International Journal Of Advanced Engineering & Innovative Technology (IJAEIT)
ISSN: 2348 7208

IMPACT FACTOR: 1.04

Privacy Preserving Information Brokering System for Multi-kiosk Government Policies

Rahul Jadhav, Manoj Jagtap, Santosh Murudkar, Aniket Ratnaparkhi

Under the Guidance of: Prof. R.N.Pathare

ABSTRACT: To facilitate extensive collaborations, today's organizations raise increasing needs for information sharing via on-demand information access. Information Brokering System (IBS) atop a peer-to-peer overlay has been proposed to support information sharing among loosely federated data sources. It consists of diverse data servers and brokering components, which help client queries to locate the data servers. However, many existing IBSs adopt server side access control deployment and honest assumptions on brokers, and shed little attention on privacy of data and meta data stored and exchanged within the IBS. In this article, we study the problem of privacy protection in information brokering process. We first give a formal presentation of the threat models with a focus on two attacks: attribute correlation attack and inference attack. Then, we propose a broker-coordinator overlay, as well as two schemes, automaton segmentation scheme and query segment encryption scheme, to share the secure query routing function among a set of brokering servers. With comprehensive analysis on privacy, end-to- end performance, and scalability, we show that the proposed system can integrate security enforcement and query routing while preserving system-wide privacy with reasonable overhead.

Technical keyword: Access Control, PPIB, Privacy, Broker, Cordinator.

1. INTRODUCTION:

In this article, we present a general solution to the privacy preserving information sharing problem. First, to address the need for privacy protection, we propose a novel IBS, namely Privacy Preserving Information Brokering (PPIB). It is an overlay infrastructure consisting of two types of brokering components, brokers and coordinators. The brokers, acting as mix anonymizer are mainly responsible for user authentication and query forwarding [1]. The coordinators, concatenated in a tree structure, enforce access control and query routing based on the embedded non-deterministic automata the query brokering automata. 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[6] so that routing decision making is decoupled into multiple correlated tasks for a set of collaborative coordinators. 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 to infer privacy, such as which data is being queried, where certain data is located, or what are the access control policies, etc. Experimental results show that PPIB provides comprehensive privacy protection for on-demand information brokering, within significant overhead and very good scalability.

2. EXISTING SYSTEM:

The existing system supposes Alice owns a k-anonymous database and needs to determine whether her database, when inserted with a tuple owned by Bob, is still k-anonymous. Also, suppose that access to the database is strictly controlled, because data are used for certain experiments that need to be maintained confidential. Clearly, allowing Alice to directly read the contents of the tuple breaks the privacy of Bob; on the other hand, the confidentiality of the database man- aged by Alice is violated once Bob has access to the contents of the database [4].Thus, the problem is to check whether the database inserted with the tuple is still k-anonymous, without letting Alice and Bob know the contents of the tuple and the database respectively.
Disadvantage:
1. The database with the tuple data does not be maintained confidentially.
2. The existing systems allows another person to easily access database.

3. PROBLEM STATEMENT:

Proposes an innovative Privacy Preserving Information Brokering (PPIB) framework to address the user data metadata privacy vulnerabilities associated with existing

----
Rahul Jadhav, Manoj Jagtap, Santosh Murudkar, Aniket Ratnaparkhi; B.E IT Engineering Zeal College Of Engineering & Research, Pune, Maharashtra
Prof. R.N.Pathare; Asst. Prof. in IT Department, Zeal College Of Engineering & Research, Pune, Maharashtra

distributed information brokering systems. The key to preserving privacy is to divide and allocate the functionality to multiple brokering components in a way that no single component can make a meaningful inference from the information disclosed to it.

4. PROPOSED SYSTEM:

In the current project, we present two efficient protocols, one of which also supports the private update of a Generalization based anonymous database. We also provide security proofs and experimental results for both protocols. So far no experimental results had been reported concerning such type of protocols; our results show that both protocols perform very efficiently.

Advantage:

1. The anonymity of DB is not affected by inserting the records.
2. We provide security proofs and experimental results for both protocols.

5. SYSTEM REQUIREMENT:

A)Domain:

PPIB Privacy Preserving System

B) Software Interfaces:

Operating system : Windows XP

Coding Language : Advance Java

Data Base : MySQL

C) Hardware Interface:

Hard Disk : 40 GB.

Floppy Drive : 1.44 Mb.

Monitor : 14 Colour Monitor.

