Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 8, August 2014, pg.41 – 48

RESEARCH ARTICLE

DESIGN AND IMPLEMENT PRIVACY PROTECTION FOR SECURE INFORMATION BROKERING SYSTEMS

SHAIK.MAHABOOB BASHA[1], A.BHASKAR[2], D.V SATISH KALADHAR REDDY[3]

[1]M.Tech 2nd Year, Dept. of CSE, ASCET, Gudur, India

[2]Asst Professor, Dept. of CSE, ASCET, Gudur, India

[3]M.Tech 2nd Year, Dept. of CSE, ASCET, Gudur, India

[1] mehaboob00786@gmail.com; [2] Alagala.bhaskar@gmail.com; [3] satheeshreddy562@gmail.com

ABSTRACT: Information Brokering Systems are attracting and increasing attention as an efficient means of sharing data among large, diverse and dynamic sets of user. The peer from logical over lay network by establishing links to some other peers they know are discover. A user in a peer-to-peer system in issues quires the describe data of interest the quires are propagated throw the overlay network to locate peer that provide data relevant to the query and only matching results are returned to the user. Information Brokering System (IBS) atop a peer-to-peer overlay has been proposed to support information sharing among loosely federated data sources. In existing IBSs adopt server side access control deployment and honest assumptions on brokers, and shack little observation on privacy of data and metadata stored and exchanged within the IBS. This paper studies the problem of privacy protection in information brokering process (PPIB). Then, this paper propose a broker-coordinator face, as well as two schemes, automaton segmentation scheme and query segment encryption scheme, to share the secure query routing use among a set of brokering servers. With comprehensive survey on privacy, end-to-end performance, and scalability, we show that the proposed system can combine security enforcement and query routing while preserving system-wide privacy with reasonable overhead. Further enhanced by Information Brokering System using Data Encryption Standard (DES), Digital Signature and XOR swap algorithm.

INDEX TERMS: PPIB, privacy, performance, segmentation, peer-to-peer system

INTRODUCTION

Privacy - preserving information sharing via on-demand information access. In this process an exile and scalable system using a broker-coordinator overlay network. Through an experimental automaton segmentation scheme, more access control implementation, and query segment encryption, our system integrates security enforcement and query forwarding while preserving system-wide privacy.

Information brokerage system [1], where sensitive information is shared among geographically distributed participants (e.g., users and data sources). To make the explanation simple, we assume that each broker has a full knowledge of whereabouts of stored data. Therefore, each broker may direct an inquiry to relevant data sources without consulting others (i.e., single-hop brokering).

In traditional DIBS, access control mechanisms are implemented at data servers so as to check the accessibility right of a query before answering it. However, claims that, whenever access control is enforced at the data source-side, suspicious queries are allowed to traverse through the whole system until they get rejected at the far end. Thus, by sending snooping queries, attackers can probe the system to get data distribution and server location information, and do further inferences after successfully ending out the location of sensitive data. In addition, source-side access control wastes substantial network.

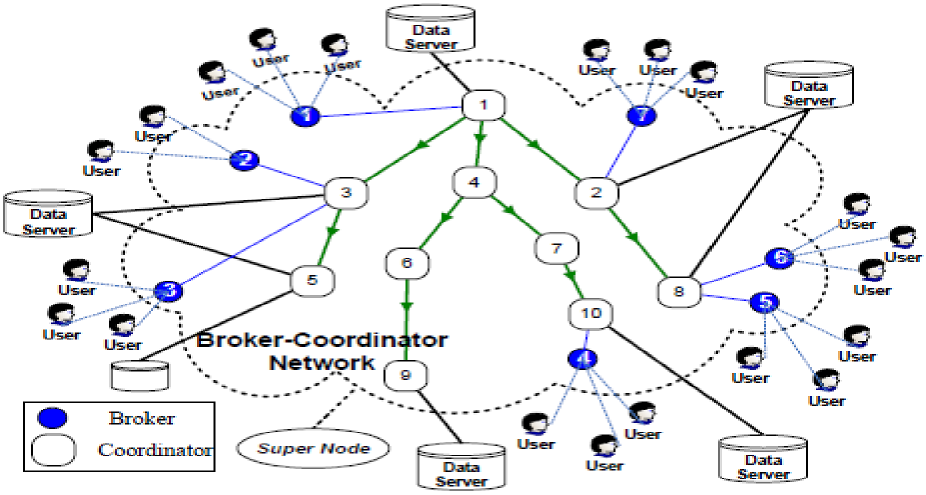


Fig: System architecture of a distributed information brokering system.

