Intelligent Way of Secure and Privacy Preserving Information Brokering

Ms. Poonam Bhise
Scholar M.E.
Department of Computer Engineering
SKN-Sinhgad Institute of Technology Science,
Lonavala, India
poonambhise@yahoo.com

Prof. Vikas Thombre
HOD of Computer Engineering
Department of Computer Engineering
SKN-Sinhgad Institute of Technology Science,
Lonavala, India

Prof. Swati Jaiswal
Assistant Professor
Department of Computer Engineering
SKN-Sinhgad Institute of Technology Science,
Lonavala, India

Abstract:- In recently large amount of information are collected in multiple organizations like health care organization, Law enforcement center, and government system. This needs of inter communication security through efficiently information sharing. Information Brokering System is collecting and re-distributing information among organization. Information brokering system fully trust on broker, who satisfied user requirement to find out particular data server without knowing address which contain data which user want. Large amount of detail data broker are collected from million providers authenticate user and routing the request to particular user. With increasing protection and privacy of data we introduce Preserve & secure privacy information brokering system. In that system fully trusted on broker we produce broker-coordinator overlay. The sensitive data encrypted before outsourcing user & data privacy. To enrich privacy used Cryptosystem with the use of Selective encryption using AES. We focused two types of privacy attacks namely inference attack and attribute-correlation attack. Solutions of this problem for preventing these attacks are automaton segmentation & segment encryption. By using these algorithm the PPIB system using web platform will require less time than Distributed PPIB.

Keywords*:- privacy, access control, attack, XML, information sharing.*

*****

I. INTRODUCTION

Storing and sharing information on the global internet has become needed of the modern technology. An important requirement of each system is to protect data and service against unauthorized user confidentiality or secrecy. An unauthorized or improper modification done by legitimate users is affecting to the system no denial of service or availability. Now a day, the modern technology and information management system made more powerful. The problem arises of enforcing data privacy and security also becomes more difficult and critical task. A basic component in enforcing protection is represented by the access control service whose main work is to control each request to services or data maintained by a system. It will determine the request should be granted or denied. The access control service established all kinds of policies and rule then enforced by the mechanism of access control to the service that stated. The provided interface, security administrator can be stated the access control policy that should be obeyed in control access to manage resource.

A many information systems have been developed exiting to provide secure and efficient information sharing [1]. We have challenging job is balance peer autonomy and system coalition. The increase of distributed data management information applications has follows the internet rise. Users on a internet site storing information for the sharing purpose it with multiple recipients .In the other way, sharing large amount of information is dangerous, because the information recipients, or the system itself its assume that it is not controlled by the owner of information. If share sensitive data the eavesdroppers who is not au It may have incentive to share sensitive data with eavesdroppers whose user not authorized user to view data, but it we knowing the information.

In Distributed Information Brokering System (DIBS) is a Peer to Peer overlay network that comprises brokering components and diverse data servers help client queries locate the data server [3]. Information federated system with diverse participants from different organizations like data producer and data consumer require of organizational information sharing. Different type application always needed various forms of sharing information. Many virtual private networks and internet provide better data communication, there are some challenges specified

An IBS system is a Peer to Peer overlay network consisting of data owners, brokers and data requester (i.e. data requestors). This type of architecture is developed in an inter-organization model. In multiple organizations have strong needs of cross organizational information sharing.

Here we define IBS as agent based systems that across loosely federatedXML or XML supported databases. XML data model and XML query languages are adopted to achieve the desired query expressiveness. In a distributed structure of the network topology and routing protocol adopted by the information broking system, one broker only holds a partial set of all routing rules. Thus, multiple brokers should collaborate in routing an XML query to its destination data source. The attacker could infer the security and privacy of different storage through attribute correlationattacks and inference attacks

Attribute Correlation Attack

Predicates of an xml query describe conditions that mostly carry more sensitive and private information (e.g., username, id, credit card id). The attacker can correlate the attributes in the predicates to infer sensitive data about owner. This is called attribute correlation attack.

Inference Attack

This attack is occurred by finding location of data server or data owner by using IP address. For example: An attacker identifies a data server location at a NASA research center, he can tag the queries as planet related.

