iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5271

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

Enforcing Secure and Privacy-Preserving Information Brokering in Distributed Information Sharing

Swati Somavanshi[1]
[1]*Computer Department, Pune University*

***Abstract:** An increasing need has been raise now a days for information sharing on demand of access. To the requested data servers, the brokers make routing decisions to direct client queries, to connect large scale loosely information brokering systems have been proposed federated data sources via a brokering overlay. Brokers are trusted in many existing IBSs, only adopt server side access control for data confidentiality. From metadata exchanged within the IBSs, privacy of data location and data consumer can still be inferred, but little attention has been put on its protection. To preserve privacy of multiple stakeholders involved, in the information brokering process in this paper, we propose a novel approach. A selected set of brokering servers, to securely share the routing decision making responsibility, the paper propose two counter measure schemes automaton segmentation and query segment encryption, we are among the first to formally define two privacy attacks namely attribute correlation attack and inference attack. With comprehensive security analysis and experimental results, to provide system wide security with insignificant overhead, we show that our approach seamlessly integrates security enforcement with query routing.*
***Keywords:** component: Access control, information sharing, and privacy.*

I. INTRODUCTION

there is an increasing need for inter organizational information sharing to facilitate extensive collaboration, ALONG with the explosion of information collected by organizations in many realms ranging from business to government agencies. The problem of balancing peer autonomy and system coalition is still challenging, while many efforts have been devoted to reconcile data heterogeneity and provide interoperability. Where peers are fully autonomous but there lacks system wide coordination, or the distributed database model, where all peers with little autonomy are managed by a unified DBMS, Most of the existing systems work on two extremes of the spectrum, adopting either the query-answering model to establish pair wise client-server connections for on-demand information access. In which organizations share information in a conservative and controlled manner due to business considerations or legal reasons; unfortunately, neither model is suitable for many newly emerged applications, such as healthcare or law enforcement information sharing.

Take healthcare information systems as example. Across collaborative healthcare providers that include a number of regional hospitals, outpatient clinics, payers, etc, Regional Health Information Organization aims to facilitate access to and retrieval of clinical data. Since its data is legally private or commercially proprietary, or both, As a data provider, a participating organization would not assume free or complete sharing with others. Over the data and the access to the data, it requires retaining full control. To preserve her privacy in the querying process, as a consumer, a healthcare provider requesting data from other providers expects. “Pouring” data into a centralized repository becomes Impractical, sharing a complete copy of the data with others. To manage locally stored data with a federated DBMS and provide unified data access, to address the need for autonomy, federated database technology has been proposed. Data heterogeneity, privacy, and trust issues, the centralized DBMS still introduces. to establish pair wise client-server relationships between each pair of peers, which is not scalable in large scale collaborative sharing, While being considered a solution between “sharing nothing” and “sharing everything”,

Peer-to-peer information sharing framework essentially. A set of brokers that make routing decisions based on the content of the queries, in the context of sensitive data and autonomous data providers, a more practical and adaptable solution is to construct a data-centric overlay consisting of data sources. Which allows users to submit queries without knowing data or server location, such infrastructure builds up semantic-aware index mechanisms to route the queries based on their content. As Information Brokering System (IBS), a distributed system providing data access through a set of brokers is referred. To the local brokers, which further “advertise” the metadata to other brokers, Databases of different organizations are connected through a set of brokers, and metadata are “pushed”. To the metadata until reaching the right data server(s), Queries are sent to the local broker and routed according. To

provide a unified, transparent, and on-demand data access, a large number of information sources in different organizations are loosely federated.

