Asian Journal of Information Science and Technology (AJIST)
and Instumentation Engineering (IJAREEIE)
Vol.2.No.1 2014 pp 37-41.
available at: www.goniv.com
Paper Received :08-03-2014
Paper Accepted:22-03-2013
Paper Reviewed by: 1. R. Venkatakrishnan 2. R. Marimuthu
Editor : Prof. P.Muthukumar

ENHANCING PRIVACY FOR LOOSELY FEDERATED DATABASE IN INFORMATION BROKERING SYSTEM

Gowri Shankar.S[1], Ida.F[2]
Computer science and Engineering
GKM College of Engineering andTechnology,
New Perungalathur.
Tamil Nadu, India.
[1]gowrishankar0710@gmail.com [2]idafrank2001@yahoo.com

ABSTRACT

This paper proposes privacy preserving technique in information brokering system. Information Brokering system which is widely used in western countries for retrieving data from an loosely federated database(i.e.,Regional health information organizations (RHIOs)). It includes automaton segmentation and query segment encryption. So the access control and privacy has been enhanced from existing IBS. The queries are in the form of XML Schema. It has been segmented into nodes which does the pre-encryption to make encrypted form. This technique provides a server side encryption does post-encryption which exhibits comprehensive security and this approach enforced security while query routing. It designed with automatic scheme that does dynamic site distribution.

***Index Terms*—**Information Sharing, access control, query routing, encryption.

1. INTRODUCTION

In recent years there is an increasing need for inter-organizational information sharing to facilitate extensive collaboration. While many efforts have been devoted to reconcile data heterogeneity and provide interoperability, the problem of balancing peer autonomy and system coalition is still challenging.

Multiple divisions cooperate within large multinational enterprise as well. For example, in GM, to maintain a proper stock level of parts, people in supply management division need to check the sale information (of car models) gathered and managed by sales people world-wide. In such information sharing systems, the data gathered by a specific division are typically stored and maintained in a database local to the division, but the needs to access the data may potentially come from any remote division.

Mediation and federation based information brokering technologies have been proposed to tackle the challenges like query brokering under heterogeneity, location discovery and secure information access. In particular, recent eXtensible Markup Language (XML) has become a promising solution by integrating incompatible data while preserving semantics. An XML-based information brokerage system comprises data sources and brokers which, respectively, hold XML documents and document distribution information. In such systems, databases can be queried through brokers with no schema-relevant or geographical difference being noticed.

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 providers and thus vulnerable to be abused by insiders or compromised by outsiders. 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. The brokers, acting as mix anonymizer 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 nondeterministic finite automata—the query brokering automata. To prevent curious or corrupted coordinators from inferring private information, we design two novel schemes to segment 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. Experimental results show that PPIB provides comprehensive privacy protection for on-demand information brokering, with insignificant overhead and very good scalability.

The work group identified the main purpose for forming a RHIO as facilitating information sharing among enrolled members of the RHIO using common, nonproprietary standards for data content and exchange over existing networks
and the Internet. The main goals in sharing patient-specific data are to:
1. Improve healthcare delivery by providing immediate, secure, confidential exchange of health information between authorized users
2. Enable providers and patients to make decisions based on near real-time access to health information
3. Provide warning and reminders at point of care
4. Reduce medical errors
5. Prevent adverse drug reactions
6. Encourage participation of patients in their own healthcare and chronic disease management
7. Allow patients, payers, and providers to evaluate quality of healthcare and to make informed choices in where
and from whom they obtain care

This technique extends the static partitioning algorithm to select dynamic data distribution which can further improve the performance of the resulting parallel program.

2.OBJECTIVE

The objective of this work is to implement privacy of multiple stakeholders involved in the information brokering process. With comprehensive security analysis and experimental results this work should provide very resistant to privacy attacks.

The main objective of this work to builds two countermeasure schemes automaton segmentation and query segment encryption to securely share the routing decision-making responsibility among a selected set of brokering servers. This approach provides integrated security enforcement with query routing to provide system-wide security. Also this work provides End-to-end query processing performance and system scalability, so PPIB is efficient and scalable.

4. RELATED WORK

L. M. Haas E. T. Lin and M. A. Roth[1] introduce database federation which employs a database engine to create a virtual database from several possibly many heterogeneous and distributed data stores. This technique handles Multidata-set integration and multi-operation integration techniques. It also handles multiserver integration and transactional integration. This work does not handle asynchrony everywhere.

Mubashar Mushtaq and Toufik Ahmed[2] develops a streaming mechanism which is receiver-centric where receiver peer selects a number of sender peers from the overlay networks to receive media contents. Hybrid overlays organization mechanism is helpful to enhance the overall QoS. A single peer might not be able to meet the requirements of any one request. Alex C. Snoeren , Kenneth Conley, and David K. Gifford[3] implements Diversity Communication Protocol, It Provides a way for peers to use redundant packet transmissions to reduce latency and improve reliability.

