Security Enforcement and Query Routing on Privacy Preserving Information Brokering System

Prof. Kiran Yesugade[1] Ketaki Thakar[2] Swanuja Mandhare[3]
[1]Professor
[1,2,3]Department of Computer Engineering
[1,2,3]Bharati Vidhyapeeth's College of Engineering for Women, Affiliated to University of Pune, Pune, India

Abstract— Nowadays in organizations information sharing has been increased via on-demand access. 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. Some of existing IBSs assume that brokers are trusted and thus only adopt server-side access control for data confidentiality. However, privacy of data location and data consumer can still be inferred from metadata (such as query and access control rules) exchanged within the IBS, but little attention has been put on its protection. With this the privacy concerns arise, as brokers are no longer assumed fully trustable – they may be abused by insiders or compromised by outsiders. For overcoming this, a novel IBS, named Privacy Preserving Information Brokering (PPIB) has been proposed. In this paper, we propose a novel approach to preserve privacy of multiple stakeholders involved in the information brokering process. PPIB has three components: brokers, coordinators and central authority. We are among the first to formally define two privacy attacks, namely attribute-correlation attack and inference attack, and propose two countermeasure schemes automaton segmentation and query segment encryption to securely share the routing decision-making responsibility among a selected set of brokering servers. The PPIB scheme is improved by supporting site distribution and load balancing mechanism. Workloads of peers and each peer's trust levels are integrated with the site distribution process. With the comprehensive analysis on scalable privacy and load balancing we show that the propose system can integrate security enforcement and query routing while preserving system wide privacy.

Key words: Automaton segmentation, Query segment encryption, Load balancing, Access control, information sharing

I. Introduction

Information has been nowadays collected by many different organizations and they are used between the organizations. Information sharing is becoming increasingly important in recent years, not only among organizations with complementary interests, but also within many fields range from business to other agencies that are becoming ever more globalized and distributed. To provide efficient large-scale information sharing, to accept data heterogeneity and provide interoperability across geographically distributed data sources, the problem of peer autonomy and system coalition is still challenging. 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 [1]. However, types of applications often need different forms of information sharing. In particular, while some applications (e.g., stock price updating) would need a publish subscribes framework, the on-demand information access is more suitable for other applications.

First, to support the need for privacy protection, we are proposing a novel IBS, which name is Privacy Preserving Information Brokering (PPIB). PPIB is an overlay infrastructure and consists of two types of brokering components, brokers and coordinators. The brokers, acting as mix anonymizer, they are mainly responsible for user authentication and query forwarding. The coordinators, arranged in a tree structure, they enforce access control and query routing based on the embedded nondeterministic finite automata (NFA)—the query brokering automata. For preventing 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 [3]. The proposed IBS by providing integrated in-network access control and content-based query routing, 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" The results show that PPIB provides comprehensive privacy protection.

The PPIB scheme is improved to support site distribution and load balancing mechanism. Peer workloads and trust level of each peer are integrated with the site distribution process [7]. The PPIB system is designed to perform data access under multiple data provider environment. The system performs data querying process using encrypted query model. Server selection and data access management operations are controlled by the brokers and coordinators.

II. Problem

In existing Information Brokering System (IBS), it is possible to hack the information with the help of corrupted coordinators. These coordinators can capture the sensitive information from queries which are forwarding between the brokers. There are two possible attacks as attribute – correlation attack and inference attack.

A. *Attribute –correlation attack:*

This type of attack is fully related to predicates. The predicates define the condition. This condition contains private and sensitive data e.g. name, SSN or credit card number, etc. If a query contains multiple predicates or composite predicate expressions, at that time attacker can “correlate” the corresponding attributes to infer sensitive information. If the predicates get matched with information then the entire query has been inferred. This attack is known as the attribute correlation attack.

Example 1: Suppose there is a patient Anne. She is shifted to the emergency room at California Hospital. Through a Medicare IBS, Doctor Bob fire queries to obtain her medical information. In this e.g., As Anne has the symptom of leukemia, the query has two predicates: name="Anne" and symptom="leukemia". In this situation corrupted broker con make possible guess by correlating two predicates in the query. These as “Anne has a blood cancer.

B. *Inference Attack:*

Several privacy issues occur when an attacker obtains more sensitive information. It associates them to study explicit and implicit knowledge about the stakeholders. In “implicit”, the attacker infers the sensitive information by “guessing”. For example, from the requestors query location (IP address) an attacker can guess the identity of a requestor. The identity of the data owner could be explicitly obtained from query content (e.g. name or SSN in the predicate). Attackers can also make use of publicly available information to obtain the sensitive information.