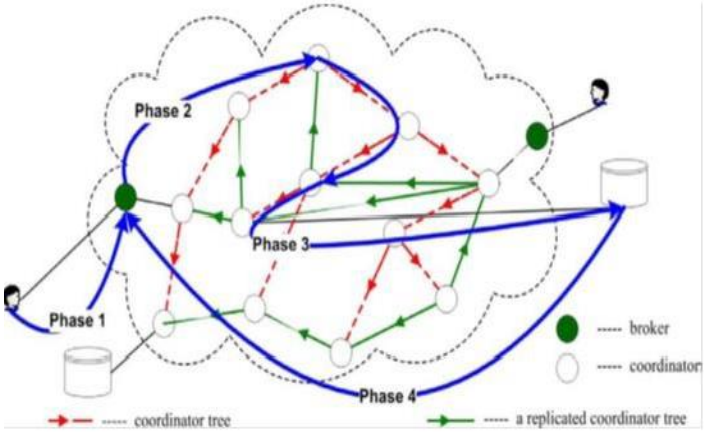
Mouse : Optical Mouse.

Ram: 512 Mb.

Keyboard: 101 Keyboard

6. SYSTEM ARCHITECTURE:

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



In particular, the brokering process consists of four phases:

Phase 1: To join the system, a user needs to authenticate himself to the local broker. After that, the user submits an XML query with each segment encrypted by the corresponding public level keys, and a unique session key KQ. KQ is encrypted with the public key of the data servers to encrypt the reply data.

Phase 2: Besides authentication, the major task of the broker is metadata preparation:(1) it retrieves the role of the authenticated user to attach to the encrypted query; (2) it creates a unique QID for each query, and attaches QID,(KQ)

7 CONCEPT AND SPECIFICATION

pkDS and its own address to the query for data servers to return data.

Phase 3: Upon receiving the encrypted query, the coordinators follow automata segmentation scheme and query segment encryption scheme to perform access control and query routing along the coordinator tree. At the leaf coordinator, all query segments should be processed and re-encrypted by the public key of the data server. If a query is denied access, a failure message with QID will be returned to the broker.

Phase 4: In this phase, 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 KQ, to the broker that originates the query.

8 MODULES:

Automaton segmentation and query segment encryption are two countermen sure schemes to securely share the routing decision-making responsibility among a selected set of brokering servers

Automaton Segmentation:

In the context of distributed information brokering [4], multiple organizations join a consortium and agree to share the data within the consortium. While different organizations may have different schemas, we assume a global schema exists by aligning and merging the local schemas. Thus, the access control rules and index rules for all the organizations can be crafted following the same shared schema and captured by a global automaton, the global QBroker.The key idea of the automaton segmentation scheme is to logically divide the global automaton8 Concept and Specification into multiple independent yet connected segments, and physically distribute the segments onto different brokering servers.

Segmentation:

The atomic unit in the segmentation is an NFA state of the original automaton [6]. Each segment is allowed to hold one or several NFA states. We further define the granularity level to denote the greatest distance between any two NFA states contained in one segment. Given a granularity level k, for each segmentation, the next i 2 [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, resulting in a smaller number of segments and less end-to-end overhead in distributed query processing. On the contrary, a coarse partition is more likely to increase the privacy risk. The tradeoff between the processing complexity and the privacy requirements should be considered in deciding the granularity level. As privacy protection is of the primary concern of this work, we suggest a granularity level 2. To reserve the logical connection between the segments after segmentation, we define heuristic segmentation rules: (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. To ensure the segments are logically connected, we 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.

9 CONCEPT AND SPECIFICATION

Query Segment Encryption:

The query segment encryption scheme consists of the pre-encryption, post-encryption, and a special commutative encryption module for processing the double-slash (//) XPath step in the query.

1. Level-based pre-encryption: According to the automaton segmentation scheme, each query is processed by a set of coordinators along a path of the coordinator tree. If we encrypt the query segments with the public key of the coordinators correspondingly, we guarantee that each segment will be decrypted and processed by the one who is supposed to do so. Moreover, each coordinator only sees a small portion of the query that is not enough for inference, but by collaborating with others, they can still fulfill the designed functions. The key problem in this approach is that the segment-coordinator association is unknown beforehand in the distributed setting, since no party other than the CA knows how the global automaton is segmented and distributed among the coordinators. To tackle the problem, we propose to encapsulate query pieces based on the static and publicly known information the global schema. XML schema forms a tree structure, in which the level of a node in the schema tree is defined as its distance to the root node. Since both the ACR and index rules[B] are constructed following the global schema, an XPath step (token) in the XPath expression of a rule is associated with level i if the corresponding node in the schema tree is at level i. We assume the nodes of the same level share a pair of public and private level keys,fpk; skg. After automaton segmentation, the segments (and the corresponding coordinators) are assigned with the private key of level i, ski, if it contains a node of level i. In pre-encryption, the XPath steps (between two / or //) of a query are encrypted from the root with the public level keys fpk1; pk2; :::g, respectively.

