ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Data Sharing Across Information Brokering System Infrastructure for Privacy-Preserving

[1]N. Sakthipriya, [2]A.R. Arunachalam

[1,2]Assistant Professor, Department of Computer Science & Engineering, Bharath University, Chennai, India

ABSTRACT: Information Brokering System (IBS)provides data access through a set of brokers and supports information sharing among loosely federated data sources. To address the need for privacy protection and information sharing problem a novel IBS, named Privacy Preserving Information Brokering (PPIB) is proposed. It is an overlay infrastructure consisting of two types of brokering components, brokers and coordinators. The brokers are responsible for user authentication and query forwarding. The coordinators, concatenated in a tree structure, enforce access control and query routing based on the query brokering automata. To prevent corrupted coordinators from inferring private information, we design two novel schemes: (a) to segment the query brokering automata, and (b) to encrypt corresponding query segments. It provides full capability to enforce in-network access control and to route queries to the right data sources, these two schemes ensure that a 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", etc. The expected outcome of PPIB provides privacy protection for on-demand information brokering, with insignificant overhead and very good scalability.

KEYWORDS: Query routing, access control, Information brokering

I. INTRODUCTION

Service Computing has become a cross-discipline that covers the science and technology of bridging the gap between business services and IT services. The underneath breaking technology suite includes Web services and service oriented architecture, cloud computing, business consulting methodology and utilities, business process modeling, transformation and integration. The scope of Service Computing covers the whole life-cycle of services innovation research that includes business componentization, services modeling, services creation, services. services monitoring, services optimization, as well as services management. It also refers to the scientific and technical body of knowledge that is emerging to enhance our understanding of complex service systems that integrate the business and technical concerns. This is an inherently inter-disciplinary endeavor which focuses on the creation of value between customers and service providers in the context of the design, solution development, delivery, and management of the service. SC covers the science and technology of leveraging computing and IT to model, create, operate, and manage business services. A Web service is a programmable module with standard interface descriptions that provide universal accessibility through communication protocols. It is an application framework facilitating services operation for service provider, requestor and registry. It is language and platform independent, machine searchable. A new cost-effective way of engineering software to quickly develop and deploy web applications that changes the internet from a repository of data into a repository of services. The goal of Service Computing is to enable IT services and computing technology to perform business services more effectively.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

II. EXISTING SYSTEM

The Information sharing approaches always assumes the use of trustable servers such as the central data warehousing server or database server. The honest assumptions may not hold for brokers. They may either be abused by insiders or compromised by outsiders. It is obvious that the brokers become the most vulnerable privacy breach which leads to security and privacy risks. The survival of information brokering depends on the trust of brokers to enforce authentication, access control as well as query forwarding and while failing to provide proper protection of information released in the process may
create circumstances that harm the privacy of user data and the system. In information brokering infrastructure, the privacy concerns arise when identifiable information is disseminated with no or poor disclosure control. Data providers push routing and access control metadata to brokers which also handles queries requestors. Therefore a corrupted brokering server could Learn query content and query location by intercepting a local query Learn routing metadata and access control metadata from local data servers and others brokers. Learn data location from routing metadata it holds. With one or several types of information the attacker could infer the privacy of different stack holders.

III. TYPES OF ATTACKS

A.The attacks are classified into two types

Attribute Correlation Attack: An attacker intercepts a query which contains several predicates. Each predicate describes a condition that involves sensitive and private data. If a query has multiple predicates the attacker can correlate the corresponding attributes to infer sensitive information about the data owner.
Example: Anitha has the symptom of cancer, the query has two predicates [name=”Anitha”] and [symptom=”cancer”].Any malicious broker that has helped routing the query could guess “Anitha has a cancer” by these two predicates in the query.Inference Attack: More severe privacy leak occurs when an attacker obtains more than one type of sensitive information and associates them to learn explicit knowledge about the stake holders (by guessing). An attacker can guess the identity of a requester from her query location (IP Address).

Example: If an attacker identifies a data server present in a cancer research center then he tags the related queries as cancer. The three combinations of private information inferences are

1.From query and data location the attacker infers knowledge about who is interested in what type of data.

2.From query location and query content the attacker may come to know who is interested in what, where, who is, if the query predicates describing one’s interests (symptom or medicine, address or name).