For example, if an attacker has the information about the data server which is located at a cancer research center, he can create the related queries to infer the cancer related information. There are three combinations of private information, and there related attacks: (1) From query location & data location, the attacker concludes information about who (i.e. a specific requestor) is interested in what (i.e. a specific type of data). (2) From query location & query content, the attacker infers knowledge about who is interested in what, or where who is, if the query has predicates describing one’s interests (e.g. symptom or medicine) or identifying a personnel (e.g. name or address). (3) From query content & data location, the attacker deduces which data server has which data.

III. EXISTING SYSTEM

In Existing Information Brokering System (IBS), it providing data access through a set of brokers.IBS contains no of organizations. Consider the diagram given below to understand the concept of Information Brokering System (IBS).

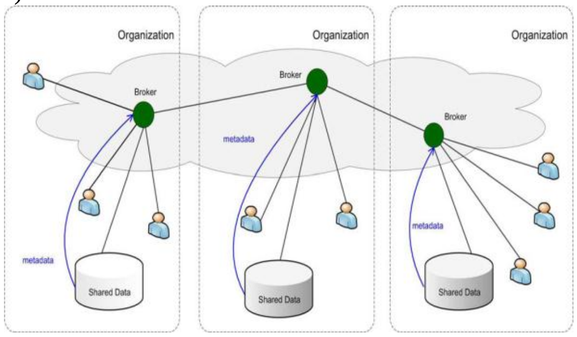

Fig. 1: Overview of the IBS infrastructure.

As shown in Fig. 1, it contains a set of organizations. Each of the organization has its own database. Through a set of brokers, and metadata (e.g., data summary, server locations) these databases are connected. The metadata are “pushed” to the *local brokers.* Which make this metadata available to other brokers without any constraint . Queries are sent to the local broker, until query reaches to right data server it is routed according to metadata. In such a way information sources of multiple organizations are loosely federated which provide an unified, transparent, and on-demand data access. But in Existing Information Brokering System (IBS), The brokers were not fully trustable. So there are the chances of inferring the private and sensitive information. Also the Existing Information Brokering System (IBS), was not handling the load of data providers.

IV. PROPOSED SYSTEM

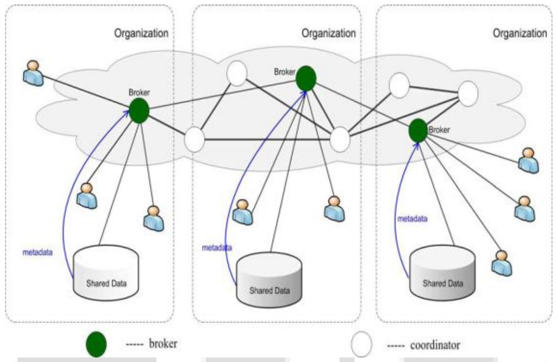

Fig. 2: Architecture of PPIB

Fig. 2 shows the architecture of PPIB. In this figure data servers and requestors from different organizations connect to the system through local brokers (i.e. Green nodes). Brokers of each organization interconnected through number of coordinators (i.e. White nodes).

Function of local broker is providing authenticationto the requestor (i.e. the user) and hides the identity of requestor from other PPIB components. It would also permute query sequence to protect against local traffic analysis. And function of coordinators is content-based query routing and access control enforcement. With privacy preserving consideration coordinator cannot hold any query in thecomplete form. Instead, automaton segmentation schemeis usedto divide metadata (query) into segments and assign each segment of query to a coordinator. To enforce secure query routing coordinators of different organizations work together. A query segment encryption scheme is used to prevent coordinators from seeing sensitive predicates (i.e. attributes) which are present in query. The query segment encryption divides a query into number of segments, and encrypts each segment in a way that coordinator cannot guess/estimate/judge the information from the part of segment which is disclose to it. In PPIB system there is a separate central authoritywhich handles key management and metadata maintenance.

The query by user submitted to the local broker which is in encrypted form. The broker forwards this query to the coordinator, then coordinator select the exact data provider and that data provider redirects the information to the user. The site distribution process is used to manage the request redirection process. Requests are redirected with reference to the server request load and count values. The response load is equally distributed to the servers. Access control verification is carried out for the data providers.

V. MODULES

The PPIB system is divided into four major modules.

(1) User Module
(2) Broker Module
(3) Co-ordinator module
(4) Admin Module

A. *User Module:*

In this module, the Users are classified into two types they are, Data Users and Data Owner Depends on the restriction the data will be passed to the Co-coordinator. The co-coordinator pass the details via broker and the data will be checked with the secret key and thus it will display for the users.

