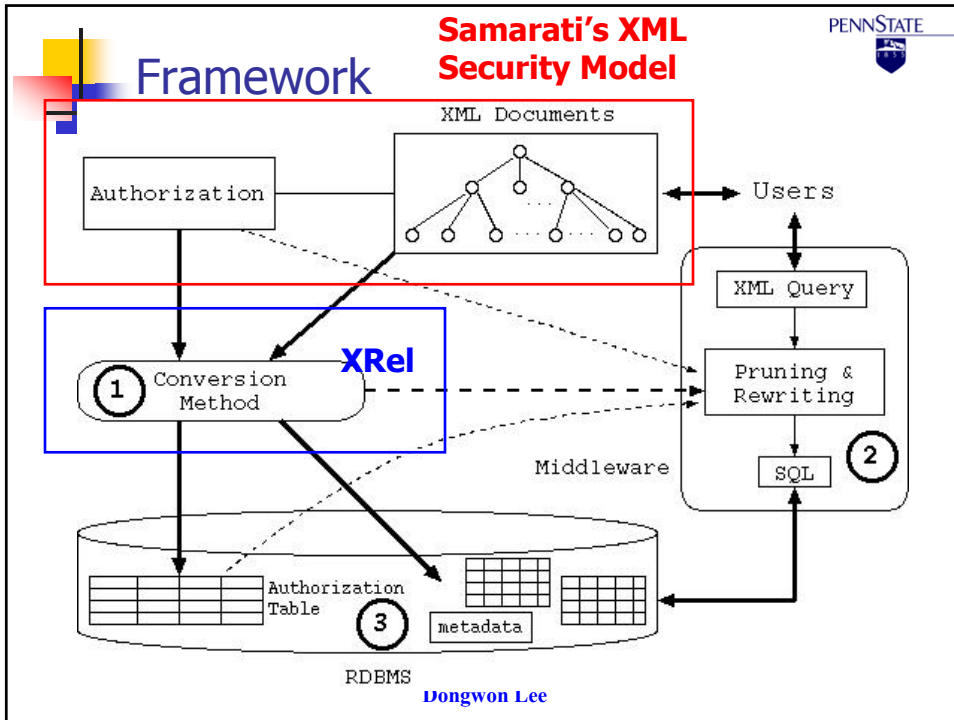


## Outline

---

- Motivation
- Related Work
- *Framework and Issues*
- Conclusion

Dongwon Lee



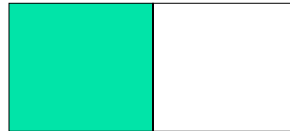
# (1) Using RDBMS's Security Support

**A1:/A/B**



**B(D,E,fk\_a)**

**A2:/A/C**



**A(C,X)**

**GRANT SELECT to  
USER Admin1 ON B**

**GRANT SELECT to  
USER Admin2 ON A(C)**

# (1) Using RDBMS's Security Support

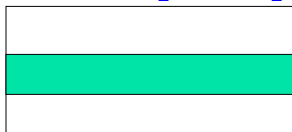
~~**GRANT SELECT to  
USER Admin3 ON B**~~



**CREATE VIEW tmp AS  
SELECT \* FROM B  
WHERE D>5;**

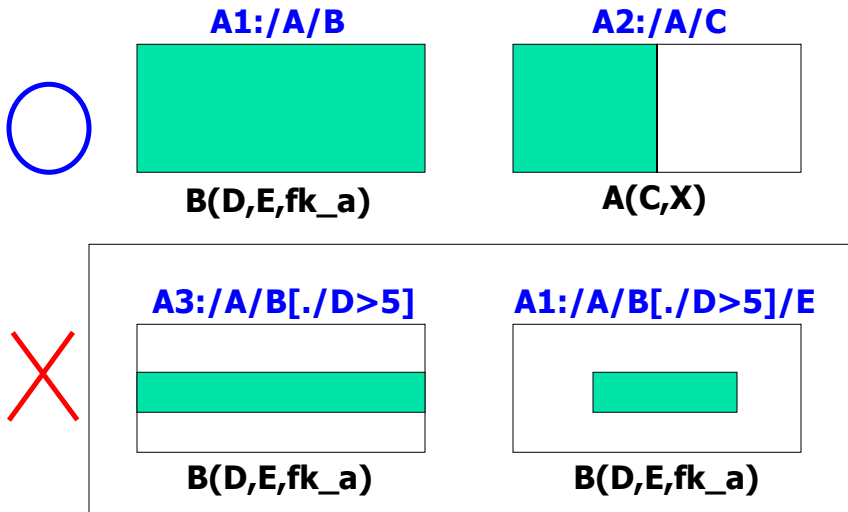
**GRANT SELECT to  
USER Admin3 on tmp;**

