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.2018.5108

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

Vrushali Ranmalkar (Guide) [1], Swati Somavanshi[2]
[1, 2]*Computer Department, Pune University*

***Abstract:** An increasing need for information sharing via on demand access is raise by today's organizations. To the requested data servers, the brokers make routing decisions to direct client queries, to connect large scale loosely federated data sources via a brokering overlay, information brokering systems have been proposed. Brokers are trusted for data confidentiality, many existing IBSs assumes, only adopt server side access control. From metadata exchanged within the IBS, privacy of data location and data consumer can still be inferred, but little attention has been put on his protection. To preserve privacy of multiple stakeholders involved, in this information brokering process. A selected set of brokering servers, to securely share the routing decision making responsibility among. 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 routings.*
***Keywords:** Access control, information sharing, and privacy.*

I. INTRODUCTION

To facilitate extensive collaboration by organizations in many realms ranging from business to government agencies, there is an increasing needing for inter organizational information sharing, along with the explosion of information collected. To reconcile data heterogeneity and provide interoperability, while many efforts have been devoted, the problem of balancing peer autonomy and system coalition is still challenging. Two extremes of the spectrum, adopting either the query answering model to establish pair wise client server connections for on demand information access most of the existing systems work. But there lacks system wide coordination, where peers are fully autonomous, where all peers with little autonomy are managed by a unified DBMS or the distributed database model. In a conservative and controlled manner due to business considerations or legal reasons, in which organizations share information. For many newly emerged applications such as healthcare or law enforcement information sharing.

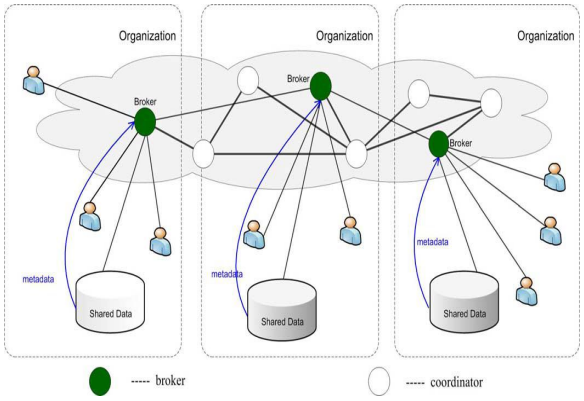
Including a number of regional hospitals, outpatient clinics, prayers, etc, across collaborative healthcare providers that take healthcare information system as example. Organization aims to facilitate access to and retrieval of clinical data from Regional Health Information Organization. A participating organization would not assume free or complete sharing with others, its data is legally private or commercially proprietary. It requires retaining full control over the data and the access to the data. Requesting data from other providers expects a healthcare provider, to preserve her privacy in the querying process as a consumer. Repository becomes impractical sharing a complete copy of the data with others is pouring data into a centralized. Federated database technology has been proposed to manage locally stored data with a federated DBMS and provide unified data access to address the need for autonomy. Which is not scalable in large scale collaborative sharing, to establish pair wise client server relationships between each pair of peers, data heterogeneity, privacy and trust issues, the centralized DBMS still introduces, while being considered a solution between "Sharing nothing" and "Sharing everything" peer to peer information sharing framework essentially. On the content of the queries, in the context of sensitive data and autonomous data providers a set of brokers that make routing decision. To construct a data centric overlay consisting of data sources, a more practical and adaptable solution. To route the queries based on their content, which allows users to submit queries without knowing data or server location, such infrastructure builds up semantic aware index mechanisms. A set of brokers is referred, as information brokering system, a distributed system providing data access. Different organizations are connected through a set of brokers and metadata are pushed of databases, to the local brokers, which further "advertise" the metadata to other brokers. 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.

To third party providers and thus vulnerable to be abused by insiders or compromised by outsiders, as brokers are no longer assumed fully trustable the broker functionality may be outsourced, while the IBS approach provides scalability and server autonomy, privacy concerns arise. A general solution to the privacy preserving information sharing problem we present. Namely Privacy preserving information brokering we proposed a novel IBS, to address the need for privacy protection. Two types of brokering components, brokers and coordinators is an overlay infrastructure consisting. Mainly responsible for user authentication and query forwarding, the brokers, acting as mix anonymizer. On the embedded non deterministic finite automata, the query brokering automata, the coordinators, concatenated in a tree structure, enforce access control and query routing based. A set of collaborative coordinators, 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. 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

Organizations has been increased these days among information sharing, information brokering system have been introduced, to connect large scale loosely federated data source. To the requested data servers, in this brokers make routing decision to direct the client queries. For server side access control for data confidentiality, many existing IBS assume that brokers are trusted and so they adopt. From metadata exchanged within the IBS, privacy of data location and data consumer can still be inferred, but little concentration has been set on its protection. In the information brokering process, two counter measure schemes are available to preserve the privacy of multiple stakeholders and that they are automaton segment and query segment encryption. From large collection of data, to extract previously unknown pattern is the main objective of data mining. there is outstanding growth in the amount data collection, with the rapid growth in hardware, software and networking technology. Databases which also contain sensitive and private information about and individual that organizations collect huge volumes of data. the data which can be used in various domains for decision making, the data mining extracts novel patterns. I also reveals some information that the problem with data mining output, which are considered to be private and personal. To individual privacy, easy access to such personal data poses a threat. The scene without the knowledge of actual data owner, there has been growing concern about the chance of misusing personal information. In many data mining applications in distributed environment, privacy is becoming an increasingly important issue. To solve this problem, privacy preserving data mining technique gives new direction. The underlying data values, PPDM gives valid data mining results without learning. The privacy of concerned individuals, the benefits of data mining can be enjoyed without compromising. In such a way that private data and private knowledge remain private even after the mining process, the original data is modified or a process is used. The modified data is then submitted as result of clients query through cryptographic approach, we have proposed a framework that allows systemic transformation of original data using randomized data perturbation technique. At client as well as data owner sites, using this approach we can achieve confidentiality. For analysis purpose but the actual or true data is not revealed, this model gives valid data mining results.