EXISTING SYSTEM

Today's world facilitates all services in information sharing via on-demand information access. In large scale information sharing, suppose that access to the database is strictly controlled, because data are used for certain experiments that need to be maintained confidential and provide privacy to the user. To provide privacy to the data and users in information sharing systems by using information brokering systems. By using IBS approach provides scalability and server autonomy, but privacy concerns brokers are not trustable.

Disadvantages:

1. Several types of attacks possible.
2. Another person to easily access database.

PROPOSED SYSTEM

In the current paper, our analysis of specify the privacy protection of information in brokering process. In the processes of protecting the information several types of attacks are possible in brokering process. Mainly focus on two major types of attacks: attribute-correlation attack and inference attack. In this process introduced an automatic segmentation scheme and query segment scheme. The information brokering system that exists suffers from a spectrum of vulnerabilities associated with user privacy, data privacy, and metadata privacy. Than proposes a new type of PPIB, a new approaches to preserve privacy in XML information brokering. The reference quoted by the user is sent through the brokers and coordinators to central web service zone where it is manipulated by the organizers. Intermediately to clear the intrusion, the quotation is secured using the concept of digital signature.

Advantages:

1. Very resistant to privacy attacks.
2. End-to-end query processing performance and
3. System scalability

MODULES

1. Co-Ordinator Module.
2. Broker Module.
3. User Module.
4. Admin Module.

Co-Ordinator Module:

In this module, the co-coordinator performs the global service between the two end users. Initially the Data possessor 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 co-Ordinator sends the key to the Data users and the Data will be passed by the broker Way.

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 [2]. The data will be passed from the co-coordinator and thus it will be submitted to the End Users (Data Users).

User Module:

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

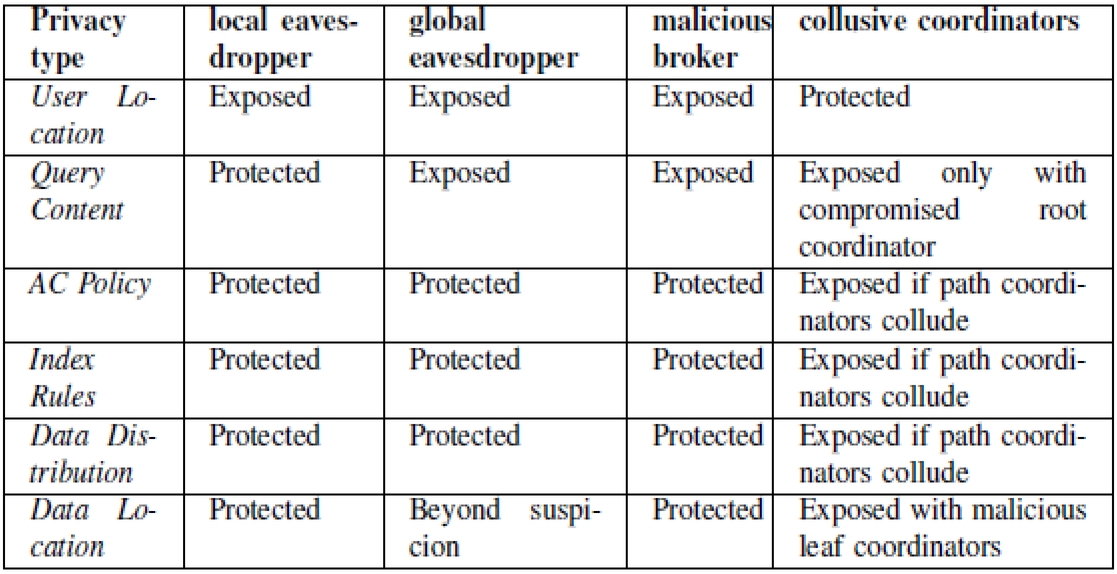
Admin Module:

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

IMPLEMENTATION

In this privacy protection analysis various types of attackers are including in information brokering process. Mainly there are three types of attackers possible, local and global eavesdroppers, mean brokers and more coordinators.

