Indian Journal of Communications Technology and Electronics (IJCTE)
Vol.2.No.1 2014pp 18-21.
available at: www.goniv.com
Paper Received :05-03-2014
Paper Published:28-03-2014
Paper Reviewed by: 1. John Arhter 2. Hendry Goyal
Editor : Prof. P.Muthukumar

PRIVACY PRESERVING IN XML INFORMATION ROKERING WITH AUTOMATON AND QUERY SEGMENTATION

K.Aishwarya, K.Usha

ABSTRACT

Information Brokering System (IBS) adopt a peer-to-peer overlay has been proposed to support information sharing among loosely federated data sources. An XML brokerage system is a distributed XML database system that comprises data sources and brokers which hold XML documents and document distribution information.The problem of privacy protection in Information brokering process on two attacks, attribute-correlation attack and inference attack. To overcome this problem apply two techniques, Automaton segmentation and Query segment encryption which segments the query brokering automata and encrypt corresponding query segments. To enforce access control routing decision making is decoupled into multiple correlated tasks. With comprehensive analysis on privacy, end to- end performance, and scalability, show that the proposed system can integrate security enforcement and query routing while preserving system-wide privacy that concerns costs and performance, while access control is a security issue that concerns information confidentiality .Information brokerage systems view or handle query brokering and access control.

Index Terms- Access control, information sharing, privacy.

1. INTRODUCTION

Information brokering systems (IBSs) have been proposed to connect large-scale loosely federated data sources via a brokering overlay, in which the brokers make routing decisions to direct client queries to the requested data servers. Many existing IBSs assume that brokers are trusted and thus only adopt server-side access control for data confidentiality. The privacy of data location and data consumer can still be inferred from metadata (such asquery and access control rules) exchanged within the IBS, but little attention has been put on its protection.

It is suitable for many newly emerged applications, such as healthcare or law enforcement information sharing, in which organizations share information in a conservative and controlled manner due to business considerations or legal reasons. Take healthcare information systems as example. Regional Health Information Organization (RHIO) and aims to facilitate access to and retrieval of clinical data across collaborative healthcare providers that include a number of regional hospitals, outpatient clinics, payers, etc. Data provider, a participating organization would not assume free or complete sharing with others, since its data is legally private or commercially proprietary, or both. Instead, it requires full control over the data and the access to data.

Sharing a complete copy of the data with others or pouring data into a centralized repository becomes impractical. To address the need for autonomy, federated database technology to manage locally stored data with a federated DBMS and provide unified data access. The centralized DBMS still introduces data heterogeneity, privacy, and trust issues. While being considered a solution between sharing nothing and sharing everything, peer-to-peer information sharing framework essentially need to establish pairwise client-server relationships between each pair of peers, which is not scalable in large scale collaborative sharing.

Databases of different organizations are linked through a set of brokers, and metadata (e.g., data summary, server locations) are pushed to the local brokers, which further advertise the metadata to other brokers. Queries are sent to the local broker and routed according to the metadata until reaching the right data server(s). A large number of information sources in different organizations are loosely federated to provide an unified, transparent, and on-demand data access Information brokering system is a peer-to-peer overlay network consisting of data servers, brokering components, and end usersapplications adopt 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. The 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.

2. RELATED WORK

Information Brokering System (IBS) always involve some sort of consortium among a set of organizations. Databases of different organizations are connected through a set of brokers, and metadata (e.g. data summary, server locations) are “pushed” to the local brokers, which further “advertise” (some of) the metadata to other brokers. Queries are sent to the local broker and routed according to the metadata until reaching the right data server(s). In this way, a large number of information sources in different organizations are loosely federated to provide a unified, transparent, and on-demand data access. While the IBS approach provides scalability and server autonomy, privacy concerns arise, as brokers are no longer assumed fully trustable – the broker functionality may be outsourced to third-party

- The brokers are mainly responsible for user authentication and query forwarding.
- 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 prevent curious or corrupted coordinators from inferring private information, we design two novel schemes

- **Automaton Segmentation**
- **Query Segment Encryption**

Global schema & PPIB components registration

Global organization, having global schema, acts as a consortium, for different organization that belongs to same field, and agree to share their data as global data. Here, a standard schema, known as global schema, is provided for the organization. So, different organization having different schema register with global organization and shares the global schema.

PPIB components such as brokers, coordinators register with Information Brokering

providers and thus vulnerable to be abused by insiders or compromised by outsiders.

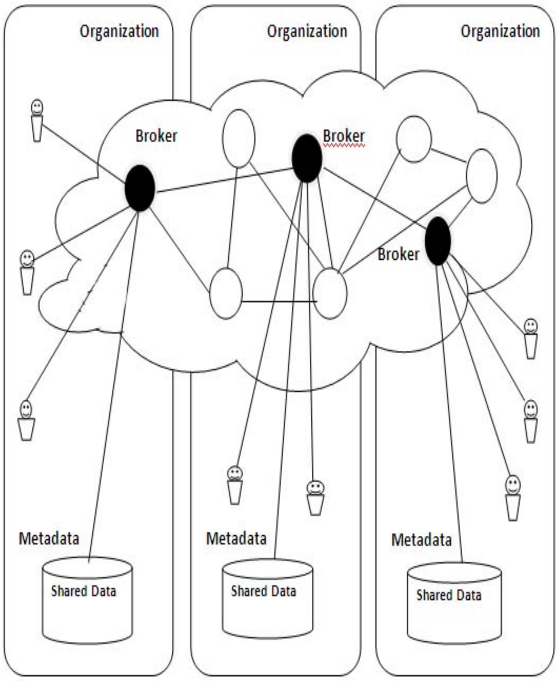

Fig1 Architecture

3. PROPOSED WORK

In this article, we present a general solution to the privacy-preserving information sharing problem. First, to address the need for privacy protection, we propose a novel IBS, namely Privacy Preserving Information Brokering (PPIB). It is an overlay infrastructure consisting of two types of brokering components, brokers and coordinators.