3.From query content and data location the attacker infers which data server has what data.
Hence the attacker could monitor user queries to learn data distribution of the system which could be used to conduct further attacks. To address the privacy vulnerabilities in information brokering PPIB is proposed. The key to preserve privacy is to divide the work among multiple components in such a way that no single node can make a meaningful interference from the information disclosed to it.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

This article tackles the problem of preserving the privacy of data in XML information brokering system and providing protection from privacy attacks.

IV. RELATED WORK

Generates an algorithm for inference proof view by eliminating the confidential and other information that could be used to infer confidential information. It represents potentially incomplete information and provides a control mechanism for enforcing inference usability confinement of XML document. The Controlled Query Evaluation (CQE) is an effective way to enforce inference control on information sets of a static inference proof database containing the XML documents. With the notion of an inference proof view of the actual XML document under the set of confidential information and the inference capabilities of the client and also presents an algorithm for an generating an inference proof view[1].

Information accountability and the social networks manipulates personal health records that refers to when one party is held liable to explain their use of information belonging to another party. It presents an effective way for sharing health information through the use of a health care social network which uses HL7 as the communication method between health information systems which provides a means to verify, analyse and investigate users's actions. Information about parties accountable should be made usable by stakeholders each of whom have different purposes and levels of accessibility to the information. The concept of information accountability and health interoperability in a secure health care social network which uses HL7 as medium for information sharing that could prove to be the ultimate solution for patient healthcare[2].

Employs link to records from different data sources in terms of complexity, efficiency, accuracy and
detects the duplicate records. Shares the data to 1.Improve the delivery of information by providing immediate secure, confidential exchange between users.2.Providing warning and reminders at point of care .3.Reduce the maximum errors in sharing the data. 4.Allow user to evaluate their information to be viewed by whom they allow. With the accurate patient identification and linking of health records it is implemented in a network that shares the patient information with safety and quality of care and address the problem of the quality linking methods in regional health information[3].

Three types of broker approaches namely embedded, source side control and in broker access control is to implement the pushing idea. Experiments shows in broker access control can simultaneously improve the performance of memory consumption, end to end query directing time with system wide security.

The access control can occur anywhere in the network freely at client, server and in-between. It focuses on access control issues in XML information brokerage systems where end users send in queries without knowing where the data is actually stored and brokers take the responsibility to locate the data sources and forward the queries[4].

A flexible document type definition based access control model is made for xml and the query rewriting, optimization in the presence of general document type definition for a rich class of XPath queries. It is an efficient algorithm for deriving security view definition from security policies for different user groups and a paradigm for specifying XML security constraints to enforce during query processing. It exposes all and only necessary schema structure and document content to authorizes users. Also employs internal XPath query annotations in the view of document type definition to describe the access paths to the relevant accessible parts of the document[[5].

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

An efficient client based evaluator of access control rules for regulating access to XML documents which takes benefit from a dedicated index to quickly converge towards the authorized parts of a document and providing security mechanisms guarantee that prohibited data can never be disclosed during the processing that is protected from any type of tampering. Accurate streaming access control rules evaluator supports fragment of XPath language, skip index structure allowing skipping the irrelevant parts in the input document with respect to access control policy, pending predicates management and random integrity checking[6]

Federated Database is used to manage and store locally stored data with a DBMS providing unified data access[7]. Fine grained access control model is used for authorization at the node level by tuple access control policy that consists of a set of access control rights[8]. A Data centric overlay is constructed with data sources and set of brokers for helping to locate data sources for queries[9].Data is shared among a large number of autonomous nodes[10].Xml access control mechanisms at the nodes filter out the data nodes which cannot be accessed by users[11]. The authorization are specified at the node level of fine grained access control model with control policy[12].Enforcing access control policy has been classified as engine, view and preprocessing, post processing based approaches[13].

V. PROPOSED SYSTEM

Privacy Preserving Information Brokering (PPIB) is an overlay infrastructure consisting of two types of brokering components, brokers and coordinators. The brokers are mainly responsible for user authentication and query forwarding.[5] The coordinators enforce access control and query routing based on the non-deterministic finite automata. In order to prevent corrupted coordinators from inferring private information the two schemes automatic segmentation and query forwarding is proposed 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. PPIB provides comprehensive privacy protection for on-demand information brokering system.