It implements Mesh-based overlay networks to achieve better latency performance than tree-based approaches. Guoli Li, Shuang Hou, Hans-Arno Jacobsen[4] makes XML documents from publishers are forwarded along these routing paths to subscribers with matching XPEs. By defining and exploiting covering and merging relations for XPEs, a compact routing table results. This techniques improve the routing time at each broker by up to 85% in the most favorable cases. Fengjun Li, Peng Liu and Dongwon Lee[5] by constructing a QFilter for each role and sit it in the brokers. In-Network Access Control approach has been developed, which pulls access control out of data sources towards the users to enjoy all the benefits of IAC architecture.

Dongwon Lee, and Chao-Hsien Chu[6] developed 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. Ion Stoica and Robert Morris[7] introduce a Chord which adapts efficiently as nodes join and leave the system, and can answer queries even if the system is continuously changing.

In this analysis, simulations, and experiments show that Chord is scalable with communication cost and the state maintained by each node scaling logarithmically with the number of Chord nodes. David Wagner and Adrian Perrig[8] develop provable secrecy for encryption, in the sense that the untrusted server cannot learn anything about the plaintext when only given the ciphertext. It provide query isolation for searches untrusted server cannot learn anything more about the plaintext than the search result.

Cengiz Örencik and Erkay Sava¸s[9] increases the security of the keyword search scheme while still satisfying efficient computation and communication requirements. The majority of previous works are not efficient for assumed scenario where documents are large files.

Panos Skyvalidas and Evaggelia Pitoura[10] introduce a simple yet efficient replication method has been implemented that is based on replication routing indexes. A replication routing index for a node is a path-based XML index that summarizes access information for each of the links of the node.

4. PPIB

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

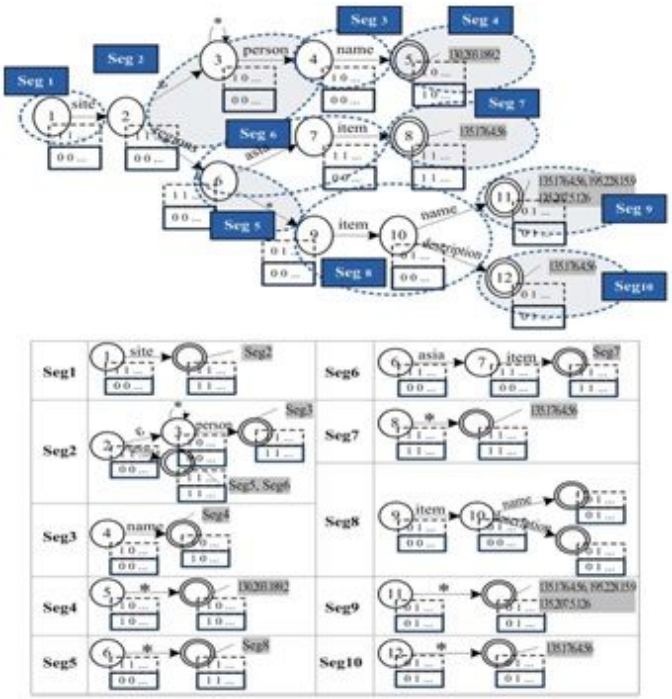
i) The brokers are mainly responsible for user authentication and query forwarding.

ii) The coordinators concatenated in a tree structure to enforce access control and query routing based on the embedded non-deterministic finite automata, which is called as query brokering automata.

To prevent curious or corrupted coordinators from inferring private information, this work has been designed by two novel schemes

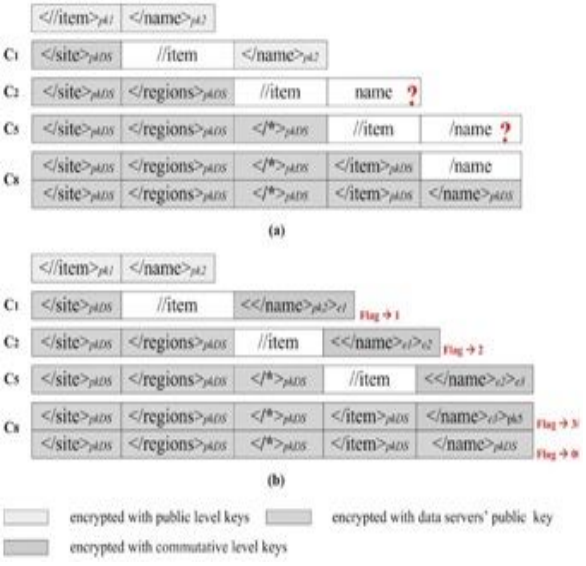
a) Automaton Segmentation

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 key idea of automaton segmentation scheme is to logically divide the global automaton into multiple independent yet connected segments, and physically distribute the segments onto different brokering components, known as coordinators.