10 CONCEPT AND SPECIFICATION

Intuitively, the ith XPath step of a query should be processed by a segment with a node at level i, and therefore, is able to be decrypted by the coordinator with that segment. Moreover, if a coordinator has a segment that contains XML nodes of k different levels, it needs to decrypt the _rst k unprocessed XPath steps of the query.

2. Post-encryption: The processed query segment should also be protected from all the coordinators in later processing, so post-encryption is necessary. In a simple scheme, we assume all the data servers share a pair o public and private keys, fpk DS; sk DSg, where pkDS is known to all the coordinators. Each coordinator first decrypts the query segment(s) with its private level key, performs authorization and indexing, and then encrypts the processed segment(s) with pkDS so that only the data servers can view it.

3. Commutative encryption for // handling: When a query has the descendant or-self axis (i.e., // in XPath expressions), a so-called mismatching problem occurs at the coordinator who takes the // XPath step as input. This is because that the // XPath step may recursively accepts several tokens until it _nds a match.

11. MATHEMATICAL MODEL:

Let U be the user
Let B be the broker
Let c be the co_ordinator
U={u1,u2,….un}
B={B1,B2,….Bn}
C={C1,C2,….Cn}
S={F1,F2,F3,F4}

1. Authentication

Input:login id ,password
F1={uid,pk,kQ,E}
Uid-User id
PK-Public Key
KQ-Session Key
E-Encription
Output:E(KQ,Pk)

2.For meta data preparation
Input:E(KQ,Pk)
F2={Uid,E,QID,KQ,baddr}
Uid-User id
QID-query id
KQ-Session Key
Badder-broker address

Output(QID,(KQ)pKDS)
3.Role of root CO-Ordinator
Input:E(Q),Qid
F3={RC,Qid PK,NFA,ACR}
RC-root Co-ordinator
Qid-Query id
Pk-Public id
NFA-non deterministic finite
ACR-Access Control Rule
RC performs autometa segmentation and query segmentencryption to perform access control and indexing
NFA={ST,PT,ID,location list}

Where,
ST-State transition table
PT-Pridicate table
ST={ESymbol,DSstate,Accesslist}

Where,
eSymbol-Child state
DSstate-Double slash state
AcessList-for which roles the state is accept state
Condition-test condition
ACR-{subject,object,action,sign,type}
Subject-role to whome authorization is granted
Object-set of xml nodes specify by an xpath expression
Action-operation as read, write,or update

Advantages:

1. Improve customer buying experience
2. Increase Customer Base.
3. Innovative approach for fraud reduction in revenue collection department of Municipality.

12. APPLICATIONS:

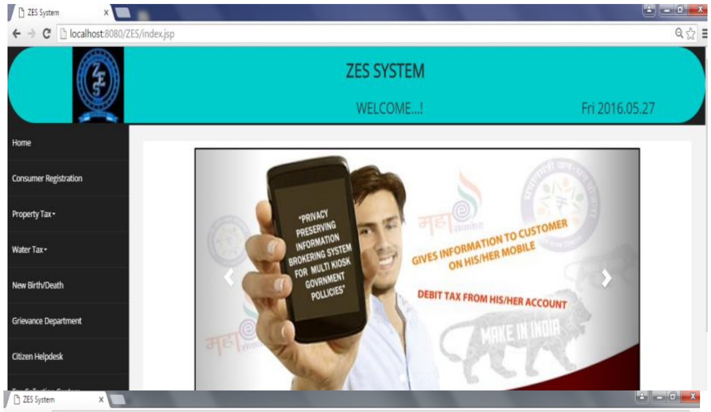
1. For Rogering Govt Policies.
2. Health care Applications
3. Banking Applications