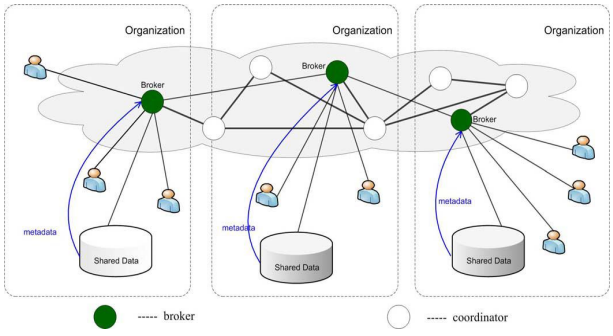
As brokers are no longer assumed fully trustable—the broker functionality may be outsourced to third-party providers and thus vulnerable to be abused by insiders or compromised by outsiders, while the IBS approach provides scalability and server autonomy, privacy concerns arise. To the privacy-preserving information sharing problem, we present a general solution. We propose a novel IBS, namely Privacy Preserving Information Brokering (PPIB), to address the need for privacy protection. It is an overlay infrastructure consisting of two types of brokering components, brokers and coordinators. For user authentication and query forwarding, the brokers, acting as mix anonymizer, are mainly responsible. The query brokering automata, the coordinators, concatenated in a tree structure, enforce access control and query routing based on the embedded nondeterministic finite automata. 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, to prevent curious or corrupted coordinators from inferring private information. To infer privacy, such as “which data is being queried”, “where certain data is located”, or “what are the access control policies”, etc, 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. On-demand information brokering, with insignificant overhead and very good scalability, Experimental results shows that PPIB provides comprehensive privacy protection.

II. RELATED WORK

Information sharing among organizations has been increased these days. To connect large scale loosely- federated data sources, information brokering system (IBSs) have been introduced. In this system, the brokers make routing decisions to direct the 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. Yet, 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 concentration has been set on its protection. This paper presents two countermeasure schemes automaton segmentation and query segment encryption schemes to preserve the privacy of multiple stakeholders involved in the information brokering process.

The main objective of data mining is to extract previously unknown patterns from large collection of data. With the rapid growth in hardware, software and networking technology there is outstanding growth in the amount data collection. Organizations collect huge volumes of data from heterogeneous databases which also contain sensitive and private information about and individual .The data mining extracts novel patterns from such data which can be used in various domains for decision making .The problem with data mining output is that I also reveals some information, which are considered to be private and personal. Easy access to such personal data poses a threat to individual privacy. There has been growing concern about the chance of misusing personal information behind the scene without the knowledge of actual data owner. Privacy is becoming an increasingly important issue in many data mining applications in distributed environment. Privacy preserving data mining technique gives new direction to solve this problem. PPDM gives valid data mining results without learning the underlying data values .The benefits of data mining can be enjoyed, without compromising the privacy of concerned individuals. The original data is modified or a process is used in such a way that private data and private knowledge remain private even after the mining process. In this paper we have proposed a framework that allows systemic transformation of original data using randomized data perturbation technique and the modified data is then submitted as result of client’s query through cryptographic approach. Using this approach we can achieve confidentiality at client as well as data owner sites. This model gives valid data mining results for analysis purpose but the actual or true data is not revealed.

III.SYSTEM ARCHITECTURE



IV. CONCLUSION

With little attention drawn on privacy of user, data, and metadata during the design stage, existing information brokering systems suffer from a spectrum of vulnerabilities associated with user privacy, data privacy, and metadata privacy. In this paper, we 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. Our analysis shows 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 scalable. Many directions are ahead for future research. First, at present, site distribution and load balancing in PPIB are conducted in an ad-hoc manner. Our next step of research is to design an automatic scheme that does dynamic site distribution. Several factors can be considered in the scheme such as the workload at each peer, trust level of each peer, and privacy conflicts between automaton segments. Designing a scheme that can strike a balance among these factors is a challenge.

Second, 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.