VI. SYSTEM ARCHITECTURE

The Privacy Preserving Information Brokering System (PPIB) has users and data servers of multiple organizations that are connected via the broker-coordinator overlay. User request for the data by sending a query to the local broker which forwards the query to the root coordinator tree. The query is processed along a path of the coordinator tree until it is denied by any coordinator or accepted by a leaf coordinator. The accepted query is rewritten into a safe query and sent to relevant data servers.[6]

The PPIB architecture consists of four phases for brokering process

Phase 1: PPIB Components Registration

Global organization having global schema acts as a consortium for different organization that belongs to the same field and agrees to share their data as global data. PPIB components such as brokers, coordinators register with Information Brokering System (IBS).[7] Requestor registers with corresponding brokers, who acts as the entrance to the IBS. Coordinator send request to Central Authority to join the system.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

The CA is assumed for off-line initiation and maintenance which holds a global view about all the rules. The data servers share a pair of public and private keys, while each of the coordinators has its own pairs of level key and commutative level key.[8]

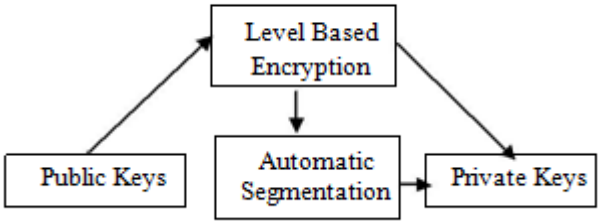

Fig.1.Central Authority

Phase 3: Query Routing

Data servers and requestors from different organizations connect to the system through local brokers. Brokers are interconnected through coordinators. A local broker functions as the

"entrance" to the system. It authenticates the requestor and hides his identity from other PPIB components. It forwards the requestor query to root coordinator.[9]

Phase 4: Query Processing

The Data Server receives the processed query in an encrypted form. After decryption, the data server evaluates the query and returns the data encrypted by KQ, to the broker that originates the query.[10]

VII. ALGORITHM

THE AUTOMATON SEGMENTATION

The atomic unit in the segmentation is an NFA state [14]of the original automaton. Each segment is allowed to hold one or several NFA states.[11] The granularity level denotes the greatest distance between any two NFA states contained in one segment. Given a granularity level k, for eachsegmentation, the next i € [1; k] NFA states will be divided into one segment with a probability 1=k. Obviously, a larger granularity level indicates that each segment contains more NFA states[15], resulting in a smaller number of segments and less end-to-end overhead in distributed query processing. A coarse partition is more likely to increase the privacy risk. The trade-off between the processing complexity and the privacy requirements should be considered in deciding the granularity level.[12] To reserve the logical connection between the segments after segmentation heuristic segmentation rules are defined: (1) multiple NFA states in the same segment should be connected via parent-child links; (2) no sibling NFA states should not be put in the same segment without the parent state; and (3) the accept state of the original global automaton should be put in separate segments.[13] To ensure the segments are logically connected can change the last states of each segment to be dummy accept states which point to the segments holding the child states in the original global automaton.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

Algorithm : The automaton segmentation algorithm:deploySegment()

INPUT : Automaton State S

OUTPUT: Segment Address: addr

```
1:  for each symbol k in S.StateTransTable do
2:   addr=deploySegment(S.StateTransTable(k)
     .nextState)
3:  DS=createDummy.AcceptState()
4:  DS.nextState ← addr
5:  S.StateTransTable(k).next State ← DS
6:  end for
7:  Seg=createSegment()
8:  Seg.addSegment(S)
9:  Coordinator=getCoordinator()
10: Coordinator.assignSegments(Seg)
11: return Coordinator.address
```

VIII. CONCLUSION AND FUTURE WORK

Several factors can be considered such as the workload at each peer, trust level of each peer andprivacy conflicts between automaton segments. Designing a scheme that can strike a balance among these factors is a challenge and the level of privacy protection is achieved by PPIB. We plan to minimize (or even eliminate) the participation of the administrator node, who decides such issues as automaton segmentation granularity. The main goal is to make PPIB self reconfigurable. The 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.