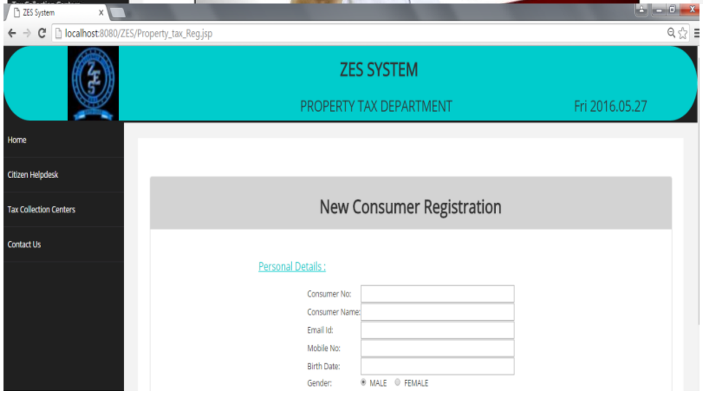
13. CONCLUSION:

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.

14. IMPLEMENTAION:

Our aim is to facilitate access to and retrieval of corporation data across collaborative information providers that include a water supplier, property tax department.

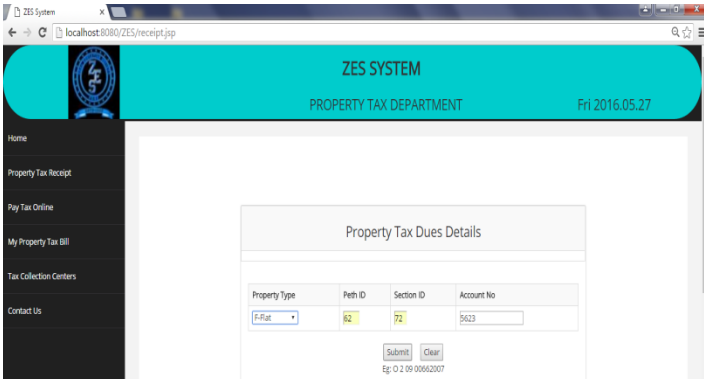

ZES System
localhost:8080/ZES/index.jsp
ZES SYSTEM
WELCOME...!
Fri 2016.05.27
Home
Consumer Registration
Property Tax
Water Tax
New Birth/Death
Grievance Department
Citizen Helpdesk
"PRIVACY PRESERVING INFORMATION BROKERING SYSTEM FOR MULTI KIOSK GOVRNMENT POLLICIES"
GIVES INFORMATION TO CUSTOMER ON HIS/HER MOBILE
DEBIT TAX FROM HIS/HER ACCOUNT
MAKE IN INDIA



New Consumer Registration

Personal Details :

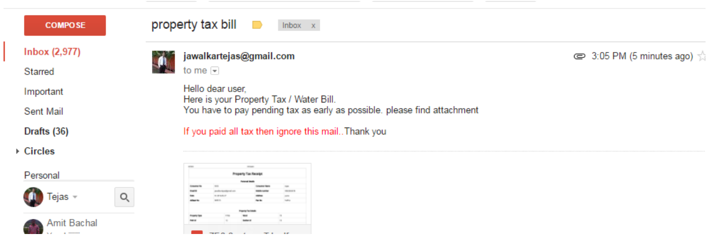
Consumer No:
Consumer Name:
Email Id:
Mobile No:
Birth Date:
Gender: ● MALE ○ FEMALE



Property Tax Dues Details

Property Type	Peth ID	Section ID	Account No
F-Flat	62	72	5623

Eg: O 2 09 00662007

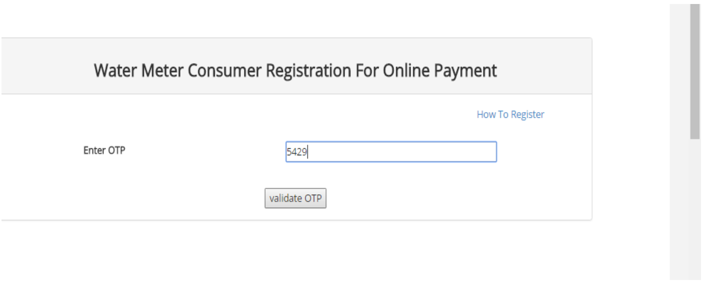


property tax bill

jawalkartejas@gmail.com
to me
3:05 PM (5 minutes ago)

