International Journal of
Scientific Engineering and Technology Research

ISSN 2319-8885
Vol.05,Issue.11
May-2016,
Pages:2250-2253

www.ijsetr.com

Secure Information Brokering in Centralized Data Information Sharing

A. LEELAVATHI[1], K. HARIGANGABHAVANI[2]

[1]Assistant Professor, Dept of MCA, Sri Vasavi Engineering College, Tadepalligudem, West Godavari, AP, India,
E-mail: leelavathee@gmail.com.

[2]PG Scholar, Dept of MCA, Sri Vasavi Engineering College, Tadepalligudem, West Godavari, AP, India,
E-mail: hariganga7@gmail.com.

Abstract: In a peer-to-peer overlay has been proposed to support information sharing among loosely federated data sources using Information Brokering System (IBS). To access the information on demand organizations raise increasing needs for information sharing. In organization information systems are designed as distributed network systems, where existing information systems and new components are connected together using a middleware. Server-side access control for data confidentiality and brokers are trusted in many existing system. In any case, in completing thus, these results unavoidably present a consequential processing overhead on the data possessor for key distribution and data authority when fine-grained data access control is in demand, and subsequently don't scale well. We also address user cancellation. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes construct for clouds which are centralized. 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 to preserve privacy of multiple stakeholders involve.

Keywords: Access Control Distributed Network, Information Sharing, Information Systems.

I. INTRODUCTION

Why network of brokers: To provide massive scalability of a large messaging fabric we typically want to allow many brokers to be connected together into a network so that we can have as many clients as we wish all logically connected together - and running as many message brokers as we need based on the number of clients and network topology. If we are using client/server or on demand information access then the broker you connect to becomes a single point of failure which is another reason for wanting a network (or cluster) of brokers so that we can survive In failure of any particular broker, machine or subnet, network of brokers allows us to support distributed queues and topics across a network of brokers. This allows a client to connect to any broker in the network - and fall over to another broker if there is a failure - providing from the client's perspective a cluster of brokers. 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.

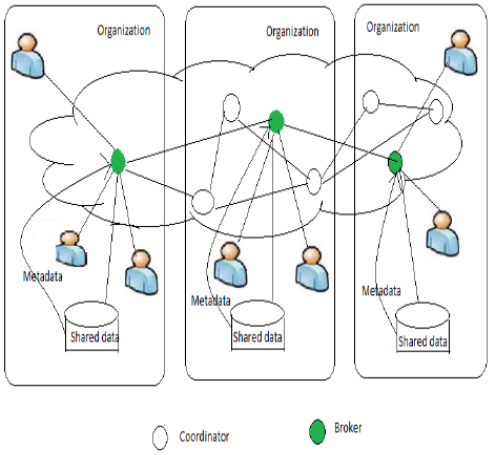

Fig.1. Information Brokering System (IBS).

II. BACKGROUND AND MOTIVATION

In order to provide privacy on on-demand information PPIB has been introduced. The brokers are responsible for user authentication and query forwarding. The coordinators formed in tree based structure and they are used for enforcing access control. The coordinators may be sometimes corrupted and private information can be easily inferred by attackers. In order to prevent from the data from the attackers two novel approaches has been included. They are automaton segmentation and query segment encryption. In this paper, mainly two attacks has been discussed and providing the

solution for overcome those attacks. Thus PPIB provides better protection on private information between inter organizations.

III. 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. In a p2p system, queries are initiated at various peers. These queries may require data that are located at a large number of peers distributed over the system. Tradition- ally, distributed systems use centralized or distributed indexes (catalogs) to store information about the location of data. For query processing, the indexes are consulted and the queries are sent to the appropriate nodes and evaluated there. Maintaining indexes in p2p systems poses additional requirements. In particular, indexes in p2p systems must support frequent updates, as peers join and leave the system constantly. Furthermore, the indexes need to be highly scalable, since the number of peers reaches Internet-scale, while in traditional distributed systems, the number of participating nodes is much smaller and controlled. Content-based communication is a communication service whereby the flow of messages from senders to receivers is driven by the content of the messages, rather than by explicit addresses assigned by senders and attached to the messages. Using a content-based communication service, receivers declare their interests by means of selection predicates, while senders simply publish messages. The service consists of delivering to any and all receivers each message that matches the selection predicates declared by those receivers.

A. 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,

The Automaton Segmentation Algorithm: In the context of distributed information brokering, multiple organizations join a consortium and agree to share the data within the consortium. While different organizations may have different schemas, we assume a global schema exists by aligning and merging the local schemas. Thus, the access control rules and index rules for all the organizations can be crafted following the same shared schema and captured by a global automaton, the global QBroker(query broker). The key idea of the automaton segmentation scheme is to logically divide the global automaton into multiple independent yet connected segments, and physically distribute the segments onto different brokering servers.

