International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622
International Conference on Humming Bird (01st March 2014)

RESEARCH ARTICLE OPEN ACCESS

Distributed Information Sharing Using Privacy Preserving Information Brokering

Praisy Nalamisha.N, PG Scholar, S.Agnes Joshy, Assistant Professor

* Department of Information Technology, Francis Xavier Engineering College
Vannarpettai, Tirunelveli. praisynalamisha@gmail.com, 9894202908
**Department of Information Technology, Francis Xavier Engineering College
Vannarpettai, Tirunelveli., sagnesjoshy@gmail.com

Abstract
Information sharing has been increased nowadays in organizations via on-demand access. There is an demand for inter organizational information sharing. Large-scale loosely federated data sources are connected through brokering overlay by Information Brokering Systems (IBS). Brokers are used to make routing decisions to direct client queries to the requested data servers. An approach to preserve privacy in information brokering process of multiple shareholders by Privacy Preserving Information Brokering (PPIB) is proposed. PPIB has three components: brokers, coordinators and central authority. The two privacy attacks are used namely attribute-correlation attack and inference attack. Decision making among the selected set of brokering servers have been achieved by automation segmentation and query segmentation encryption. This approach integrates security with query routing to provide system wide security. In order to preserve privacy is to divide and allocate the functionality to brokering components in a way that no single encrypted segment can make a meaningful inference from the information disclosed to it.
Index Terms—Information Brokering, PPIB, IBS.

I. INTRODUCTION

Information has been nowadays collected by many different organizations and they are used between the organizations. There is an increasing need for inter organizational information sharing with collaboration. There is always a need for peer autonomy. The existing system either work on query answering model or distributed database model in which all peers are managed by centralized DBMS with little autonomy.

In the case of sensitive and autonomous data providers centralized DBMs is not suitable. Hence a data centric overlay consisting of data sources and brokers are needed. Brokers make the routing decisions based on the queries. The system providing data access through a set of brokers is known as Information Brokering System(IBS).

In IBS databases of different organizations are connected through the set of brokers. The metadata such as data location and summary are transferred to the brokers. The client queries are submitted to the local brokers and they are forwarded to the data servers with the help of metadata provided. Thus IBS provide an on-demand data access with transparency.

However IBS provides server autonomy, privacy conflicts occurs. Here brokers are not trusted fully because attackers may outsource the information which are provided by clients.

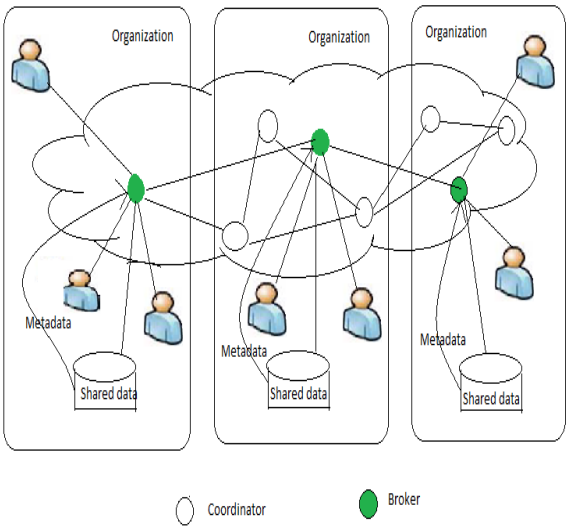

Fig.1.PPIB structure

To overcome this privacy measures a novel approach of Privacy Preserving Information Brokering (PPIB) has been proposed. It mainly consists of two components namely brokers and coordinators. PPIB provides privacy preserving Information with on-demand access and good scalability.

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. THE PROBLEM

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.

A. 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.

B. 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.

C. Solution

To overcome these attacks Privacy Preserving Information Brokering (PPIB) has been provided with brokers and coordinators. In order to preserve privacy no single query can make a meaningful inference.