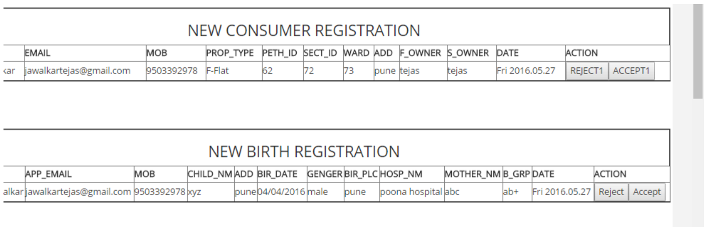
Hello dear user,
Here is your Property Tax / Water Bill.
You have to pay pending tax as early as possible. please find attachment

If you paid all tax then ignore this mail..Thank you



Water Meter Consumer Registration For Online Payment

Enter OTP: 5429

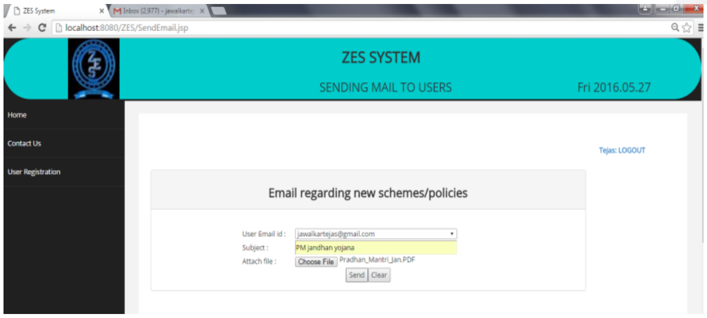


NEW CONSUMER REGISTRATION

	EMAIL	MOB	PROP_TYPE	PETH_ID	SECT_ID	WARD	ADD	F_OWNER	S_OWNER	DATE	ACTION
kar	jawalkartejas@gmail.com	9503392978	F-Flat	62	72	73	pune	tejas	tejas	Fri 2016.05.27	REJECT1 ACCEPT1

NEW BIRTH REGISTRATION

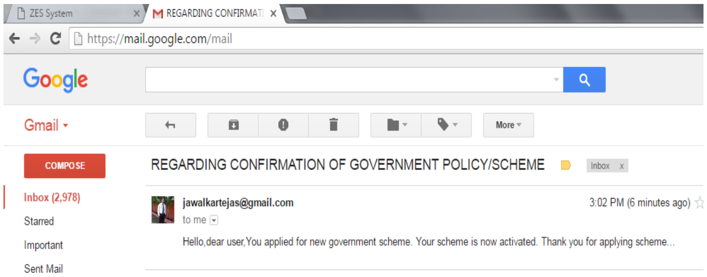
	APP_EMAIL	MOB	CHILD_NM	ADD	BIR_DATE	GENGER	BIR_PLC	HOSP_NM	MOTHER_NM	B_GRP	DATE	ACTION
alkar	jawalkartejas@gmail.com	9503392978	xyz	pune	04/04/2016	male	pune	poona hospital	abc	ab+	Fri 2016.05.27	Reject Accept



Email regarding new schemes/policies

User Email id : jawalkartejas@gmail.com
Subject : PM jandhan yojana
Attach file : Pradhan_Mantri_Jan.PDF

.



REGARDING CONFIRMATION OF GOVERNMENT POLICY/SCHEME

jawalkartejas@gmail.com
to me
3:02 PM (6 minutes ago)

Hello,dear user,You applied for new government scheme. Your scheme is now activated. Thank you for applying scheme...

15. REFERENCES:

1. R. Agrawal, A. Ev_mivski, and R. Srikant, "Information sharing across private databases", in Proceedings of the 2003 ACM SIGMOD, 2003.

2. F. Li, B. Luo, P. Liu, D. Lee, P. Mitra, W. Lee, and C. Chu, "In-broker access control: Towards e_cient end-to-end performance of information brokerage
systems", in Proc. IEEE SUTC, 2006.

3. 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.

4. 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 identication", J.AHIMA, vol. 77, pp. 64A-64D,
Jan. 2006

5. M. Siegenthaler and K. Birman, "Privacy enforcement for distributed healthcare queries", in Pervasive Health 2009, 2009.

6. 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 Proc.ACM CCS 07, 2007, pp. 508-518.

7. M.Murata, A. Tozawa, andM. Kudo, "XML access control using static analysis", in Proc. ACM CCS, 2003, pp. 73-84.34.

8. M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and effciently searchable encryption", in Proc. CRYPTO"07, Santa Barbara, CA, USA, pp.535"552.

9. G. Koloniari and E. Pitoura, "Content-based routing of path queries in peer-to-peer systems", in Proc. EDBT, 2004, pp.29-47