IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 45-50
www.iosrjournals.org

Review on Enforcing Secure And Privacy Preserving Information Brokering In Distributed Information Sharing

Mr. Mukesh Kawatghare[1], Ms. Pradnya Kamble[2]
[1](Assistant Professor, Computer Technology, PCE Nagpur, India)
[2](Student, ME (WCC), PCE Nagpur, India)

ABSTRACT : *Today's organizations (e.g. enterprise, government agencies, libraries, "Smart" Home) raise increasing needs for information sharing via on-demand information access. A Information Brokering System (IBS) is a peer-to-peer overlay network that comprises diverse data servers and brokering components helping client queries locate the data server(s). Peer-to-peer (P2P) systems are gaining increasing popularity as a scalable means to share data among a large number of autonomous nodes. We study the privacy in Privacy-Preserving Information Brokering in Distributed Information Sharing through an innovative automaton segmentation scheme and query segment encryption and data management issues for processing XML data in a p2p setting, namely indexing, replication and query routing and processing.*
Keywords **-**automaton segmentation, query segment encryption, privacy, Access control, information sharing.

I. INTRODUCTION

Information sharing is becoming increasingly important in recent years, not only among organizations with common or complementary interests, but also within many field ranging from business to other agencies that are becoming ever more globalized and distributed. To provide efficient large-scale information sharing, to reconcile data heterogeneity and provide interoperability across geographically distributed data sources.

The systems work on two extremes of the spectrum: (1) in the query-answering model, peers are fully autonomous but there is no system-wide communication; so that user creates one-to-one client-server connections for information sharing; (2) in the distributed database systems, all the user lost autonomy and are managed by a unified DBMS. However, different types of applications often need different forms of information sharing. In particular, while some applications (e.g., stock price updating) would need a publish subscribe framework, the on-demand information access is more suitable for other applications [8].

As an example, imagine a future where many people have their DNA sequenced. A medical researcher wants to validate a hypothesis connecting a DNA sequence D with a reaction to drug G. People who have taken the drug are partitioned into four groups, based on whether or not they had an adverse reaction and whether or not their DNA contained the specific sequence; the researcher needs the number of people in each group. DNA sequences and medical histories are stored in databases in autonomous enterprises. [9]

As a data provider, a participant would not assume free or complete sharing with others, since its data is legally private or commercially proprietary, or both. Instead, it is required to retain full control over the data and access to the data.

In the sensitive data and autonomous data owners, a more practical and adaptable solution is to construct a data centric overlay [3], [4], including the data sources and a set of brokers helping to locate data sources for queries [6], [7]. Mechanisms to route the queries based on their content, which allows users to submit queries without knowing data or server location. In previous study [7], [8], such a distributed system providing data access through a set of brokers is referred to as Information Brokering System (IBS).This system provide scalability and server autonomy. In IBS infrastructure

given broker and coordinator, broker are no longer fully trustable. So, system may be abuse by insider or outsider.

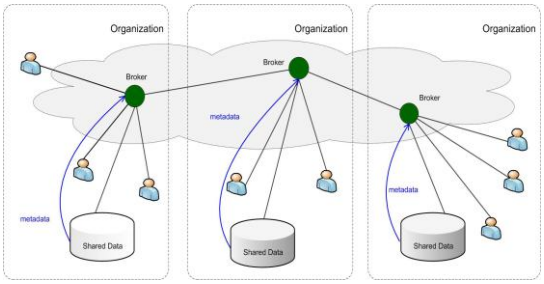

Fig.1. Overview of the IBS infrastructure.

II.PRIVACY- PRESERVING INFORMATION BROKERING

Privacy protection is need for the Information Brokering System (novel IBS), named Privacy Preserving Information Brokering (PPIB). PPIB has two type of brokering Component: (1) brokers and (2) co-ordinators. The brokering are mainly responsible for user authentication and query forwarding, the broker performs the role who can act between the Co-coordinator and the data Users. The request which is all submitted from the data user will be verified and thus it will be passed to the co-coordinator. The coordinators which are linked in a tree structure enforce access control and query routing based on the embedded nondeterministic finite automata also known as query brokering automata. The coordinators, each holding a segment of access control automaton and routing guidelines, are mainly responsible for access control and query routing. [8]

PPIB takes an innovator automaton segmentation approach to privacy protection. In particular, two critical forms of privacy, namely query content privacy and data object distribution privacy (or data location privacy), are enabled by a novel automaton Segmentation scheme, with a “little" help from an assisting query segment encryption scheme.

To prevent inquisitive or unserviceable coordinators from inferring private information, we design two novel schemes: (a) to segment the query brokering automata, and (b) to encrypt corresponding query segments. System will providing full capability to wage in network access control and to path queries to the right data sources, these two schemes ensure that inquisitive or unserviceable coordinator is not capable to collect sufficient information to guess privacy, like “which data need to be queried, where located and what are the policies to access data”. Privacy Preserving Information Brokering (PPIB) enables wide-ranging security and privacy protection for claimed information brokering, with minor overhead and major scalability.