II. RELATED WORK

F. Li, B. Luo, P. Liu, D. Lee, P. Mitra, 2006, W. Lee, and C. Chu [2] authors specified in Broker Access control for Information Brokering System. An xml brokering systems is a information distributed xml database system that comprises between data sources and brokers. System holds xml document and documents distribution information. All previous information brokering systems handle or view query brokering and access control. As two issues in query brokering is issue of the system that concerns with cost and performance. Access control is an issue related to system that concern confidential information. As a result of access control deployment strategy define a terms of where and when to do access control such strategy end to end system performance. Propose the Inbroker access control deployment strategy where access control is pushed from the boundary into the heart of the information brokerage system.

S.Rizvi, A. Mendelzon, S. Sudarshan, and P. Roy [4] define model Query Rewriting Techniques for Fine Grained Access control. In this model every users are members of appropriate roles and an access control policy consists of a set of role based 5tuple access control rules (ACR): R = {subject, object, action, sign, type}. Where 1) subject is a role to whom granted an authorization 2) object is xml nodes set specified by XPath 3) action is read, write and update; 4) sign 2 {+, −} refers to access control granted or denied and 5) type {LC,RC} refer to either local check (authorization is only apply to attribute or text data of context nodes “self::text()| self::attribute()”) or recursive check (authorization is apply to the context node and propagate to all descendants (descendant-or-self::node())).

G. Koloniari and E. Pitoura [6] represent Content Based Routing (CBR) of Path Queries in Peer to Peer Systems .Where Peer to Peer (P2P) systems are increasing popularity because to sharing data between large numbers of autonomous node. The nodes in a P2P system store xml documents. A fully decentralized approach to solve problem of routing queries path between the nodes of a P2P system on maintaining special data structures is called filters. Filters will efficiently summarization the content, build a hierarchical organization of nodes by cluster together with same content of nodes. The similarity among nodes is related to the similarity between the corresponding filters. The previous CBR System used hierarchical organization, processing the data among the mediator and the remote located user is time consuming job.

III. IMPLEMENTATION DETAIL

Architecture

System Overview

Privacy preserving information broking system has three types of brokering components 1) Brokers 2) Coordinators and 3) Central authority (CA). The privacy is to main part of the work on more than one components in such a way that more than one node can make a meaningful presumption from the information disclosed to it. Through local brokers the data servers and data requestors from various organizations connecting to the system.

Brokers:

It is local broker which intercommunicate via coordinators. A local broker functions as enter to the system. It is responsible for authenticates requestors and hides it. It can permute query sequence to defend against local traffic occurred in the network.

Coordinators:

Coordinators are responsible for access control and content based query routing. With privacy preserving idea, coordinator cannot hold any rule and data in the complete form, its hold partial. A novel automaton segmentation scheme to dividing metadata information rule into segments and assign each segment to a respective coordinator. Coordinator operates collaboratively to act enforcing secure routing query. Coordinator prevents sensitive predicates by using a query segment encryption scheme and automaton segmentation scheme. By this scheme query divide into segment and each segment encrypt.

Central Authority (CA):

It is responsible to metadata maintenance and key management.

Automaton Segmentation

In PPIB adopt the free automaton based access control mechanism, and extend it in a decentralized approach with Automaton segmentation scheme. The concept of automaton segmentation arise from the multilateral security split sensitive information too largely meaningless session multiple parties held who cooperate to share the privacy preserving responsibility. An automaton segmentation schemes first divide the global access control automaton data into several segments. Granularity of segmentation is maintained by a size of parameter partition, which specified how many XPath state in the global automaton are divided and combine into the one segment. The large the granularity is depend on the system administrator. Higher granularity represents to good privacy preserving but also more needed complex query process. Each accepts state of the global automaton is partitioned as a separate segment. Then we assign each segment to one independent site.

1. Segmentation: The atomic unit in the segmentation is an NFA state of the original automaton. Each segment is allowed to hold one or several NFA states.

2. Deployment: We deploy physical brokering servers is called *coordinators* to store the logical segments. To reduce the number of needed coordinators, several segments can be deployed in the one coordinator using different port numbers. So, the tuple uniquely identifies a segment.

3.Replication: All the queries are to be processed by the root coordinator first; it becomes a single point of failure and a performance bottleneck. For robustness, we require replication the root coordinator as well as the coordinators at higher levels of the coordinator tree. Replication has been extensively described in distributed systems

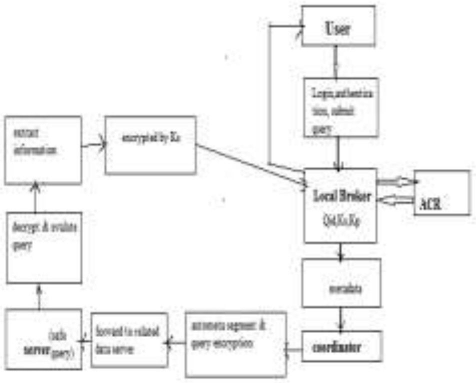


Figure 1. System Architecture

B. Algorithms:
Input: submit data or search query Q

Output: store data in segment & encrypted form or obtain result of search query in secure form.