B. *Broker Module:*

In this module, the broker performs the role who can act between the Co-coordinator and the data Users. The requests which are all submitted from the data user will be verified and thus it will be passed to the co-coordinator. The data will be passed from the co-coordinator and thus it will be submitted to the End Users (Data Users).

C. *Co-ordinator Module:*

In this module, the co-coordinator performs the global service between the two end users. Initially the Data Owner needs to submit the details of the patient in the server. Data Users needs to search the data which is stored in the servers and they give request for the data and the coordinator sends the key to the Data users and the Data will be passed by the broker Way.

D. *Admin Module:*

In this module, to arrange the database based on the patient and doctor details and records. The admin needs to register and register the Organization and Users Forms.

VI. OVERALL PPIB ARCHITECTURE

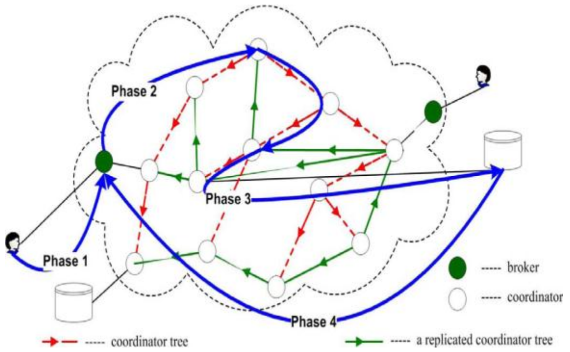

Fig. 3: We explain the query brokering process in four phases.

The architecture of PPIB is shown in Fig. 3, where users and data servers of multiple organizations are connected via a broker-coordinator overlay.

Initially, local broker authenticate the user to connect to the system. The query fromat of user is XML query with segment of query is in encrypted form with public key and unique session key K_Q . K_Q is encrypted with the public key of the data servers to encrypt the reply data. Other than authentication, the main task of broker is metadata protection.

(1) It accepts the query and encrypts that query.
(2) Create unique ID for each query (Q_{ID}) with own address to the query for data servers to return data.

Then root coordinator receives the query and its metadata a from local broker and it follows an automata segmentation scheme and query segment encryption scheme to perform access control and query routing along the leaf coordinator. If the required data is not found then failure message will be returned to broker with Q_{ID}.

The finally, the data server receives a safe query in an encrypted form. After decryption, the data server evaluates the query and returns the data, encrypted by , to the broker that originates the query.

A. *Advantages:*

(1) End-to-end query processing performance and system scalability are evaluated therefore PPIB is efficient and scalable.
(2) PPIB integrates security enforcement and query forwarding while providing comprehensive privacy protection.
(3) Load balancing and site distribution schemes are managed by the system. i.e. Data provider load is efficiently handled by the system.

VII. 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.

Many directions are ahead for future research. First at present, we would like to quantify the level of privacy protection achieved by PPIB. 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] Fengjun Li, Bo Luo, Peng Liu, Dongwon Lee, and Chao-Hsien Chu" Enforcing Secure and Privacy-Preserving Information Brokering in Distributed Information Sharing" IEEE Transaction on Informaton Forensics and Security, VOL. 8, NO. 6, JUNE 2013

[2] Mohamad Tabrez Khamar,Syed Abdulhaq,P.Babu”Providing Secure And PPIB in Distribured Information Sharing Through A.S.T And Q.S.T” 2nd International Conference on Emerging Trends on Engineering and Techno-Sciences (ETETS)-13th April 2014

[3] Yamunadevi.M.A,Nithya.K “Secure and Privacy-Preserving Information in Distributed Information Sharing “IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014

[4] Mukesh Kawatghare, Pradnya Kamble“Result on Enforce Secure and Privacy Preserving Information Brokering in Distributed Information Sharing” International Journal of Computer Science and Mobile Computing, Vol.3 Issue.7, July- 2014, pg. 437-444

[5] Ashutosh Kamble, Deepak Kapgate”Effective Concept of Implementing Secure DIBS using Query Segmentation” International Journal of Computer Science and Mobile Computing, Vol.3 Issue.5, May- 2014, pg. 472-479

[6] Ashutosh Kamble, Deepak Kapgate, Prakash Prasad” A Review on Privacy Problems in Distributed Information Brokering System and Solutions” IJCSMC, Vol. 3, Issue. 2, February 2014

[7] Rajalakshmi, A. M. J. Md Zubair Rahman” Decentralized Data Allocation with Load Balancing Mechanism” IJIRCCE Vol.2, Special Issue 1, March 2014