

Secure Information Brokering in Distributed Information Sharing

Priyanka M. Jamunkar¹, Prof. G. M. Bhandari²

¹P.G. Student, Savitribai Phule Pune University, Department of Computer Engineering, BSIOTR, Wagholi, Pune, Maharashtra, India

²Head of Department, Savitribai Phule Pune University, Department of Computer Engineering, BSIOTR, Wagholi, Pune, Maharashtra, India

Abstract: Information Brokering System (IBS) on a peer-to-peer overlay has been proposed to support information sharing among loosely federated data sources. Today's organizations raise increasing needs for information sharing through on demand information access. To aid requirement of organization information systems are designed as distributed network systems, where existing information systems and new components are connected together using a middleware. Many existing IBSs assume that brokers are trusted and only adopt server-side access control for data confidentiality. One commonly accepted and used system is Distributed Information Brokering System, which is a peer-to-peer network that comprises different data servers, and brokering components helping client queries locate the data. Preserve privacy of multiple stakeholders involved in the information brokering process and define two privacy attacks, attribute-correlation attack and inference attack, and propose two countermeasure schemes automaton segmentation and query segment encryption to securely share the routing decision. The idea of information sharing across such databases, and increase protocol that no single entity hold the complete data that can be misused but it is passed on to the requested entity securely.

Keywords: Access control Distributed network, information sharing, information systems

1. Introduction

The Internet enables global sharing of data across organizational boundaries. Distributed file systems facilitate data sharing in the form of remote file access. The information can be collected from a variety of public and non-public sources including courthouse records, website cookies. In Information brokering system, data broker called an information broker or information reseller. They collect information about consumers and sell that information to other organization. Data brokers can refer to themselves as database marketers or consumer data analytics firms. Brokers create profiles of individuals for marketing purposes and sell them to businesses The information can be collected from a variety of public and non-public sources including website cookies and loyalty card programs.

Now, there is no legislation that requires a data broker to distribute the information. They have gathered with consumers they have profiled. In differentiate with the situations when the information seeker knows where needed data is located, Distributed Information Brokering System needs to help each information requesting query locate the corresponding information. Data owners collect data separately and control it with independent data servers. Though providing data access to honest users, data servers have to release assured privacy sensitive information that needs to be secure.

In Information Brokerage Systems, broker access control uses XML. An XML brokerage system is a distributed XML database system that comprises data sources and brokers which, hold XML documents and document distribution information. All existing information brokerage systems view or handle query brokering and access control orthogonal

issues. Query brokering is a system issue concerns costs and performance and access control is a security issue that concerns information privacy. So that, access controls implementation strategies. The impact of such strategies on system performance is neglected in existing information brokerage systems.

Information Brokering System (IBS) shown in Fig. 1, applications on IBS involve some association like RHIO along with a set of organizations. Databases of different organizations are connected throughout a set of brokers and metadata (e.g.data abstract) are pushed to local brokers, which advance advertises the metadata to other brokers. Queries are sent to local broker and routed according to the metadata until reaching right data server(s). Thus, a large number of information sources in different organizations are freely federated to provide combined, visible and on demand data access.

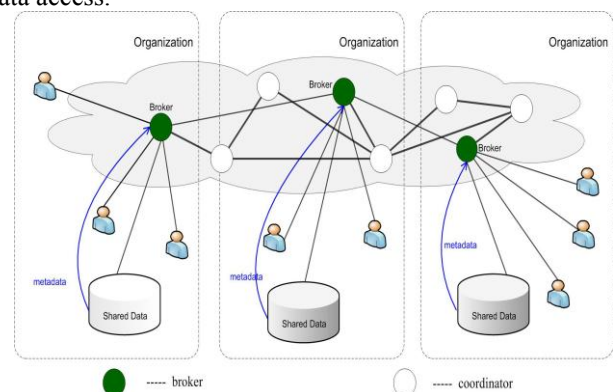


Figure 1: Information Brokering System (IBS)

2. Literature Review

The distributed information systems are designed when a

network of communicating and partially independent components several studies have been contributed for decentralized systems with correct data sharing, distributed processing, reservation of resources and reliable communication infrastructure.