The erosion of trust put in traditional database servers and in Database Service Providers, the growing interest for different forms of data dissemination and the concern for protecting children from suspicious Internet content are different factors that lead to move the access control from servers to clients. Several encryption schemes can be used to serve this purpose but all suffer from a static way of sharing data. With the emergence of hardware and software security elements on client devices, more dynamic client-based access control schemes can be devised. This is an efficient client-based evaluator of access control rules for regulating access to XML documents.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015

REFERENCES

1. Joachim Biskup and Lan Li *" On Inference- Proof View Processing of XML Documents"* IEEE Transactions on dependable and secure computing, Vol.10, no.2, March (2013).
2. Vijayaragavan S.P., Karthik B., Kiran T.V.U., Sundar Raj M., "Robotic surveillance for patient care in hospitals", Middle - East Journal of Scientific Research, ISSN : 1990-9233, 16(12) (2013) pp. 1820-1824
3. Gajanayake, Randile, Iannello, Renato &SahamaTony R, "*Sharing with care: An Accountability Perspective"* IEEE Internet Computing,15(4), pp. 31-38 (2011).
4. Vijayaragavan, S.P., Karthik, B., Kiran Kumar, T.V.U., Sundar Raj, M."Analysis of chaotic DC-DC converter using wavelet transform", Middle - East Journal of Scientific Research, ISSN : B27, 16(12) (2013) pp.1813-1819.
5. F. Li, B. Luo, P. Liu, D. Lee, P. Mitra, W. Lee, and C. Chu, "In-broker access control: "*In broker Access Control Towards efficient end-to-end performance of information brokerage systems* " in Proc. IEEE SUTC, (2006).
6. Vijayaraghavan K., Nalini S.P.K., Prakash N.U., Madhankumar D.,"Biomimetic synthesis of silver nanoparticles by aqueous extract of Syzygium aromaticum", Materials Letters, ISSN : 0167-577X, 75() (2012) pp. 33-35.
7. W.Fan, C.-Y. Chan and M. Garofalakis, "*Securexml querying with security views"* in ACM SIGMOD, pp. 587–598, (2004).
8. Vijayaraghavan, K., Nalini, S.P.K., Prakash, N.U., Madhankumar, D., "One step green synthesis of silver nano/microparticles using extracts of Trachyspermum ammi and Papaver somniferum", Colloids and Surfaces B: Biointerfaces, ISSN : 0927-7765, 94() (2012) pp. 114-117.
9. L. Bouganim, F.D.Ngoc, and P.Pucher "*Client-based access control management for XML documents.*," in VLDB, (2004).
10. Kulanthaivel L., Srinivasan P., Shanmugam V., Periyasamy B.M., "Therapeutic efficacy of kaempferol against AFB1 induced experimental hepatocarcinogenesis with reference to lipid peroxidation, antioxidants and biotransformation enzymes", Biomedicine and Preventive Nutrition, ISSN : 2210-5239, 2(4) (2012) pp.252-259.
11. B. Luo, D. Lee, W. C. Lee, and P. Liu, "*Qfilter: Fine-grained runtime XML access control via nfa-based query rewriting enforcement mechanisms*," in CIKM, 2004.
12. N. Koudas, M. Rabinovich, D. Srivastava, and T. Yu, "*Routing XML queries*," in ICDE '04, p. 844, 2004.
13. G. Koloniari and E. Pitoura, "*Content-basedrouting of path queries in peer-to-peer systems*.," in EDBT, pp. 29–47, 2004.
14. Dr.A.Muthu Kumaravel, KNOWLEDGE BASED WEB SERVICE, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 5881-5888, Vol. 2, Issue 9, September 2014
15. Dr.A.Muthu Kumaravel, Data Representation in web portals, International Journal of Innovative Research in Computerand Communication Engineering, ISSN(Online): 2320-9801,pp 5693-5699, Vol. 2, Issue 9, September 2014
16. Dr.Kathir.Viswalingam, Mr.G.Ayyappan,A Victimization Optical Back Propagation Technique in Content Based Mostly Spam Filtering ,International Journal of Innovative Research in Computerand Communication Engineering ,ISSN(Online): 2320-9801 , pp 7279-7283, Vol. 2, Issue 12, December 2014
17. KannanSubramanian,FACE ECOGNITION USINGEIGENFACE AND SUPPORT ECTORMACHINE,International Journal of Innovative Research in Computerand Communication Engineering,ISSN(Online): 2320-9801,pp 4974-4980, Vol. 2, Issue 7, July 2014.
18..Vinothlakshmi.S,To Provide Security & Integrity for StorageServices in Cloud Computing ,International Journal of Innovative Research in Computer and Communication Engineering ,ISSN(Online): 2320-9801 , pp 2381-2385 ,Volume 1, Issue 10, December 2013

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 7, July 2015