A. Submit the query

1. User authenticate from broker Ua.
2. Password is generated random function Fn
3. User submit query store in Xml form Q;
4. Key generated by using hash function Fh;
5. Encrypt the query using AES & public key Pk, unique session Ps

B. Prepare metadata

1. Prepare metadata set privacy policy { P1,.Pn}

2. Create unique id for each query Uid

C. Automata segmentations & query encryption

1. Seg=createSegment

2. Seg.addSegment(seg)

3. Coordinator = getCornordidinator();

4. Coordinator.assignSegment(seg);

D. Retrieve Query

1. Server receive safe query Qe

2. Return query Ru user via broker with session key

IV. RESULT AND DISCUSSION

Result of Preserve Privacy information brokering system performance analyzing using processing query to end to end system and scalability of system. In this system coordinator are coded by using C#.ASP.net and results are taken from coordinator running using web services. This application mostly used in real world. In the analysis of result show PPIB provides privacy protection with good scalability and insignificant overload for on-demand information brokering system.

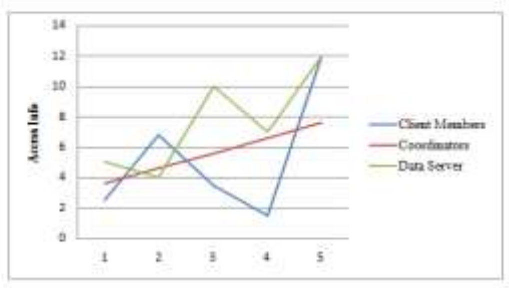


Figure 2 System Performance analyzing

System Scalability:

In this system scalability we evaluates the scalability of thePPIB system against complicity of data size(number of data objects and data servers) and ACR (access control rule) and following aspects.

Complicity of XML Schema and ACR:

When the segmentation scheme is discovered, the demand of coordinators is determined by the number of ACR segments, which is linear with the number of access control rules. Assuming finest granularity automaton segmentation is adopted. We can see that the increase of demanded number of coordinators is linear or even better. This is because similar access control rules with same prefix may share XPath steps, and save the number of coordinators. However different logical coordinators or ACR segments may reside at the same physical site. So reduce the actual demand of physical sites. In this framework, the numbers of coordinators m, and the height of the coordinator tree h, are highly dependent on how access control policies are segmented. In this part, the segments are received fully.

Data Size:

*W*hen data volume increases (e.g adding more data items into the online auction database) the number of indexing rules also increases. This results in increasing of the number of leaf coordinators. However, in PPIB query indexing is implemented through hash tables, which is scalable. Thus, the system is scalable when data size increases. Also shared secure and privacy- preserving information using brokering system

B. End to End Query Processing Time:

In the results, the total forward query processing time is calculated as, T forward≃ 1.9 × 5.7 + 100 5.7 + 1 ≃ 681 ms . It is obvious that network latency TN*(NHOP+1) dominates total forward end-to-end query processing time, because the value of TC is negligible compared with TN. since TN remains the same (as an estimation from Internet traffic), NHOP becomes the deterministic factor that affects end-to-end query processing time. Note that for other information brokering systems, although they use different query routing scheme, network latency is not avoidable. As a conclusion, the proposed PPIB approach achieves privacy-preserving query brokering and access control with limited computation.

Average Request Brokering Time

Figure 3 show time require in information brokering system and Privacy preserving brokering-coordinator system vs number of keyword. When number of keyword searching increases existing system required more time due to overload in broker but proposed system work is divided into number of coordinator .Also Privacy and security increases due to authentication, segmentation.