III. ARCHITECTURE



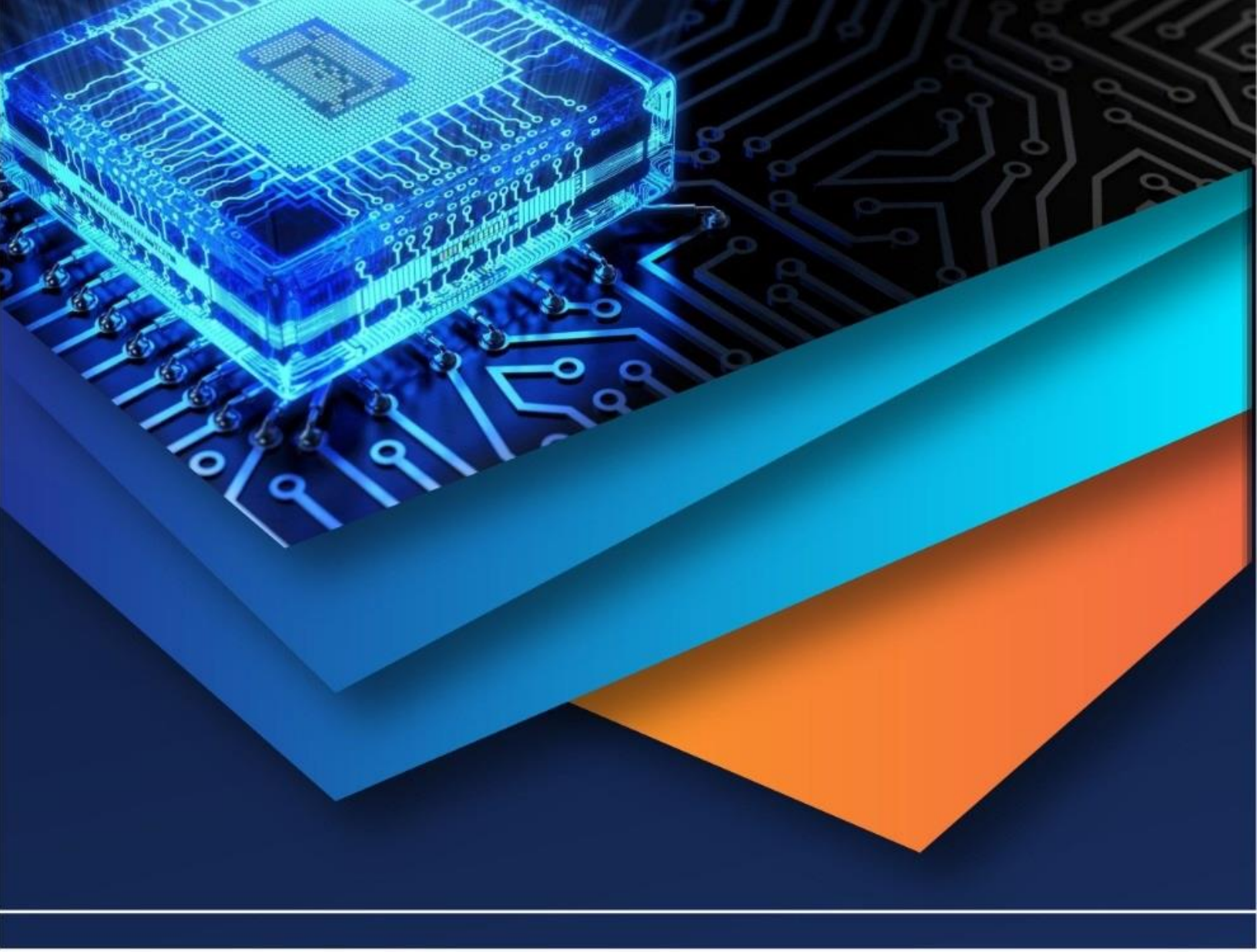
IV. CONCLUSIONS

With user privacy, data privacy and metadata privacy, existing information brokering systems suffer from a spectrum of vulnerabilities associated, with little attention drawn on privacy of user, data and metadata during the design stage. To preserve privacy in XML information brokering, we propose PPIB a new approach. While providing comprehensive privacy protection, PPIB integrates security enforcement and query forwarding, through an innovative automaton segmentation scheme in network access control and query segment encryption. It is very resistant to privacy attacks, our analysis shows. The result shows that PPIB is efficient and scalable, End to end query processing performance and system scalability are also evaluated.

For future research, many directions are ahead. In PPIB are conducted in an ad-hoc manner, at present site distribution and load balancing. AN automatic scheme that does dynamic site distribution, our next step of research is to design. Trust level of each peer and privacy conflicts between automaton segments, several factors can be considered in the scheme such as the workload at each peer. A balance among these factors is a challenge, designing a scheme that can strike. who decides such issues as automaton segmentation granularity, we plan to minimize the participation of administrator node. To make PPIB self reconfigurable is the main goal to make.

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