**A3:/A/B[./D>5]**



**B(D,E,fk\_a)**

# (1) Using RDBMS's Security Support



Dongwon Lee

# (1) Using RDBMS's Security Support

- Issue: **Granularity discrepancy** between XML and relational security models
- Issue: **Model-to-model mapping** (eg, expressive power, etc)
  - More theoretical study is needed

Dongwon Lee



## (2) Middleware Approach

- A underlying RDBMS is used as a simple storage
  - Its security support may or may not be used
  
- A middleware atop RDBMS handles security check via Query-Rewriting
  - Incoming queries from users are XML format
  - XML access controls are specified via XML queries too
  - Therefore, one can view the access control as additional query constraint over the incoming query

Dongwon Lee



## (2) Middleware Approach

- Query  $Q$ , Access control rule  $R$
  
- $Q+R \Rightarrow Q'$
- Answers that satisfy  $Q'$  are:
  - **Secure** w.r.t  $R$
  - **Valid** w.r.t  $Q$

Dongwon Lee



## (2) Middleware Approach

- XML security authorization table:
  - R1: (s1, /a/b, read, +, Recursive)
  - R2: (s1, /a/d, read, +, Recursive)
  
- Query Q: /a//c
  
- Q': /a/ [b | d] // c

Dongwon Lee



## (2) Middleware Approach

- XML security authorization table:
  - R1: (s1, /a/b, read, +, Recursive)
  - R2: (s1, /a/d, read, --, Recursive)
  
- Query Q: /a//c
  
- Q': /a/ b // c

Dongwon Lee



## (2) Middleware Approach

- XML security authorization table:
  - R1: (s1, /a/b, read, --, Recursive)
  - R2: (s1, /a/d, read, --, Recursive)
  
- Query Q: /a//c
  
- Q': /a//c - (/a/b//c union /a/d//c)

Dongwon Lee



## (2) Middleware Approach

- Issues...
  
- How to rewrite Q to Q'?
  - Which access control rule R to use?
  - How to quickly find?
  - Optimization issue for Q'
  - Security-specific features' effect? (eg, recursive vs. local)
  - ...

Dongwon Lee



# Outline

---

- Motivation
- Related Work
- Framework and Issues
- Conclusion

Dongwon Lee



# Conclusion

---

- L<sup>3</sup> project
  - <http://nike.psu.edu/l3/>
- Preliminary thoughts to support XML security models using RDBMS
  - Many approaches
  - Many issues
  - More details in the paper
- Hope to have more researchers interested in the topic