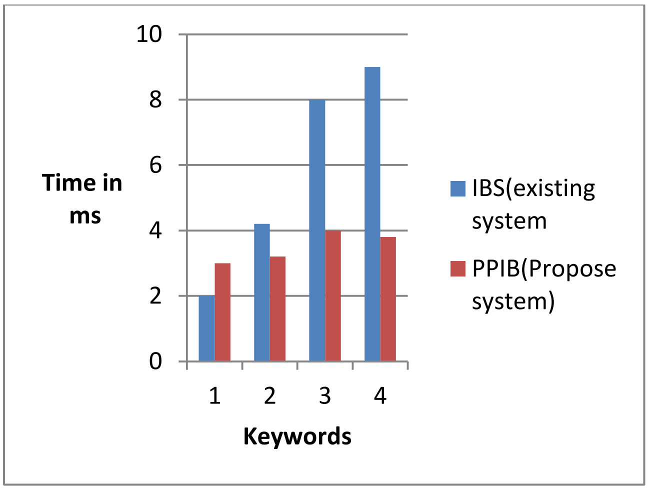
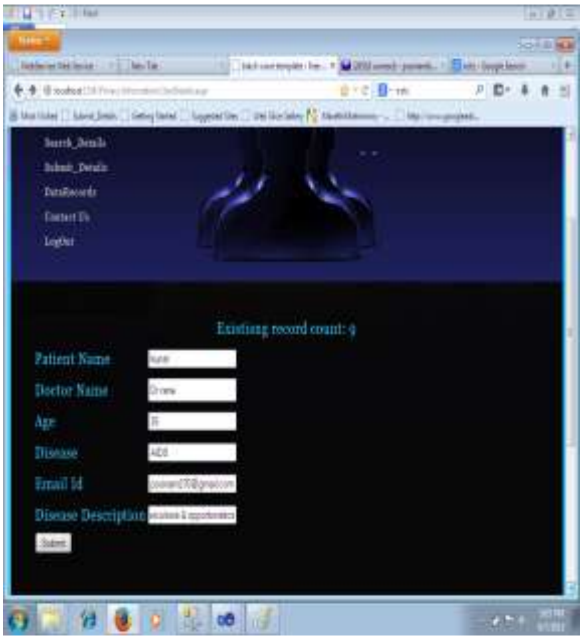


Figure 3 : Average Request Brokering time

Proposed Solution and Prototype:

The application is able to demonstrate various layers of security with privacy preserving information brokering. Our application was built using C#.ASP.net platform using Web Forms. Multiple users interact with the system through access right. Information flow as access control & business legal issues as Privacy & security.

Figure 4, 5 show that user screen where user after authentication he can submit the data detail also search query without knowing server location.

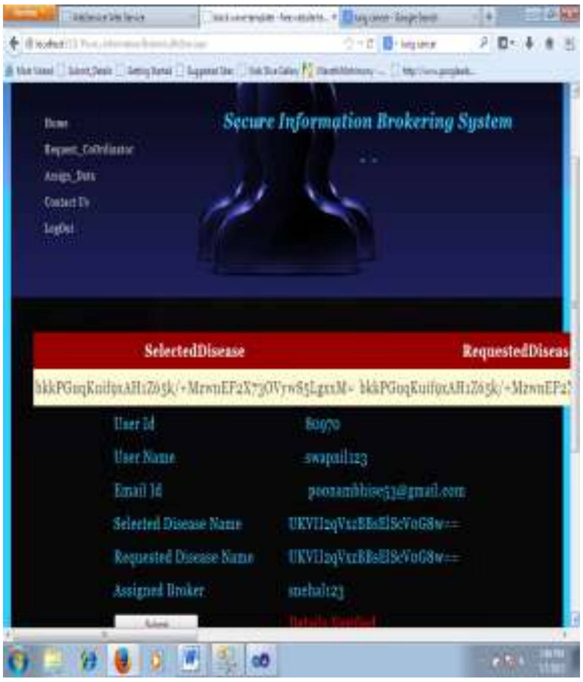


Existiung record count: 9

Patient Name	kunal
Doctor Name	Dr.rane
Age	35
Disease	AIDS
Email Id	poonam0170@gmail.com
Disease Description	infections & opportunistics