2.1 Privacy Preserving Information Brokering System

In privacy-preserving information sharing problem first, need for privacy protection and propose a novel IBS is *Privacy Preserving Information Brokering (PPIB)*. It is a overlay infrastructure consisting of two types of brokering components, *brokers* and *coordinators*. The brokers, acting as mix anonymizer [10], are mainly responsible for user authentication and query forwarding. The coordinators, concatenated in a tree structure, enforce access control. To prevent curious or corrupted coordinators from inferring private information,

2.2 XML access control model

Fengjun Li and Bo Luo [4] states that though access control is required in most unless all DIBS. The popular approach[6][7] of XML access control model is proposed where users are members of proper roles and access control policy consists of a set of role based 5 tuple access control.

2.3 Peer (P2P) computing

Georgia koloniari and Evaggelia Pitoura has spurred much attention to peer to peer (P2P) computing [3]. Peer to peer computing refers to a structure of distributed computing that involves large number of autonomous computing nodes that collaborate to share resources and services. When opposed to traditional client-server computing, nodes in P2P systems have equal roles and act as data providers and data consumers.

2.4 XML access control model

The XML access control model proposed in [10] is adopted. In this model, users are members of appropriate roles and an access control policy consists of a set of role based 5-tuple of access control rules ,(ACR): $R = \{ \text{subject, object, action, sign, type} \}$ where, (1) subject is a role to whom an authorization is granted (2) object is a set of XML nodes specified by XPath (3) action is one of “read”, “write,” and “update” (4) sign 2 {+, -} refers to access “granted” or “denied,” (5) type 2 {LC,RC} refers to either “Local Check” (i.e., authorization is only applied to attributes or textual data of context nodes or “Recursive Check” (i.e., authorization is applied to content nodes and propagated to all descendants.

3. System Implementation

3.1 Query Segmentation Algorithm

It is difficult to protect the query from intercepted by irrelevant brokering servers. Hide the query content from any of the brokers, as they are needed to search or match a string in the metadata or the database, based on which the broker

requests coordinator for the data in brokering approaches. It is responsible for matching the query with the database index rules, which enforce query routing, or authorization. In study, the automaton segmentation scheme provides a new encryption opportunity to encrypt the query in pieces and allow each coordinator to decrypt the piece it is about to process. The query segment scheme consists of the string matching, content validation, and a special secret key based authentication module for processing.

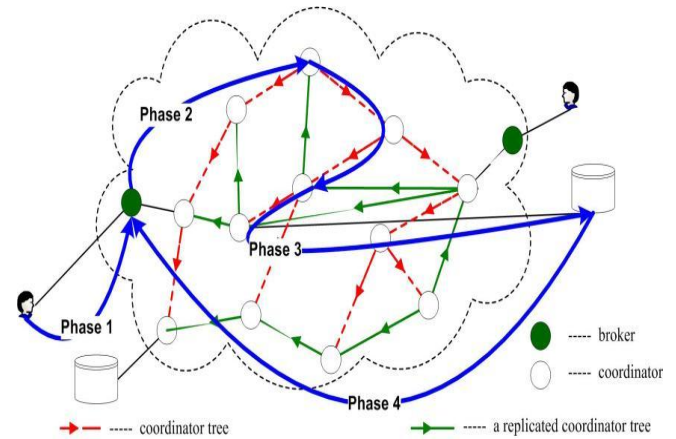


Figure 3: The four phases of Query brokering process

Phase 1: A user needs to authenticate him self to local broker then user submit query to broker in the form of string.

Phase 2: Broker authenticates as well as prepares metadata. The broker signs this query with his ID and forwards it to the coordinator.