III. SECURITY AND PRIVACY NEED FOR PPIB

In information brokering scenario, there are three types of entrepreneur, namely data owners, data providers, and data requestors. Each entrepreneur has its own privacy: (1) the privacy of a data owner (e.g. a patient) is identifiable data and the information keep together by this data (e.g. medical records). Data owners usually sign stiff privacy agreements with data providers to protect their privacy from unauthorized disclosure/user. (2) Data providers store collected data, and create two types of metadata, namely routing metadata and access control metadata. (3) Data requestors divulge identifiable and private information in the querying process. For example, a query process about AIDS or DNA treatment reveals the (possible) disease of the requestor.
Assume that for the brokers, two types of enemy, outside attackers and curious or corrupted brokering components. Outside attackers passively eavesdrop communication channels. Curious or corrupted brokering components follow the protocols be seemingly to accomplish their functions, others’ private information from the information disclosed in the querying process.

Data providers push routing and access control metadata to brokers [8], which also strut queries from requestors. Therefore, a curious or corrupted brokering server could: (1) learn query content and query location by impede a local query; (2) learn routing metadata and access control metadata from local data servers and other brokers; (3) learn data location from routing metadata it holds Although attacker may not obtain plaintext data over encrypted data, they can still learn query location and data location from eavesdrop. The attacks into two major classes: (1) the attribute-correlation attack and (2) inference attack.

Attribute-correlation attack: An attacker prevents a query, which typically contains several predicates. Each predicate describes a condition, which sometimes involves sensitive and private data (e.g. name, credit card number, etc.).

Inference attack: Attacker some techniques and result more than one other type of sensitive information so more sever, and further associates to learn explicit and implicit knowledge about entrepreneur

IBS work is designed with user and data privacy. Such privacy protection requirements, therefore a novel IBS, named as Privacy Preserving Information Brokering system (PPIB). As shown in Figure, PPIB contains a broker-coordinator overlay network, in which the brokers are amenable for onus transmission user queries to coordinators concatenated in tree structure while preserving privacy. The coordinators, each holding a segment of access control automaton and routing guidelines, are mainly responsible for access control and query routing.

IV. ARCHITECTURE OF PPIB

PPIB has three types of brokering components: (1) Brokers (2) Coordinators and (3) Central authority (CA). The key to defend privacy is to part the work on more than one components in such a way that more than one node can make a meaningful presumption from the information disclosed to it.
Figure 2 shows the architecture of PPIB. Through local brokers (green nodes in Fig) Data servers and requestors from different organizations connect to the system

Brokers: It is intercommunicating through coordinators (white nodes in Fig). A local broker functions as the "entry" to the system. It's responsible for authenticates requestors and hides their. It would also permute query sequence to defend against local traffic analysis.

Coordinators: It is responsible for content-based query routing and access control actuation. With privacy-preserving idea, coordinator cannot hold any rule in the complete form. Instead, a novel automaton segmentation scheme to divide (i.e. metadata) rules into segments and assign each segment to a coordinator. Coordinators operate collaboratively to enforce secure query routing.

Coordinator prevents from sensitive predicates, a query segment encryption scheme and automaton segmentation scheme, query divide into segment and encrypt it (each segment)

Central Authority (CA): It is responsible for key management and metadata maintenance.

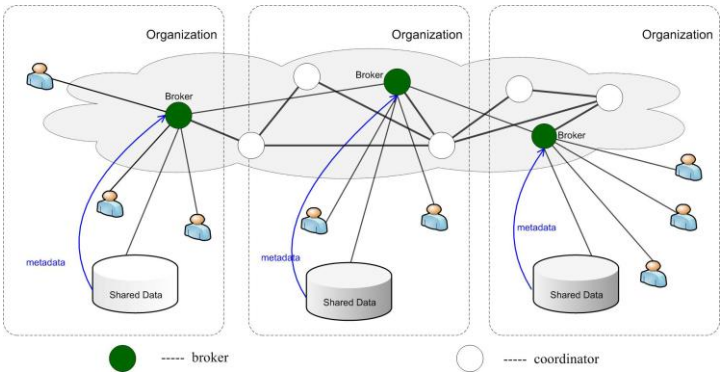

Fig.2. Architecture of PPIB

The architecture of the privacy preserving information brokering system is shown in Fig. 2, where users and data servers of more than one organizations are communicate via a Broker, coordinator overlay component. User requests for data by sending a XML query to the local broker, which further carry the query to the root of the coordinator tree. The query is processed along a path of the multiple organizations coordinator. The brokering process consists of 4 phases:

Phase 1: For join the system, a user needs to authenticate to the local broker. And the user submits encrypted segment an XML query by public level keys, and a unique session key Ks, data servers encrypted with the public key, to return data.

Phase 2: The major task of the broker is metadata preparation: (1) it extracts the role of the user authenticated and attaches it to the encrypted XML query; (2) it make a unique ID for each query, and attaches QID with its own address (as well as < Ks >pkDS) to the query so that the data server can directly return the data.