Figure 4, 5 UI for User

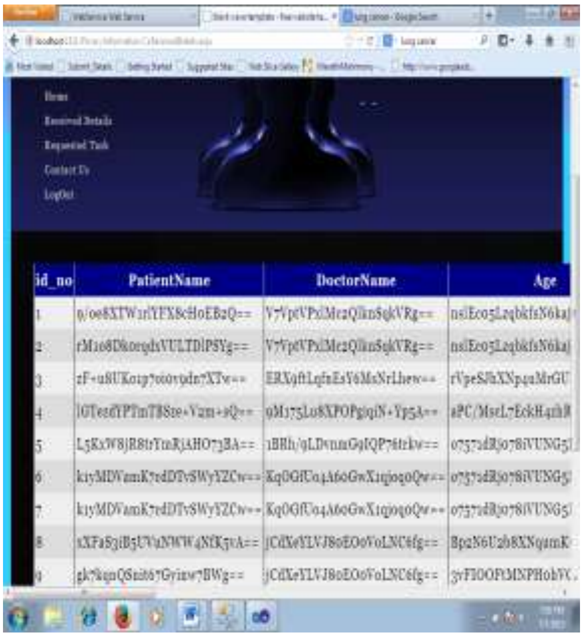
Figure 6, show the broker screen who can request coordinator to search the query also assign data to appropriate user which came from coordinator.



SelectedDisease	RequestedDiseas
hkkPGuqKuif9xAH1Z65k/+MzwnEF2X73OVyw85LgxxM=	hkkPGuqKuif9xAH1Z65k/+MzwnEF2

User Id	80970
User Name	swapnil123
Email Id	poonambhise53@gmail.com
Selected Disease Name	UKVIl2qVxzBBsElScVoG8w==
Requested Disease Name	UKVIl2qVxzBBsElScVoG8w==
Assigned Broker	snehal123

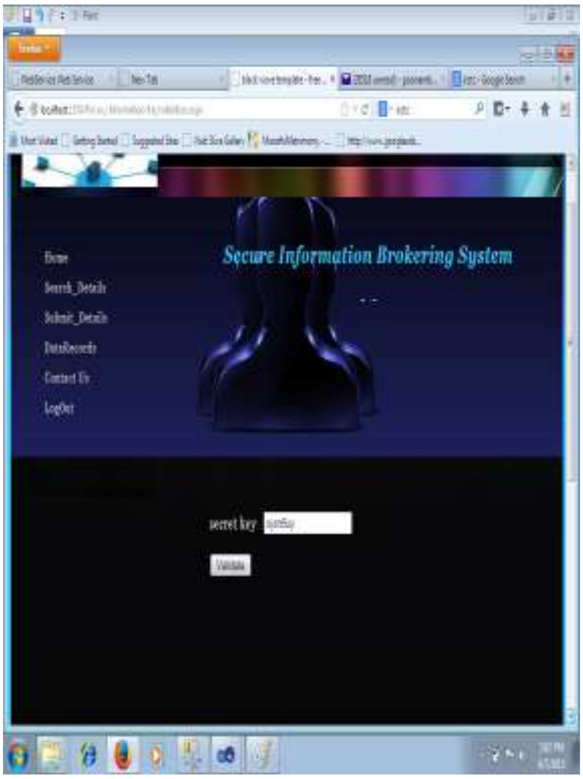
Figure 6 UI for Broker



id_no	PatientName	DoctorName	Age
1	9/oe8XTW1rlYFX8cHoEB2Q==	V7VpfVPxlMe2QlinSqkVRg==	nslEco5LzqbkfsN6kaj
2	rM1o8DkorqdxVULTDIPSYg==	V7VpfVPxlMe2QlinSqkVRg==	nslEco5LzqbkfsN6kaj
3	zF+u8UKo1p7oiovqdn7XTw==	ERXqftLqfnEsY6MxNrLhew==	rVpeSJhXNp4uMrGU
4	lGTesdYPTmTBSre+Vzm+9Q==	9M175Lo8XPOPg9qiN+Yp5A==	aPC/MseL7EckH4zhR
5	L5KxW8jR8trYmRjAHO73BA==	1BRh/9LDvnmG9IQP76trkw==	07572dRj078iVUNG5I
6	k1yMDVamK7edDTvSWyYZCw==	Kq0GfUo4A6oGwX1qjoq0Qw==	07572dRj078iVUNG5
7	k1yMDVamK7edDTvSWyYZCw==	Kq0GfUo4A6oGwX1qjoq0Qw==	07572dRj078iVUNG5
8	sXFaS3iB5UVaNWW4NfK5vA==	jCdXeYLVJ8oEOoVoLNC6fg==	Bp2N6U2b8XNqamK
9	gk7kqnQSni67Gyinw7BWg==	jCdXeYLVJ8oEOoVoLNC6fg==	3vFIOOFtMNPHobVC