Algorithm:
deploySegment()
Input: Automaton State S
Output: Segment Address: addr
1: for each symbol k in S:StateT ransT able do
2: addr=deploySegment(S:StateT ransT able(k):nextState)
3: DS=createDummyAcceptState()
4: DS:nextState addr
5: S:StateT ransT able(k):nextState DS
6: end for
7: Seg = createSegment()
8: Seg:addSegment(S)
9: Coordinator = getCoordinator()
10: Coordinator:assignSegment(Seg)
11: return Coordinator:address

IV. THE PROBLEM

A. Problem Definition

Conceptually, IBS is a peer-to-peer overlay network consisting of data servers, brokering components, and end users. Applications on top IBS always involve some sort of consortium among a set of data owners (or organizations). While expressing a strong need of cross-organizational information sharing, data owners in such a consortium still expect to remain as much autonomous as possible. As a result, data owners collect data independently, and manage it in their local data servers. Data is not poured into some center data warehouse or replicated in distributed databases. Instead, data servers send metadata about their data objects distribution as well as access control rules to the consortium, which will further assign them to brokers to help information brokering. Traditional information sharing approaches always assume the use of trustable servers, such as the central data warehousing server or database servers. However, the honest or semi-honest assumptions (e.g., honest-but-curious assumption as adopted in [2]) may not hold for brokers. In practice, they may either be abused by insiders or compromised by outsiders. It is obvious that the brokers become the most vulnerable privacy breach of a IBS, which leads to inevitable security and privacy risks. On one hand, the survival of information brokering depends on the trust of brokers to enforce authentication, access control as well as query forwarding, while on the other hand, failing to provide proper protection of information released in this process may create circumstances that harm the privacy of user, data and the system. The problem has been mainly created by the attackers. These attackers are external attackers who eavesdrop the communication. By the use of corrupted coordinators they infer the sensitive information from queries which are forwarding between the brokers. There are three types of stakeholders mainly data owners, data providers and data requestors. The information which they are using may be different from others. The attackers mainly use two different type of attacks they are attribute –correlation attack and inference attack.

B. Attribute-Correlation Attack

This attack is fully based on the predicates. All information is private and sensitive. An attacker interrupts the query with multiple predicates to infer the information. If the predicates are matched with the information the entire query has been inferred.

C. Inference Attack

Here the attackers will infer the sensitive information by guessing the query. If the guess matches the forwarded query then that query will be inferred. Thus the information has been revealed by the external attackers.

V. PROPOSED WORK

A. 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 as shown in Fig.2.

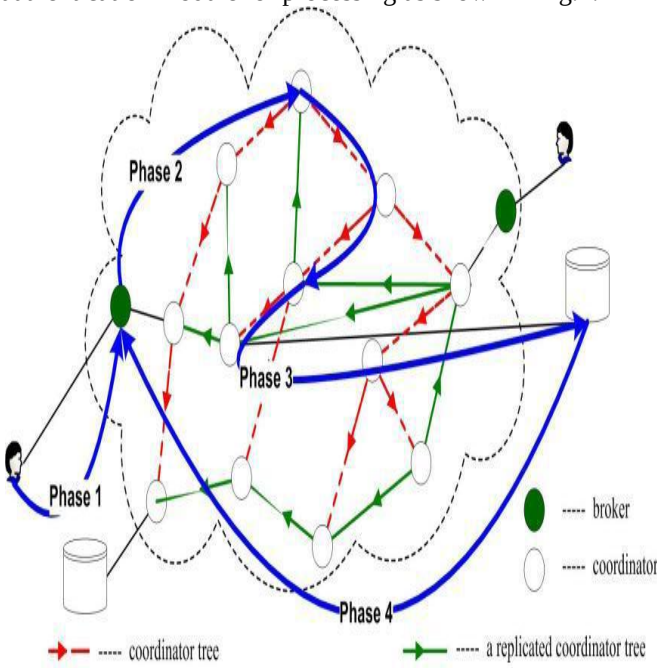

Fig. 2. The four phases of Query brokering process.

Phase 1: A user needs to authenticate himself 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.

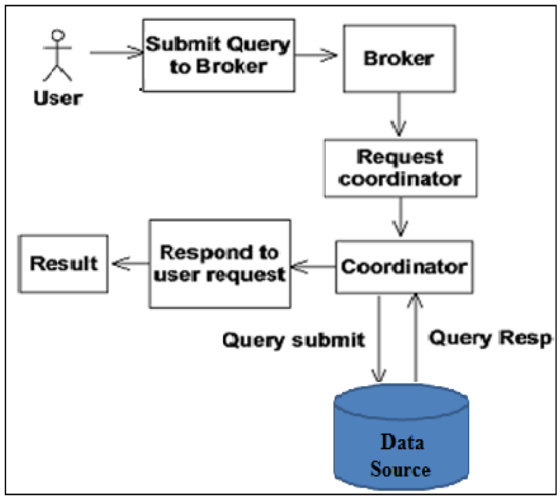

Fig.3. System Architecture.