b) Query Segment Encryption

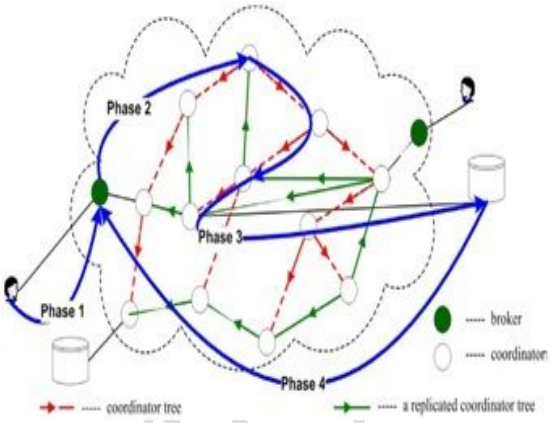
Informative hints can be learned from query content, so it is critical to hide the query from irrelevant brokering servers. In traditional brokering approaches, it is difficult, if not impossible, to do that, since brokering servers need to view query content to fulfill access control and query routing. Fortunately, the automaton segmentation scheme provides new opportunities to encrypt the query in pieces and only allows a coordinator to decrypt the pieces it is supposed to process. The query segment encryption scheme proposed in this work consists of the pre-encryption and post-encryption modules, and a special commutative encryption module for processing the double-slash ("//") XPath step in the query.



Overall PPIB:

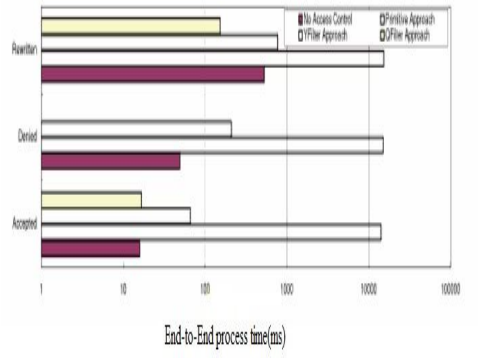
PPIB shows that Data servers and requestors from different organizations connect to the system through local brokers. Brokers are interconnected through coordinators. A local broker functions as the "entrance" to the system. It authenticates the requestor and hides his identity from other PPIB components. It would also permute query sequence to defend against local traffic analysis. Coordinators are responsible for content-based query routing and access control enforcement. With privacy-preserving considerations, user cannot let a coordinator hold any rule in the complete form.

A novel automaton segmentation scheme to divide (metadata) rules into segments and assign each segment to a coordinator. Coordinators operate collaboratively to enforce secure query routing. A query segment encryption scheme is further proposed to prevent coordinators from seeing sensitive predicates. The scheme divides a query into segments, and encrypts each segment in a way that to each coordinator enroute only the segments that are needed for secure routing are revealed. In this work a separate central authority handles key management and metadata maintenance.



5. PERFORMANCE ANALYSIS

End-to-End Query Processing Time:



The above figure shows the results of End-to-End Query which the sender forwards a query and receives the relevant data. This shows performance of the proposed PPIB.

6. CONCLUSION

In this work different organization having different schema register with global organization and shares the global schema has been developed. Those organization send request to join the system. For each and every organization they can add broker within the organization. PPIB components such as brokers, coordinators register with Information Brokering 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. 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. Brokers have to inter-connect through coordinators. A local broker authenticates the requestor and hides his identity from other PPIB components. It forwards the requestor query to root coordinator. After successful processing, it sends the query to the child coordinators for further processing. If denied, it sends the failure message the corresponding broker. 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. To design an automatic scheme that does dynamic site distribution.

.

REFERENCES

[1] 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.

[2] X. Zhang, J. Liu, B. Li, and T.-S. P. Yum, "Cool Streaming/DONet: A data-driven overlay network for efficient live media streaming," in *Proc. IEEE INFOCOM*, Miami, FL, USA, 2005, vol. 3, pp. 2102–2111.

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

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

[5] 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*, Taichung, Taiwan, 2006, pp. 252–259.

[6] 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*, 2007, pp. 508–518.

[7] 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," *IEEE/ACM Trans. Netw.*, vol. 11, no. 1, pp. 17–32, Feb. 2003.

[8] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches on encrypted data," in *Proc. IEEE Symposium on Security and Privacy*, 2000, pp. 44–55.

[9] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, "Secure ranked keyword search over encrypted cloud data," in *Proc. ICDCS'10*, Genoa, Italy, pp. 253–262.

[10] P. Skyvalidas, E. Pitoura, and V. Dimakopoulos, "Replication routing indexes for XML documents," in *Proc. DBISP2P Workshop*, Vienna, Austria, 2007.