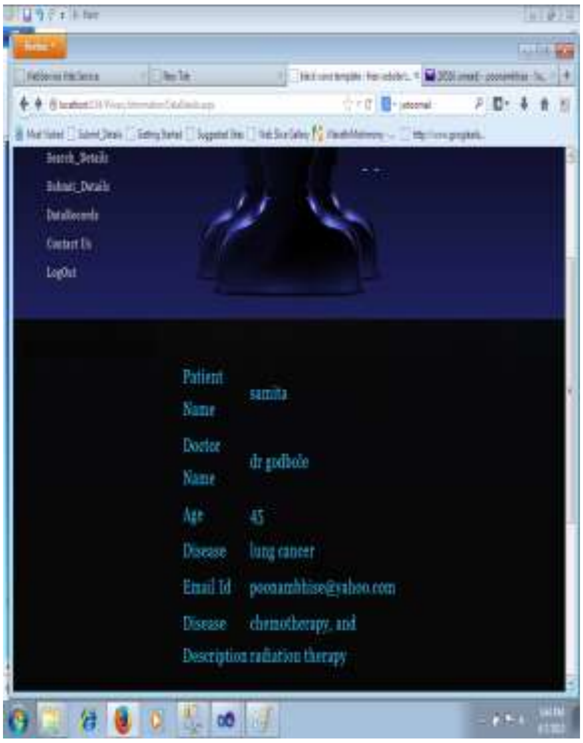
Figure 7 UI for Coordinator

Figure 7, show coordinator screen which show receive details in encrypted from which submitted by user.



secret key: sjsnfkjs

Figure 8 UI for user Data Record



Patient Name samita
Doctor Name dr godbole
Age 45
Disease lung cancer
Email Id poonambhise@yahoo.com
Disease Description chemotherapy, and radiation therapy

Figure 9 UI for user query result

Figure 8 show that user screen data record which is result of query submitted that user.by using secrete key which is provided to registered email address by using this secrete key user can get query result as shown figure 9.

V. CONCLUSION

In this project more concentrate on user privacy, data privacy and metadata. In previous information broking system suffered on privacy and security. In this project we propose a new approach to preserve privacy & security in information broking system. Also work on automaton segmentation schema, query segmentation scheme, access control.

VI. FUTURE SCOPE

Future enhancement is to minimize or eliminate the participation of the administrator, who decides such issues as automaton segmentation, site distribution and replication. A main goal is to make system self-reconfigurable.

REFERENCES

[1] Fengjun Li, Bo Luo, Peng Liu Dongwon Lee and Chao-Hsien Chu, "Enforcing Secure and Privacy-Preserving Information Brokering in Distributed Information Sharing", IEEE TRANSCATIONS ON INFORMATION FORENSICS AND SECURITY, 2013.

[2] F. Li, B. Luo, P. Liu, D. Lee, P. Mitra, W. Lee, and C. Chu, "In-broker access control: Towards efficient end-to-end performance of information brokerage systems," in Proc. IEEE SUTC,2006.

[3] A.P.Sheth and J. A. Larson, Federated database systems for managing distributed, heterogeneous, and autonomous databases,‖ ACM Comput. Surveys (CSUR), vol. 22, no. 3, p p. 183–236, and 1990.

[4] S. Rizvi, A. Mendelzon, S. Sudarshan, and P. Roy, Extending query rewriting techniques for fine-grained.

[5] W. Bartschat, J. Burrington-Brown, S. Carey, J. Chen, S.Deming, and S. Durkin, "Surveying the RHIO landscape: A description of current {RHIO} models, with a focus on patient identification," J. AHIMA, vol. 77, pp. 64A–64D, Jan. 2006.

[6] G. Koloniari and E. Pitoura, "Content-based routing of path queries in peer-to-peer systems," in Proc. EDBT, pp. 29–47,2004.

[7] F. Li, B. Luo, P. Liu, D. Lee, and C.-H. Chu, "Automaton segmentation :A new approach to preserve privacy in XML information brokering," in Proc. ACM CCS'07, pp. 508–518,2007.

[8] A. C. Snoeren, K. Conley, and D. K. Gifford, "Mesh-based content routing using XML," in Proc. SOSP, pp. 160–173,2001.

[9] N. Koudas, M. Rabinovich, D. Srivastava, and T. Yu, "Routing XML queries," in Proc. ICDE'04, p. 844, 2001.

[10] G. Koloniari and E. Pitoura, "Peer-to-peer management of XML data: Issues and research challenges," SIGMOD Rec., vol. 34, no. 2, pp. 6–17, 2005.