IV. PRIVACY PRESERVING QUERY BROKERING

In the existing QBrokert has been used. But that QBroker is not fully trusted by data providers and requestors. Thus PPIB introduces two novel schemes automata segmentation and query segment encryption.

A. Automata Segmentation

Multiple organizations join together and share the data between them. Different organizations have their own goals and ideas. Thus global components are locally divided and forwarded to the coordinators. Thus the entire query must be divided into several parts and forwarded to the local coordinators. This phase includes segmentation, deployment and replication.

B. Query Segment Encryption

In this phase, the segmented query is encrypted by the coordinator which is supposed to process. It consists of pre-encryption and post-encryption modules. Here the coordinator uses the key to encrypt the query segment. The coordinator used the public key to encrypt. It only sees the small portion of the query that cannot be inferred. Other then central authority no one knows the global segmentation.

Once the query has been encrypted by the coordinator it has been send to the next coordinator. In that case the query must be prevented until it reaches its data server. Thus the post encryption has been handled ad the query has been successfully forwarded to the destination.

C. 4-Phases of PPIB

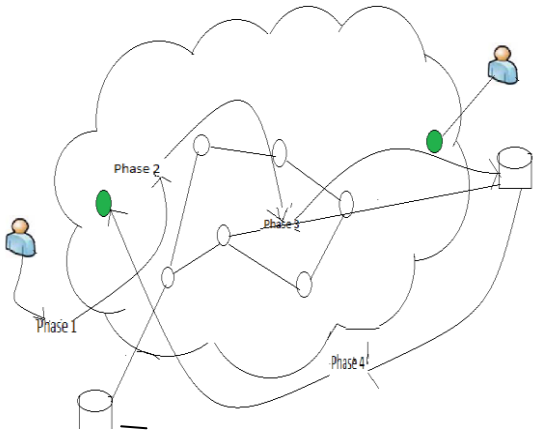

Fig.2. Phases of PPIB

1. Phase-1

User needs to authenticate to the local broker. Then user needs to submit the encrypted query with the public key.

2. Phase-2

In this phase broker needs to prepare the metadata. It creates the unique ID for each query and attaches its own address.

3. Phase-3

After receiving the encrypted query the coordinator follows the automata segmentation and query segment encryption. All query must be once again re-encrypted by the public key of data server.

4. Phase-4

In this phase the data server receives the safe query in encrypted form. After that the data server decrypts the query using the key.

V. SECURITY ANALYSIS

Attackers mainly infer the information while the query has been forwarding from one coordinator to another. Attackers in information brokering system can be classified into different types. They are mainly eavesdroppers, malicious brokers and malicious coordinators. Eavesdropper is an attacker who can identify the communication content done by the user.

The traffic while forwarding the query can be observed by global eavesdropper. The malicious broker himself deviates from the correct path and happens to reveal the sensitive information. Likewise the malicious coordinator also reveals some information by deviation from protocol.

Even the coordinator may not able to find the information because each segment has been encrypted by the key which is protected by the broker. Thus the security among the brokers and the coordinators are more protected. Thus analysis shows that PPIB is secure and scalable.

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.

REFERENCES

[1] M. Kudo, "Access-condition-table-driven access control for XML databases," in *Proc. ESORICS 2004*, 2004, pp. 17–32.

[2] S. Mohan, A. Sengupta, and Y. Wu, "Access control for XML: A dynamic query rewriting approach," in *Proc. IKM*, 2005, pp. 251–252.

[3] N. Qi and M. Kudo, "XML access control with policy matching tree," in *Proc. ESORICS 2005*, 2005, pp. 3–23.

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

[5] G. Skobeltsyn, "Query-Driven Indexing in Large-Scale Distributed Systems," Ph.D. Thesis, EPFL, Lausanne, 2009.

[6] P. Rao and B. Moon, "Locating XML documents in a peer-to-peer network using distributed hash tables," *IEEE Trans. Knowl. Data Eng.*, vol. 21, no. 12, pp. 1737–1752, Dec. 2009.

[7] 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.

[8] 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.

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

[10] 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.