ISSN 2395-1621

Enforcing Secure Privacy Preserving Information Brokering Using Load Balancing In Distributed Information Sharing For Hospital Management

[#1]Miss. Dipali Rajendra Mahajan, [#2]Miss. Shweta Rajesh Nimbalkar,
[#3]Miss. Swati Laxman Kendre, [#4]Prof. D.P. Salapurkar

[1]dipalimahajan77@gmail.com
[2]shweta.nimbalkar7@gmail.com
[3]swati.kendre1994@gmail.com
[4]dpsalapurkar.scoe@sinhgadn.edu

[#1234]Computer Engineering Department,
Sinhgad College of Engineering Pune, Maharashtra, India

ABSTRACT

Today's organizations raise increasing needs for information sharing via on-demand information access to facilitate extensive collaborations. To support information sharing among loosely federated data sources, Information Brokering System or IBS atop a peer-to-peer overlay has been proposed. Client queries to locate the data servers, it consists of diverse data servers and brokering components However, many existing IBSs shed little attention on privacy of data and metadata stored and exchanged within the IBS and adopt server side access control deployment and honest assumptions on brokers. In this paper, in information brokering process we study the problem of privacy protection. We first give a formal presentation of the threat models with a focus on two attacks: First one is attribute-correlation attack and second one is inference attack. After that we have proposed a broker coordinator overlay. To share the secure query routing function among a set of brokering servers, We also proposed, automaton segmentation and query segment encryption scheme. To preserving system-wide privacy with reasonable overhead, we show that the proposed system can integrate security enforcement and query routing, With comprehensive analysis on privacy, end -to- end performance, and scalability.

ARTICLE INFO

Article History

Received: 13th May 2016

Received in revised form :

13th May 2016

Accepted: 17th May 2016

Published online :

19th May 2016

Keywords: **Access control, Information Brokering System, Information sharing, Privacy.**

I. INTRODUCTION

A. Project Idea

In this paper we described a general solution to the privacy-preserving information sharing problem. First, we propose Privacy Preserving Information Brokering or PPIB, to address the need for privacy protection. Two types of brokering components contain in its overlay infrastructure, first one is brokers and second one is coordinators. The brokers, acting as mix anonymizer. The brokers are mainly responsible for user authentication and query forwarding. The second brokering components are the coordinators. The coordinators concatenated in a tree structure, enforce access control and query routing based on the embedded non-deterministic finite automata the query brokering automata. To segment the query brokering automata and encrypt corresponding query segments we have designed two novel schemes, so that for a set of collaborative coordinators, routing decision making is decoupled into multiple correlated tasks, to prevent curious or corrupted coordinators from inferring private information. The proposed IBS also ensures that a curious or corrupted coordinator is not capable to collect enough information to infer privacy, such as which data is being queried, where certain data is located, or what are the access control policies, while providing integrated in-network access control and content-based query routing. Experimental results show that for on-demand information brokering, within significant overhead and very good scalability, PPIB provides comprehensive privacy protection. To preserve privacy of patient record and medical report in

the proposed system (PPIB) is used for privacy preservation, encryption and decryption algorithms to provide security to the system, load balancing to improve work redistribution and response time.

B. Goals and Objective

Today's organizations raise increasing needs for information sharing via on-demand information access to facilitate extensive collaborations. To support information sharing among loosely federated data sources, Information Brokering System or IBS atop a peer-to-peer overlay has been proposed. The main objective of this project is use PPIB Method for providing the security on Storage sharing data for access only authenticated person. Other objectives are listed below:

First is for distributed data achieving scalable, agile and secure remote access. Second is the data formats which are not always structured and incompatible with each other, handling such heterogeneity among data management systems. Third is handling the dynamics of modern business applications where new schema elements may emerge every day.

C. Scope

This project proposes an innovative Privacy Preserving Information Brokering (PPIB) framework. To address the user or data or metadata privacy vulnerabilities that are associated with existing distributed IBS, this project proposes an innovative Privacy Preserving Information Brokering or PPIB framework. Dividing and allocating the functionality to multiple brokering components in a way that no single component can make a meaningful inference from the information disclosed to it, is the key to preserving privacy.

II. EXISTING SYSTEM

In the existing system consider 'A' owns a k-anonymous database and she needs to determine whether her database, when inserted with a tuple owned by 'B', is still k-anonymous. Suppose that access to the database is strictly controlled, because data are used for certain experiments that need to be maintained confidential. Clearly, allowing 'A' to directly read the contents of the tuple breaks the privacy of 'B'; on the other hand, the confidentiality of the database managed by 'A' is violated once 'B' has access to the contents of the database. Thus, the problem is to check whether the database inserted with the tuple is still k-anonymous, without letting 'A' and 'B' know the contents of the tuple and the database respectively. The Disadvantage of existing system is that thee database with the tuple data does not be maintained confidentially and the existing systems allows another person to easily access database.