Phase 3: Coordinator receives query and metadata from broker. Coordinator validates brokers ID and submits this query to the database.

Phase 4: In final phase the data server receives query. In database, unique secret key present for data relevant to the requested query is fetched and passed from coordinator to user via broker.

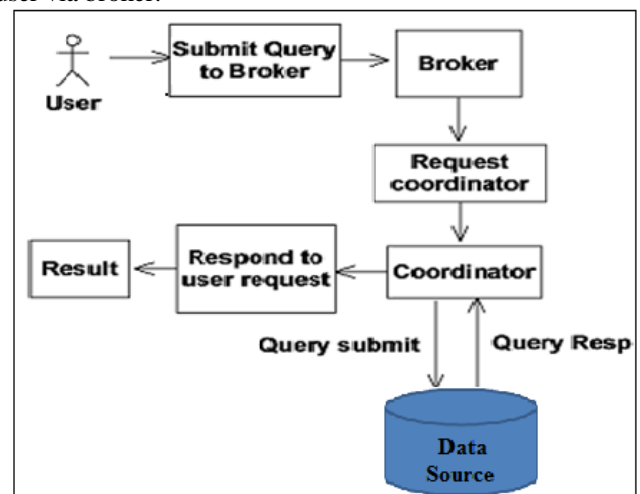


Figure 3: System Architecture

The implementation is achieved throughout approach for Regional Health information Organization (RHIO) as a case study. There are four modules are as follows.

- 1) **Admin Module:** Admin performs critical roles in registration of data owners and users, brokers, coordinators and organization in DIBS. He also manages the database.
- 2) **User Module:** Users are Data Users and Data Owner differing on their role and limitation on the data that will be passed to the Co-coordinator. The coordinator passes the details by broker and verified it with the secret key and so will get displayed to the users.
- 3) **Broker Module:** The broker is mediator between coordinator and data Users. The query submitted by a data user gets verified and passed to the co-coordinator.
- 4) **Coordinator Module:** Once the broker with his ID verifies a query, he submits it to the coordinator who in turn searches and sends the key to the data users by the broker. Coordinator also performs the global service between two end users via broker.

4. Result

Information is divided among broker and coordinator to protect access control, data privacy and query segmentation. Distributed information brokering system require minimum trust in all coordinator. So result in Table 1 shows system's level of trust without hurting privacy. The system privacy capability will be enhanced.

4.1 Registration Page

The Above implementation screenshot shows registration page. This is the registration page for a user, broker or and coordinator based on the role that they are eligible. At he time of registration the admin needs to appoint them to an organization. Each role has a unique ID correlated with it

4.2 Login Page

4.3 Screenshot shows query submitted by user to broker

User Id	User Name	Email Id	Disease Name
3	madhur	mady@gmail.com	fever
3	madhur	mady@gmail.com	fever
3	madhur	mady@gmail.com	fever
3	madhur	mady@gmail.com	fever

User Id: 3
 User Name: madhur
 Email Id: mady@gmail.com
 Disease Name: fever
 Broker Name:

4.4 Coordinator page shows user details sent to the broker

id_no	PatientName	DoctorName	Age	DiseaseName	Email	DiseaseDescription	SecretKey
1	pradip Patil	Bharti	20	headche	an@gmail.com	pain in head	sjkrp56
2	Sitaram Gaikwad	Dr. Chabukwar	50	Stomach Upset	sitaram@gmail.com	Having a problem of stomach upset.	m7c5sfw1

4.5 Given Screenshot shows data records received by the user with a secret key which after authentication displays the data .