These schemes segments the query brokering automata and encrypt corresponding query segments so that routing decision making is decoupled into multiple correlated tasks for a set of collaborative coordinators. While providing integrated in network access control and content-based query routing, 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”, etc. PPIB provides comprehensive privacy protection for on-demand information brokering, with insignificant overhead and very good scalability.

System (IBS). Requestor registers with corresponding brokers, who acts as the entrance to the IBS. Coordinator send request to Central Authority to join the system.

Central Authority

The CA is assumed for off-line initiation and maintenance. With the highest level of trust, the CA holds a global view about all the rules and plays a critical role in automaton segmentation and key management except the query session keys created by the user; the other keys are generated and maintained by the CA. The data servers are treated as a unique party and share a pair of public and private keys, while each of the coordinators has its own pairs of level key and commutative level key. Along with the automaton segmentation and deployment process, the CA creates key pairs for coordinators at each level and assigns the private keys with the segments. The level keys need to be revoked in a batch once a certificate expires or when a coordinator at the same level quits the system.

Query routing

Data servers and requestors from different organizations connect to the system through local brokers. Brokers are interconnected through coordinators. A local broker functions as the “entrance” to the system. It authenticates the requestor To join the system, a user needs to authenticate

himself to the local broker. After that, the user sends XML query with each segment encrypted by the correspondingpublic level keys, and a unique session key is encrypted with the public key of the data servers toencrypt the reply data.Besides authentication, the major task of thebroker is metadata preparation. It retrievestheauthenticated user to attach to the encrypted query, it creates a unique for each query, and attachesand its own address to the query for dataservers to return dataUpon receiving the encrypted query, the coordinators follow automaton segmentation scheme and querysegment encryption scheme to perform access control andquery routing along the coordinator tree. At the leaf coordinator, all querysegments should be processed and reencrypted by thepublic key of the data server. If a query is denied access, a failure

message with will be returned to the broker, then the data server receives a safequery in an encrypted form. After decryption, the data server evaluates the

and hides his identity from other PPIB components. It forwards the requestor query to root coordinator. The coordinator process the query against its automaton segment assigned to it. After successful processing, it sends the query to the child coordinators for further processing. If denied, it sends the failure message the corresponding broker.

Query processing

Finally, the data server receives the processed query in an encrypted form. After decryption, the data server evaluates the query and returns the data, encrypted by KQ, to the broker that originates the query.

4. RESULT ANALYSIS

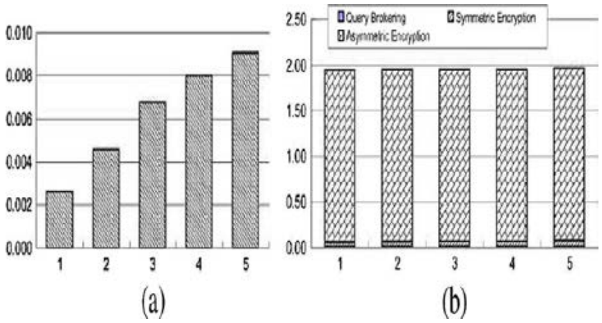

Fig 2(a)Average query brokering time
(b) Average encryption time

query and returns the data to the broker that originates the query.

5. CONCLUSION

The information brokering systems suffer from a spectrum of vulnerabilities associated with user privacy, data privacy, and metadata privacy. propose PPIB, a new approach to preserve privacy in XML information brokering. Through an innovative automaton segmentation scheme, in-network access control, and query segment encryption, PPIB integrates security enforcement and query forwarding while providing comprehensive privacy protection, that it is very resistant to privacy attacks. End-to-end query processing performance and system scalability are also evaluated and the results show that PPIB is efficient and scalability

REFERENCES

[1] W. Bartschat, J. Burrington-Brown, S. Carey, J. Chen, S.Deming, andS. 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.

[2] A. P. Sheth and J. A. Larson, “Federated database systems for managingdistributed, heterogeneous, and autonomous databases,” *ACMComput. Surveys (CSUR)*, vol. 22, no. 3, pp. 183–236, 1990.

[3] L. M.Haas, E. T. Lin, andM.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, “CoolStreamingDONet:A data-driven overlay network for efficient live media streaming,” in
Proc. IEEE INFOCOM,Miami, FL, USA, 2005, vol. 3, pp. 2102–2111.

[5] A. C. Snoeren, K. Conley, and D. K. Gifford, “Mesh-based contentrouting using XML,” in *Proc. SOSP*, 2001, pp. 160–173.

[6] N. Koudas, M. Rabinovich, D. Srivastava, and T. Yu, “Routing XMLqueries,” in *Proc. ICDE’04*, 2004, p. 844.

[7] 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.

[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.