The implementation is achieved throughout approach for Regional Health information Organization (RHIO) as a case study as shown in Fig.3. There are four modules are as follows.

- **Admin Module:** Admin performs critical roles in registration of data owners and users, brokers, coordinators and organization in DIBS.He also manages the database.
- **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.
- **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.
- **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.

VI. EXPERIMENTAL RESULT

PPIB system has implemented through two different processes. The file has been selected by the client to send to the server. The stakeholder may be data owner, data receiver or data sender. The selected files send to the server or destination location without revealing the data location. First the file is spited using query segmentation and each segment is encrypted using the automata segmentation algorithm. At the receiver end using the same decrypt key the file may be opened. The spitted segment is merged to reassemble the same file. Using this process the fake files can be identified.

The intruders or attackers may not able to corrupt the files. The original file and the fake files can be identified.

VII. CONCLUSION

In this paper, PPIB has been introduced to preserve privacy in information brokering. PPIB provides security and query forwarding scheme for privacy protection. PPIB integrates security enforcement and query forwarding with protection. PPIB is efficient and scalable. In future, the next step is to provide an automatic scheme that does dynamic site distribution. Also, to minimize the participation of the administrator node. Also the access control mechanism can be included. The next goal is to make PPIB self-reconfigurable. Finally, we plan to minimize (or even eliminate) the participation of the administrator node, who decides such issues as automaton segmentation granularity. A main goal is to make PPIB self-reconfigurable.

VIII. REFERENCES

[1] 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," Journal of AHIMA 77, pp. 64A–D, January 2006.

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

[3] 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.

[4] 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.

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

[6] N. Koudas, M. Rabinovich, D. Srivastava, and T. Yu, "Routing XML queries," in ICDE '04, p. 844, 2004.

[7] G. Koloniari and E. Pitoura, "Peer-to-peer management of XML data: issues and research challenges," SIGMOD Rec., vol. 34, no. 2, 2005.

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

[9] 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.

[10] 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.

[11] D. L. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," Communications of the ACM, vol. 24, no. 2, 1981.

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

[13] M. Genesereth, A. Keller, and O. Duschka, "Informaster: An information integration system," in SIGMOD, (Tucson), 1997.

[14] I. Manolescu, D. Florescu, and D. Kossmann, "Answering XML queries on heterogeneous data sources," in VLDB, pp. 241–250, 2001.

[15] J. Kang and J. F. Naughton, "On schema matching with opaque column names and data values," in SIGMOD, pp. 205–216, 2003.

[16] I. Stoica, R. Morris, D. Liben-Nowell, D. Karger, M. Kaashoek, F. Dabek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup protocol for Internet applications," in IEEE/ACM Transactions on Networking,
vol. 11 of 1, 2003.

[17] 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 CIDR, pp. 28–43, 2005.

[18] O. Sahin, A. Gupta, D. Agrawal, and A. E. Abbadi, "A peer-to-peer framework for caching range queries," in ICDE, 2004.

[19] A. Carzaniga, M. J. Rutherford, and A. L. Wolf, "A routing scheme for content-based networking," in Proc. of INFOCOM, 2004.

[20] Y. Diao, S. Rizvi, and M. J. Franklin, "Towards an Internet-scale XML dissemination service," in VLDB Conference, (Toronto), August 2004.

Author's Profile:

A.Leelavathi had Received her M.Tech in Computer science and Engineering from JNTUK in 2010, finished M.Sc. (Computer science) from Andhra University in 2003, and B.Sc (Computers) from Andhra University in 2001 . At Present, working as an assistant professor in Sri vasavi Engineering College ,Pedatadepalli from 2006. Before that, worked as a Teaching assistant, Lecturer, Assistant professor, with Department of Computer Science in various colleges. Participated in workshops and conducted many campus selection Technical training programs for students. My name was printed on back side cover page of text book titled "Programming in C" 2nd Edition by author Reema Thareja from Oxford publications (ISBN 0-19-945614-3) for submission of feedback and topic wise comments and objectives for 1st Edition textbook. Interested areas are object Oriented Programming(C++,Java) and Designing .

K.HariGangaBhavani Pursuing Master of Computer Applications in Sri Vasavi Engineering College, Pedatadepalli, Tade-palligudem, West Godavari District, Affiliated to JNTUK.