4.6 XML Code showing stored Secret keys for each user.

```

<New_Table>
  <id_no>1</id_no>
  <PatientName>pradip Patil</PatientName>
  <DoctorName>Bharti</DoctorName>
  <Age>20</Age>
  <DiseaseName>headche</DiseaseName>
  <Email>an@gmail.com</Email>
  <DiseaseDescription>pain in head</DiseaseDescription>
  <SecretKey>sjtkrp56</SecretKey>
</New_Table>
<New_Table>
  <id_no>2</id_no>
  <PatientName>Sitaram Gaiwad</PatientName>
  <DoctorName>Dr. Chabukswar</DoctorName>
  <Age>50</Age>
  <DiseaseName>Stomach Upset</DiseaseName>
  <Email>sitaram@gmail.com</Email>
  <DiseaseDescription>Having a problem of stomach upset.</DiseaseDescription>
  <SecretKey>m7cssfw1</SecretKey>
</New_Table>
    
```

Table 1: Brokering components showing trust on systems privacy which is restricted

Privacy Type	Broker	Coordinator	Database
User Location	Trust	Hide	Hide
Query Content	Trust (Partially)	Trust (Partially)	Trust
Data Object Distribution	Hide	Hide	Trust
Access Control Policy	Hide	Trust (Partially)	Trust
Query Segmentation	NA	Trust	Trust

5. Conclusion

Information brokering systems has some of the critical weaknesses in the system. We propose new approach of PPIB in information brokering. Our system combines security implementation and query forwarding as providing comprehensive protection through novel Query segmentation scheme, in-network access control, and secret key based authentication. Our study shows that privacy concerns where trust factor is always changing from system wide brokers. Query processing scalable to suitable for small to medium organizations.

6. Acknowledgement

I would like to express my sincere gratitude to my guide Prof.G.M.Bhandari for her continuous support, patience, motivation, enthusiasm, and immense knowledge. Her guidance helped me in all the time of research and writing of this paper.

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 TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, 2013

[2] Distributed Information System as a System of Asynchronous Concurrent Processes MarekRychl'y and Jaroslav Zendulka.

[3] Georgia koloniari and EvaggeliaPitoura.Content-based Routing of Path Queries in Peer-to-Peer Systems.

[4] Fengjun Li, Bo Luo, Peng Liu, Dongwon Lee, and Chao-Hsien Chu. "Automaton Segmentation: A New

Approach to Preserve Privacy in XML Information Brokering", CCS'07, October 29–November 2, 2007, Alexandria, Virginia, USA.

[5] 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 ACM CCS '07, pp. 508–518, 2007.

[6] 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.

[7] X. Zhang, J. Liu, B. Li, and T.-S. P. Yum, "CoolStreaming/DONet. A data-driven overlay network for efficient live media streaming," in Proceedings of IEEE INFOCOM, 2005.

[8] M. Franklin, A. Halevy, and D. Maier, "From databases to dataspace: A new abstraction for information management," SIGMOD Rec., vol. 34, no. 4, pp. 27–33, 2005.

[9] E. Damiani, S. Vimercati, S. Paraboschi, and P. Samarati. A fine-grained access control system for XML documents. ACM Trans. Inf. Syst. Secur., 5(2):169-202, 2002.

[10] Berglund, S. Boag, D. Chamberlin, M. F. Fernandez, M. Kay, J. Robie, and J. Simon, XML Path Language (XPath). ver. 2.0, 2003 [Online]. Available: <http://www.w3.org/TR/xpath20/>

[11] L. M. Haas, E. T. Lin, and M. A. Roth, "Data integration through database federation," IBM Syst. J., vol. 41, no. 4, pp. 578–596, 2002.

Author Profile

Ms. Priyanka M. Jamunkar received the Bachelors degree (B.E.) Computer Science and Engineering in 2010 from JDIET, Yavatmal. She is now pursuing Masters degree (Computer Engineering), from BSIOTR, Wagholi, Pune, Maharashtra.

Prof. G. M. Bhandari received her M.Tech (Computer Engineering) and now pursuing Ph.D. She is also working as Head Of Computer Engineering Department, Bhivarabai Sawant Institute of Technology & Research, Wagholi, Pune, Maharashtra. Her research areas are Cloud, Sound Processing, and Computer Network.