Phase 3: When the root of the coordinator tree receives the query and its metadata from a local broker, it follows schemes i.e. the automata segmentation scheme for segment the XML query and the query segment encryption scheme to perform access control and to route the query within the coordinator tree, until it reaches a leaf coordinator, which forwards the query to the related data servers.

Phase 4: In the final phase, the data server gets a safe query in an encrypted form. The data server evaluates the query and returns the data after decryption, encrypted by Ks, to the broker of the query.

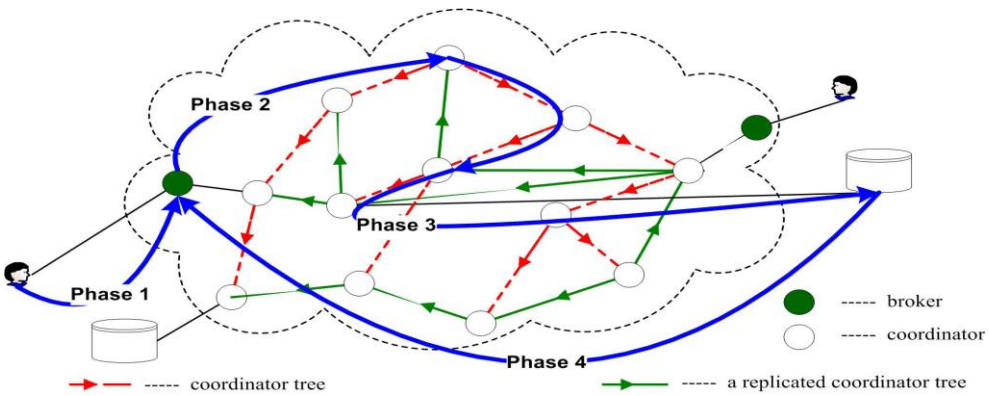

Fig. 3. Query brokering process in 4 phases.

V. APPLICATIONS

Information (Data) Brokers collect data and provide data mining services for various organizations, for example in the FBI, Credit Monitoring Services, DoD, etc. The companies are a high value target for social engineers as they contain huge amounts of information that could be used to further elevate. Because of relaxed regulations and federal laws much of our personal information is collected by government agencies and stored or managed by these Information Broker Companies.

Information brokering is suitable for many newly emerged applications, such as information sharing for healthcare or law enforcement, in which organizations share information in ailliberal and controlled manner, not only from business considerations but also due to legal reasons.

1) Healthcare information systems, such as Regional Health Information Organization (RHIO) [1], to facilitate retrieval of clinical data thereon collaborative health providers.
2) Law enforcement, for example young police officers, police academics, researchers agencies use information brokering technologies to share on demand data with other agencies and the public.

VI. EXISTING PROBLEM

In this system has some existing problem as like site distribution and load balancing. In PPIB, site distribution and load balancing are conducted in an ad-hoc manner.

PPIB can suffer from certain load imbalances due to data storing and query routing, load imbalance caused by these factors can be efficiently tackled without substantial performance degradation. However, no load balancing is considered and no explicit results showing query processing costs are reported. [11]. Load balancing of the load caused by resolving queries from caches is more crucial due to the high traffic it creates to supply query results compared to the metadata-index lookup.

Another problem is drawing an automatic scheme which performs dynamic site distribution. There is a need o consider several other factors such as the workload and trust level of each peer, and privacy disagreement between automaton segments. A scheme that can strike a balance among these factors is a point of consideration. Second, we would like to quantify the level of privacy protection achieved by PPIB. A plan to minimize or eliminate the participation of the administrator, whose role is decide some issues such as automaton segmentation granularity will also worked out. A primary intention is to build PPIB self-reconfigurable.

V. CONCLUSION

Privacy issues of user and data during the design stage is considered and concluded that existing information brokering systems suffer from a spectrum of vulnerabilities associated with user privacy, data privacy, and metadata privacy. In this paper, PPIB proposed architecture is discussed, a new approach to preserve privacy in XML information brokering. By using automaton segmentation scheme, within network access control and query segment encryption, PPIB put together security enforcement and query forwarding at the same time as providing comprehensive privacy protection. We claim that our analysis is very resistant to privacy attacks. Node-to-node query processing performance and system scalability are also evaluated and the results show that PPIB is efficient and scalable.

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] 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.
[4] A. C. Snoeren, K. Conley, and D. K. Gifford, "Mesh-based content routing using XML," in SOSP, pp. 160–173, 2001.
[5] G. Koloniari and E. Pitoura, "Peer-to-peer management of XML data: issues and research challenges," SIGMOD Rec., vol. 34, no. 2, 2005.
[6] 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.
[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, 2006.
[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 ACM CCS '07, pp. 508–518, 2007.
[9] R. Agrawal, A. Evfimivski, and R. Srikant, "Information sharing across private databases," in Proceedings of the 2003 ACM SIGMOD, 2003.
[10] S. Mohan, A. Sengupta, and Y. Wu, "Access control for XML: a dynamic query rewriting approach," in Proc. IKM, pp. 251–252, 2005.
[11] G. Skobeltsyn, Query-driven indexing in large-scale distributed systems. PhD thesis, EPFL, 2009.