One idea is to build an XML overlay architecture that supports expressive query processing and security checking on top of normal IP network. In particular, designed data structures are maintained on nodes of the overlay networks to route path queries. In, a robust mesh has been built to



Privacy type	local eaves-dropper	global eavesdropper	malicious broker	collusive coordinators
User Location	Exposed	Exposed	Exposed	Protected
Query Content	Protected	Exposed	Exposed	Exposed only with compromised root coordinator
AC Policy	Protected	Protected	Protected	Exposed if path coordinators collude
Index Rules	Protected	Protected	Protected	Exposed if path coordinators collude
Data Distribution	Protected	Protected	Protected	Exposed if path coordinators collude
Data Location	Protected	Beyond suspicion	Protected	Exposed with malicious leaf coordinators

Table: The Possible Privacy Exposure Caused By Four Types of Attackers: Local Eavesdropper (LE), Global Eavesdropper (GE), Malicious Broker (ME), and Collusive Coordinators (CC).

Effectively route XML packets [3] by making the use of self-describing XML tags and the overlay networks. This describes a decentralized architecture for ad hoc XPath query routing across a collection of XML databases using the open and agreement cooperation models. In, content-based routing of path queries in peer-to-peer systems [6] is studied to serve the purpose as sharing data among a large number of independent nodes. The main difference between these approaches and ours is that they focus on distributed query routing, while we seamlessly combine query routing and security checking (e.g. access control) so as to preserve relevant privacy information.

Algorithm.1: Data Encryption Standard Algorithm:

```
Cipher (plain Block [64], Round Keys [16, 48], cipher Block [64])
{
    Permute (64, 64, plain Block, in Block, InitialPermutationTable)
     Split (64, 32, in Block, right Block, Round Keys [round])
      For (round =1 to 16)
       {
           Mixer (left Block, right Block, Round Keys [round])
           If  (round! =16) swapper (left Block, right Block)
       }
         Combine (32, 64, left Block, right Block, out Block)
         Permute (64, 64, out Block, chiperBlock, FinalPermutationTable)
 }
  Mixer (left Block [48], right Block [48], and Round Key [48])
    {
       Copy (32.rightBlock, T1)
       Function (T1, Round Key, T2)
       Exclusive Or (32, left Block, T2, T3)
       Copy (32, T3, right Block)
    }
   Swapper (left Block [32], right Block [32])
         {
              Copy (32, left Block, T)
              Copy (32, right Block, left Block)
              Copy (32, left Block, right Block)
         }
Function (in Block [32], Round Key [48], out Block [32])
{
Permute (32, 48, in Block, T1, ExpansionPermutationTable)
Exclusive Or (48, T1, Round Key, T2)
Substitute (T2, T3, Substitute Tables)
Permute (32, 32, T3, out Block, StraightPermutationTable)
}
Substitute (in Block [32], out Block [48], Substitution Table [8, 4, and 16])
```

```
{
   For (i=1to8)
   {
      Row←2×inBlock [i×6+1] +in Block [i×6+6]
      Col←2×inBlock [i×6+2] +4×in Block [i×6+3] +2×inBlock [i×6+4] +in Block [i×6+5]
          Value=SubstitutaionTable [i][row][col]
            Out Block [[i×4+1]←value/8;
            Out Block [[i×4+2]←value/4;             value←value mod 8
            Out Block [[i×4+3]←value/2;             value←value mod 4
            Out Block [[i×4+4]←value                value← value mod 2

      }
}
```

Algorithm.2: XOR SWAP ALGORITHM: In computer programming languages, the XOR swap is an algorithm that uses the XOR bitwise operation to swap values of distinct variables having the same data type without using a temporary variable. "Decided" means that the variables are stored at different memory addresses; the actual values of the variables do not have to be different. Conventional swapping requires the use of a temporary storage variable. Using the XOR swap algorithm, however, no temporary storage is needed. The algorithm is as follows:

```
X: = X XOR Y
Y: = X XOR Y
X: = X XOR Y
```

The XOR algorithm typically corresponds to three machine code instructions. Since XOR is a commutative operation, X XOR Y can be replaced with Y XOR X in any of the lines. When coded in assembly language, this commutatively is often exercised in the second line.

```
   XR    R1, R2
   XR    R2, R1
XR    R1, R2
```

Where R1 and R2 are distinct registers and each XR operation leaves its result in the register named in the first argument. However, the algorithm fails if x and y use the same storage location, since the value stored in that location will be zeroed out by the first XOR instruction, and then remain zero; it will not be "swapped with itself".