III. LITERATURE OF SURVEY

A. Enforcing Secure and Privacy-Preserving Information Brokering in Distributed Information Sharing by Fengjun Li, Bo Luo, Peng Liu, Dongwon Lee, and Chao-Hsien Chu

We studied proposed Information Brokering System or IBS to support information sharing among loosely federated data sources. We also studied formal presentation of the threat models, broker coordinator overlay and automaton segmentation and query segment encryption scheme. For privacy issue like to prevent curious and corrupted coordinators two schemes are applied which are to segment the query brokering automata and encrypt corresponding query segments.

B. Information Sharing Across Private Databases by R. Agrawal, A. Evfimivski, and R. Srikant

We studied formalize how to minimize information sharing across private databases, and develop protocols for intersection, equijoin, intersection size, and equijoin size. We also studied how new applications can be built using the proposed protocols in this paper.

IV. COMPONENT

A. Module

1. Coordinator Module

Between the two end users, the co-coordinator performs the global service. At Initial stage the Data Owner have to submit the details of the patient to the server. Then the data Users needs to search the data and data user give request for the data. Then the Coordinator sends the key to the Data users, after getting key the data will be passed by the broker Way.

2. Broker Module

The broker can act between the Co-coordinator and the data Users. The request will be passed to the co-coordinator after verifying all request submitted from the data user. Then the data will be passed from the co-coordinator and submitted to the End Users(Data Users).

3. User Module

The Users are classified into two types depends on the restriction the data will be passed to the Co-coordinator they are Data Users and Data Owner. The co-coordinator pass the details via broker and with the help of secret key the data will be checked and thus it will display for the users.

4. Admin Module

Arrange the database based on the details and records of patient and doctor. The admin needs to register and register the Organization and Users Forms.

All paragraphs must be indented. All paragraphs must be justified, i.e. both left-justified and right-justified.