Dongwon Lee



# Placeholders

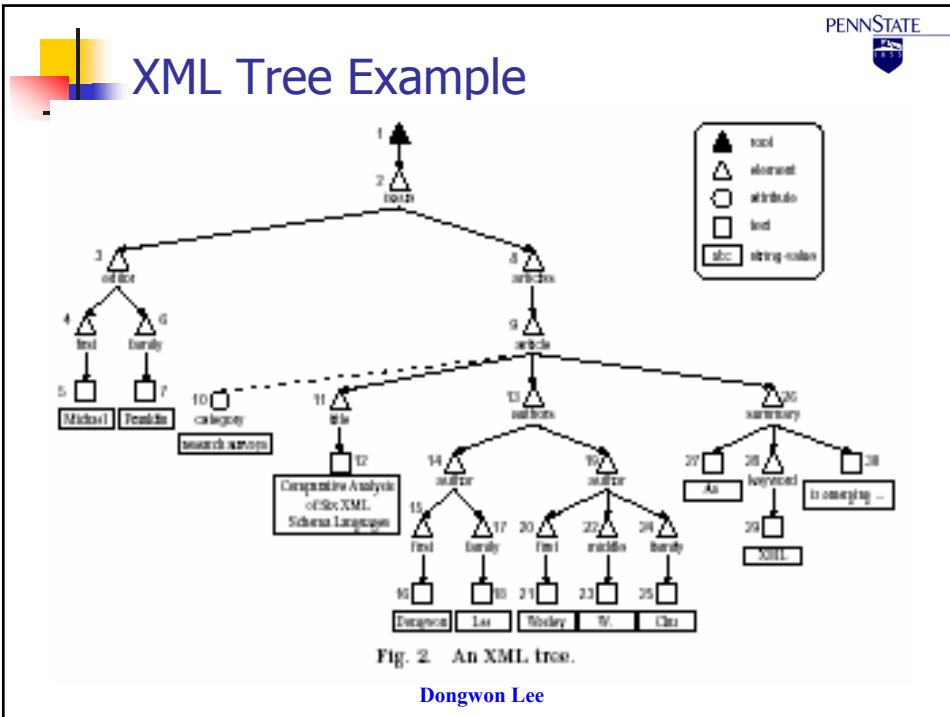
Dongwon Lee



# Samarati's XML Security Model II

- Def: 5-tuple (subject, object, action, sign, type), where:
  - **Subject:** to whom the authorization is granted
  - **Object:** nodes (returned by URI:XPath) to which the authorization is applied
  - **Action:** read (select) or write (insert/delete/update)
  - **Sign:** {+,-}, where + (access granted) and - (access forbidden)
  - **Type:** {LDH, RDH, L, R, LD, RD, LS, RS}; i.e., local, recursive, ...

Dongwon Lee



PENNSTATE

# Tables

Element						NodeID
docID	pathID	start	end	index	retindex	
1	1	0	729	1	1	2
1	2	7	70	1	1	3
1	3	15	36	1	1	4
1	4	37	61	1	1	6
1	5	71	721	1	1	8
1	6	81	710	1	1	9
1	8	118	180	1	1	11
1	9	181	335	1	1	13
1	10	190	248	1	2	14
1	11	198	219	1	1	15
1	12	220	239	1	1	17
1	10	249	325	2	1	19
1	11	257	277	1	1	20
1	13	278	296	1	1	22
1	12	297	316	1	1	24
1	14	336	700	1	1	26
1	15	348	369	1	1	28

Attribute						NodeID
docID	pathID	start	end	value		
1	7	82	82	research surveys		10

Text						NodeID
docID	pathID	start	end	value		
1	3	22	28	Michael		5
1	4	45	52	Franklin		7
1	8	125	172	Comparative Analysis ...		12
1	11	205	211	Dongwon		16
1	12	228	230	Lee		18
1	11	264	269	Wesley		21
1	13	286	287	W.		23
1	12	305	307	Chiu		25
1	14	345	347	As		27
1	15	357	359	XML		29
1	14	370	690	is emerging as the ...		30

Path	
pathID	pathexp
1	#/issue
2	#/issue/editor
3	#/issue/editor/first
4	#/issue/editor/family
5	#/issue/articles
6	#/issue/articles/article
7	#/issue/articles/article/@category
8	#/issue/articles/article/title
9	#/issue/articles/article/authors
10	#/issue/articles/article/authors/author
11	#/issue/articles/article/authors/author/first
12	#/issue/articles/article/authors/author/family
13	#/issue/articles/article/authors/author/middle
14	#/issue/articles/article/summary
15	#/issue/articles/article/summary/keyword

Dongwon Lee