DES is the archetypal block cipher — an algorithm that takes a fixed-length string of plaintext bits and transforms it through a series of complicated operations into another cipher text bit string of the same length. In the case of DES, the block size is 64 bits. DES also uses a key to modify the transformation, so that decryption can believe only be performed by those who know the particular key used to encrypt. The key professedly consists of 64 bits; however, only 56 of these are literally used by the algorithm. Eight bits are used solely for survey parity, and are thereafter dispose. Hence the effective key length is 56 bits, and it is always quoted as such then we assign each segment to one independent site. However, in the state transition table of the last state of each segment, the “next state" points to a root state at a remote site, instead of a local state. The dummy accept states do Not accept queries. Instead, they are used to store the location of actual “next states," i.e. the address (es) of the coordinators who hold the next segment of the global automaton. At runtime, they are used to forward the halfway processed query to the next coordinators. On the other hand, only the sites holding original accept states accept queries and forward them to the data servers. As a result, access control and query brokering are seamlessly integrated at coordinators, and the global automaton-based query brokering mechanism is decentralized and distributed among many coordinators.

CONCLUSION AND FUTURE ENHANCEMENT

The information brokering system that exists suffers from a spectrum of vulnerabilities associated with user privacy, data privacy, and metadata privacy. By compose the access authority policies into the data encryption, accessible client based access control solutions diminish the trust required on the client at the price of a certain extent static way of sharing data. It advances PPIB, a new approach to maintain privacy in XML information brokering. The reference quoted by the user is sent through the brokers and coordinators to central web service zone where it is manipulated by the organizers. Intermediately to circumvent the intrusion, the quotation is attached using the concept of digital signature. In future prospective, we want to develop an automatic scheme that does dynamic site allotment. And also consider the several factors can be in the scheme such as workload at each peer, trust level of each peer and privacy dispute between automaton segments. In near future we investigating the client-based security solutions. And also we planned to minimize or eliminate or eliminate the participation of the admin node.

REFERENCES

1. P. F. Syverson, D. M. Goldschlag, and M. G. Reed.Anonymous connections and onion routing. In IEEE Symposium on Security and Privacy, pages 44-54, Oakland, California, 1997.

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

3. Fengjun Li, Bo Luo, Peng Liu, Dongwon Lee, and Chao-Hsien Chu**,”** Automaton Segmentation: A New Approach to Preserve Privacy in XML Information Brokering **“,** the Pennsylvania State University University Park, PA 16802, USA {fengjun, bluo, pxl20, dongwon, chc4}@psu.edu.

4. Internet traffic report.http://www.internettra_creport.com.

5. R. Agrawal, A. V. Evmievski, and R. Srikant. Information sharing across private databases. In SIGMOD, pages 86-97, 2003.

6. A. Carzaniga, M. J. Rutherford, and A. L. Wolf. A routing scheme for content-based networking. In Proc. Of.INFOCOM, 2004.

7. S. Cho, S. Amer-Yahia, L. V. S. Lakshmanan, and D. Srivastava. Optimizing the secure evaluation Of twig queries. In VLDB, pages 490-501, China, 2002.

8. E. Damiani, S. Vimercati, S. Paraboschi, and P. Samarati. A fine-grained access control system for XML documents. ACM Trans. Inf. Syst. Secur., 5(2):169{202, 2002.

9. Y. Diao, S. Rizvi, and M. J. Franklin. Towards an Internet-scale XML dissemination service. In VLDB, Toronto, 2004.

AUTHORS

Shaik. Mahaboob Basha received the Quba college of Engineering &Technology B-Tech degree in computer science engineering from the Jawaharlal Nehru technological university Anantapur, in 2012, and received the Audisankara College of Engineering and Technology M-Tech degree in Software engineering from the Jawaharlal Nehru technological university Anantapur in 2014; He interests Secure Computing and Software Engineering.

A.Bhaskar received the PBR Visvodaya Institute of Technology & Science B-Tech degree in computer science engineering from the Jawaharlal Nehru technological university Hyderabad, and received the M.E degree in Computer Science engineering from the Anna University Chennai, respectively. He interests DMDW and Distributed systems and Service-Oriented Architecture.

D.V Sateesh Kaladhar Reddy received the PBR Visvodaya Institute of Technology & Science B-Tech degree in computer science engineering from the Jawaharlal Nehru technological university Anantapur, in 2011, and received the Audisankara College of Engineering and Technology M-Tech degree in Software engineering from the Jawaharlal Nehru technological university Anantapur in 2014, respectively. He interests Computer Networks and Mobile Computing and network programming. He is a member of the IEEE.