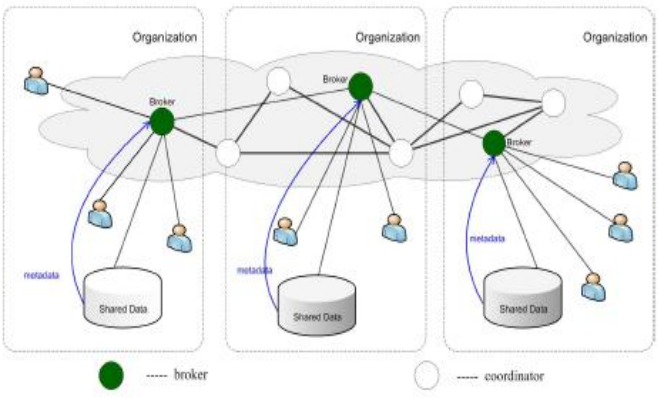

Fig 1. PPIB Architecture

V. RESULTS

A. Home Page

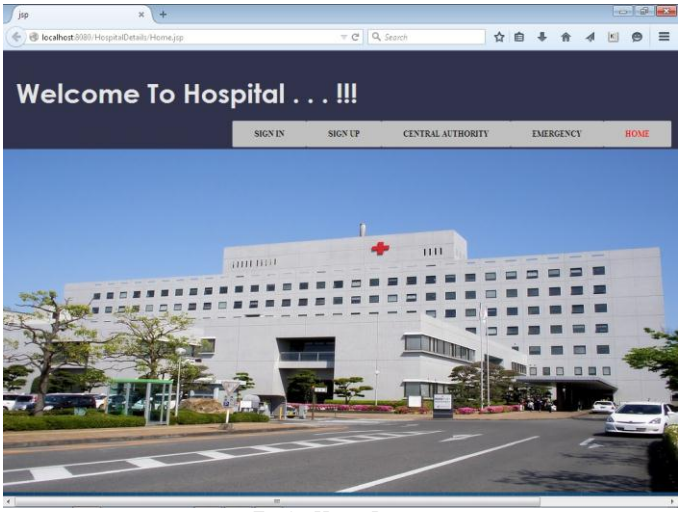

Fig 2. Home Page

B. Registration Form for Broker

Fig 3. Registration Form for Broker

C. User Query Forward

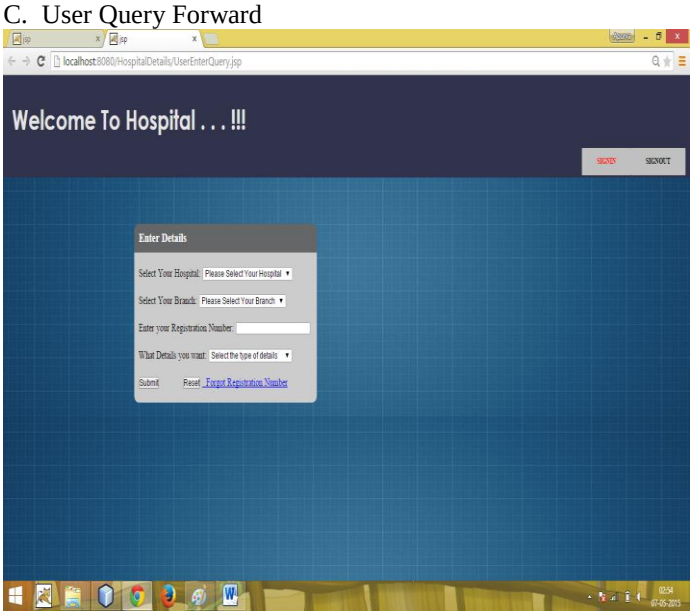

Fig 4. User Query Forward

VI. TESTING

A. Check the details on home page: Sign-in, sign-up, Central authority, Emergency.

Pre-requisite	Test cases	Required result	Actual result (Pass/Fail)
1. Browser should be open. 2. User should already logged in.	1. Click on required link. 2. Check the fields on the home page. 3. All the fields spelled correctly and in specific format and fond.	All the fields spelled correctly and in specific format	Pass

B. To check the sign-in functionality for valid or invalid password and username.

Pre-requisite	Test cases	Required result	Actual result (Pass/Fail)
1.User should already logged in.	1. Enter the valid user name and password.	The user is sign-in successfully.	Pass
2. To check for invalid password and valid user name	Enter invalid password and valid username	The application should display an error message and re-open the sign-in page.	Pass

C. To check the reset functionality

Pre-requisite	Test cases	Required result	Actual result (Pass/Fail)
Admin should be logged in.	1.Enter the user name and password. 2. Select the fields like: Server join, Server Leave, risk management etc. 3.Click on reset button.	All the fields should be null after clicking reset button.	Pass

D. To check the server leave and server join functionality.

Pre-requisite	Test cases	Required result	Actual result (Pass/Fail)
Admin should logged in	1.Click on sign in button. 2. In the server join and server leave panel enter the permission. 3. Click on accept or reject button. 4. Click on Sign out.	Here, the broker joins or leave the system according to their send request.	Pass

E. To check ACR functionality.

Pre-requisite	Test cases	Required result	Actual result (Pass/Fail)
1. Admin should logged in	1.Again click on sign-in button. 2. Click on right approval. i.e. ACR 3. Enter the work of CO and location. 4. Save the object and location of CO to IR table. 5. Click save. 6. Click on Sign-out option.	All the data should be stored in ACR table successfully.	Pass

VII. CONCLUSION

For privacy of user, data or and metadata during the design stage, existing information brokering systems suffer from a spectrum of vulnerabilities associated with user, data and metadata privacy. A new approach to preserve privacy in XML information brokering is PPIB. While providing comprehensive privacy protection, the PPIB integrates security enforcement and query forwarding. The evaluation of End-to-end query processing performance and system scalability show that PPIB is efficient and scalable. There are many directions are ahead for future research. Site distribution and load balancing in PPIB are in an ad-hoc manner. We will extends the research to provide an automatic scheme that does dynamic site distribution.

ACKNOWLEDGEMENT

It gives us great pleasure in presenting the preliminary project report on '**Enforcing Secure Privacy Preserving Information Brokering Using Load Balancing in DIS for Hospital Management**'. We are highly indebted to my internal guide **Prof. D. P. Salapurkar**. for their guidance and constant supervision as well as providing necessary information regarding the project. We are really grateful to them for their kind support. Their valuable suggestions were very helpful. We are also grateful to **Prof. P. R. Futane**, Head of Computer Engineering Department, Sinhgad College of Engineering for his indispensable support, suggestions.

REFERENCE

[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, VOL. 8, NO. 6, JUNE 2013.

[2] R. Agrawal, A. Evfimivski, and R. Srikant, "Information sharing across private databases", in Proceedings of the 2003 ACM SIGMOD, 2003.

[3] 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.

[4] A. P. Sheth and J. A. Larson, Federated database systems for managing distributed, heterogeneous, and autonomous databases, ACMComputing Surveys (CSUR), vol. 22, no. 3, pp. 183236, 1990.

[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. 64A64D, Jan. 2006.

[6] M. Siegenthaler and K. Birman, Privacy enforcement for distributed healthcare queries, in Pervasive Health 2009, 2009.

[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 CCS07, 2007, pp. 508518.

[8] M.Murata, A. Tozawa, andM. Kudo, XML access control using static analysis, in Proc. ACM CCS, 2003, pp. 7384.

[9] M. Bellare, A. Boldyreva, and A. ONeill, Deterministic and efficiently searchable encryption, in Proc. CRYPTO07, Santa Barbara, CA, USA, pp. 535552.

[10] G. Koloniari and E. Pitoura, Content-based routing of path queries in peer-topeer systems, in Proc. EDBT, 2004, pp. 2947.

[11] R. Huebsch, B. Chun, J. Hellerstein, B. Loo, P. Maniatis, T. Roscoe, S. Shenker, I. Stoica, and A. Yumerefendi, The architecture of PIER: An Internet-scale query processor, in Proc. CIDR, 2005, pp. 2843.