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,” J. AHIMA, vol. 77, pp. 64A–64D, Jan. 2006

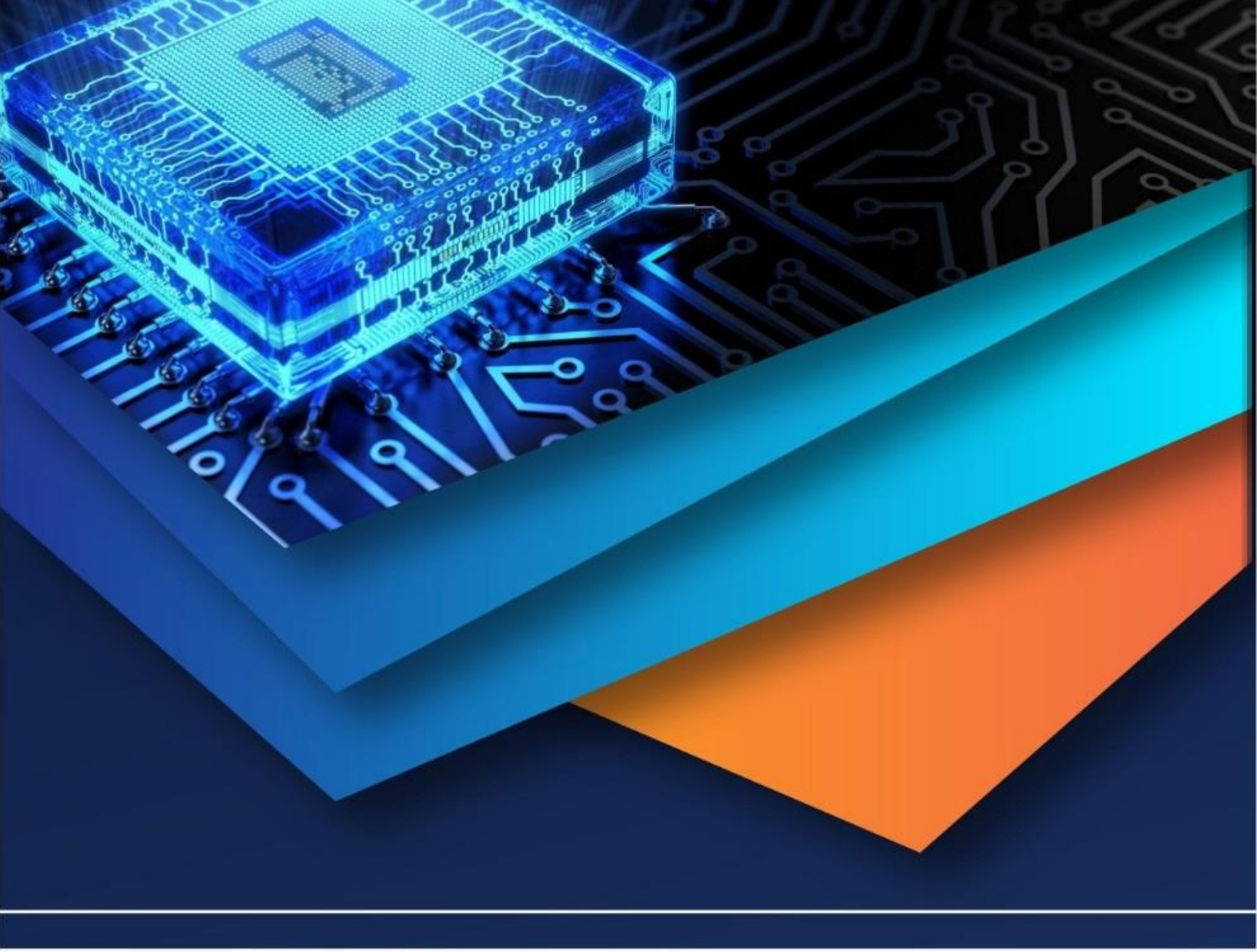
[2] A. P. Sheth and J. A. Larson, “Federated database systems for managing distributed, heterogeneous, and autonomous databases,” ACM Comput. Surveys (CSUR), vol. 22, no. 3, pp. 183–236, 1990.

[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, “CoolStreaming/DONet: 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 content routing using XML,” in Proc. SOSP, 2001, pp. 160–173

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



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY