PRIVACY INFORMATION BROKERING SYSTEM USING AUTOMATON SEGMENTATION ALGORITHM

Subhedar Pitamber[1], Sapkal Prajyot[2], More Dhairyashil[3]

[1] *BE Computer, Department of Computer Engineering, DGOIFOE Daund, Maharashtra, India*
[2] *BE Computer, Department of Computer Engineering, DGOIFOE Daund, Maharashtra, India*
[3] *BE Computer, Department of Computer Engineering, DGOIFOE Daund, Maharashtra, India*

Abstract - ***This system is develop for secure information brokering. The system provides information sharing in more secure and privacy preserving manner. It show that the system can integrate security enforcement and query routing. In this system we implement automaton segmentation algorithm. The need of information sharing via on demand information access increases rapidly. The system provides access control for user and broker. The broker performs the important role in brokering process. The admin maintains database in system. Many existing systems assume that brokers are trusted and thus only perform database side access control for data confidentiality. The privacy of data location and data user can still be inferred from database (using query and access control rules) exchanged within the system, but small attention has been put on system protection.***

Key Words: *Access control, Automaton segmentation, Information sharing, Query segment encryption.*

1. INTRODUCTION

The privacy information brokering system is dedicated to those organizations where privacy of information is first priority. The need of efficient and secure information is more in government and private organization. The system provides security to information while sharing. The aim of system is provide efficient and secure data sharing. The variety of data or information is available but some data are private such as medical information of patient, confidential information about security of country.

In this system admin provides the platform to user and broker to share the information. The coordinator is not active while during the process of brokering. The system manages admin, user, broker and coordinator records. The mainly information brokering process is carried out between user and user. The system assign unique secrete key for each transaction or sharing process.

Once the secrete key is generated and it assign to the transaction then without this secrete key does not possible to access those information. The system provides privileges to user such as Insert, Delete, Update etc. User works with provided privilege. The secrete key is send to user via E-mail which is provided in User Profile.

1.1 IDENTIFICATION OF PROBLEM

The old system does not provides the unique secrete key for transaction of sharing information. The modification of shared information is possible to unauthorized person but in this system that problem is overcome using sending secrete key to user via E-mail.

The older system only share information in organization. The information is open and accessible to each and every user in organization. The privacy of information is not preserved in older system.

1.2 OBJECTIVES

1. To provide a cost effective comfortable safe and more secure information brokering system.
2. To provide efficient mechanism for managing privacy in information brokering.

2. SYSTEM OVERVIEW

Proposed system is fully integrated. The huge amount of time is save with system. Database is maintain so properly so that managing and keeping brokering record is very easy. The system works real time with privacy preserving manner. Mainly system is divided into four modules. Each module coordinates each other while system is running. In this system we preserve the privacy of information. The system keeps information safe from unauthorized persons.

3. SYSTEM ARCHITECTURE

The implementation is achieved throughout approach for privacy information brokering system. There are four modules are as follows

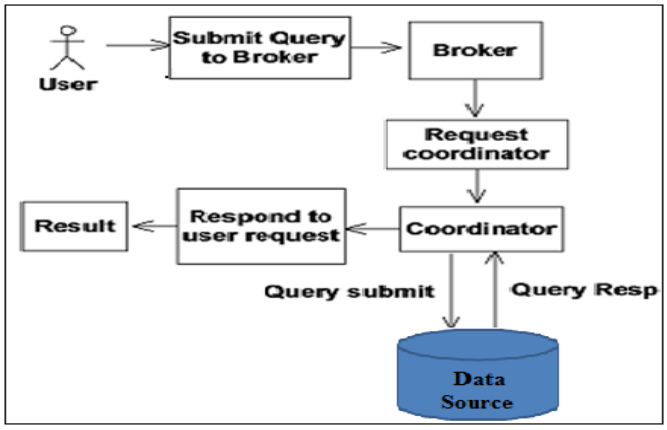

Fig 1. System Architecture

Admin Module:

Admin performs important roles in registration of data owners and users, brokers, coordinators and organization in PIBS. Admin also manages the database.

User Module:

The Users are Data Users and Data Owner. The role and privileges on the data that will be send to the coordinator. The coordinator sends the details to broker and verified it with the secret key. The data will be displayed to users.

Broker Module:

The broker is mediator between data Users and coordinator. The query submitted by a data user gets verified using secret key and passed to the coordinator.

Coordinator Module:

The broker with his secrete key verifies a query, he submits it to the coordinator and turn searches are sends the key to the data users via broker. Coordinator also performs the global service between two end users via broker.

4. AUTOMATON SEGMENTATION ALGORITHAM

Input: Automaton State S
Output: Segment Address: addr

Step 1 : User submits a query to broker in the form of string.

for each symbol k in S:StateT ransT able do
addr=deploySegment(S:StateT ransT able(k):nextState)

Step 2 : The broker verifies the query with his secrete key and forward query to the coordinator.

DS=createDummyAcceptState()
DS:nextState addr
S:StateT ransT able(k):nextState DS

Step 3 : The coordinator validates brokers secrete key and submits this query to the database.

Seg = createSegment()
Seg:addSegment(S)
Coordinator = getCoordinator()

Step 4 : The unique secret key is present in the database. The fetched query is passed throw coordinator to user by the broker way.

Coordinator:assignSegment(Seg)
return Coordinator : address

5. INFORMATION BROKERING SYSTEM

The IBS has three brokering components:
1. Brokers
2. Coordinators
3. Central authority

The local brokers (green nodes in Fig 2) and database request to the different organizations for connecting the system.

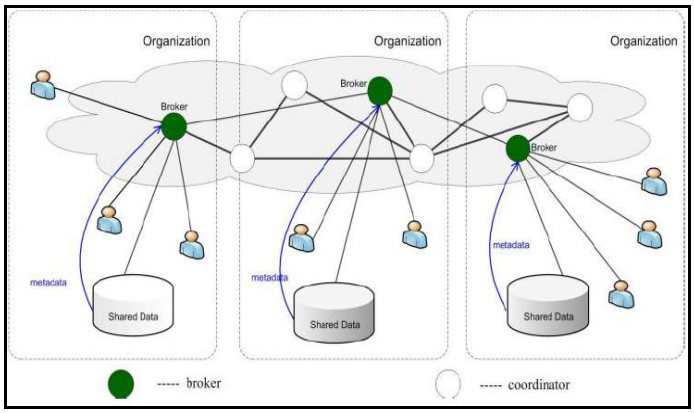

Fig 2. Information Brokering System.

Brokers :

The broker communicate through coordinators. The function of local broker is the “entry” to the system. The broker is responsible for authenticates requestors and hides them. It would also permute query sequence to protect against local traffic analysis.

Coordinators :

The coordinators responsible for content-based query routing and access control authentication. With privacy-preserving manner, coordinator cannot hold any rule in the complete form. The Coordinators operate

collaboratively to enforce secure query routing. Coordinator prevents from sensitive predicates, a query segment encryption scheme and automaton segmentation scheme, query divide into segment and encrypt in each segment.

Central authority :

It is responsible for key management and database maintenance.

6. INFORMATION BROKERING PROCESS

Phase 1:

In this system, a user needs to authenticate to the local broker and the user submits encrypted segment an XML query using public level keys, and a unique session key Ks, data servers encrypted with the public key, to return data.

Phase 2:

The major task of the broker is database preparation. It extracts the role of the user authenticated and attaches it to the encrypted XML query. It make a unique secrete key for each query, and attaches secrete key with its own address (As < Ks >pkDS) to the query so that the database can directly return the data.

Phase 3:

When the query receives the root of the coordinator and its database from a local broker, it take place following schemes i.e. the automata segmentation scheme for segment the XML query. The query segment encryption scheme to perform access control and to route the query within the coordinator tree. Until it reaches a leaf coordinator, which sends the query to the related database.

Phase 4:

In the final phase, the database gets a safe query in an encrypted form. The data server evaluates the query and returns the data after decryption, encrypted by Ks, to the broker of the query.

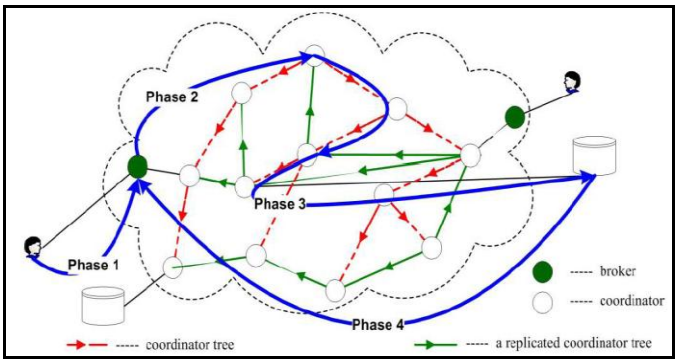

Fig 3. Query brokering process.

7. CONCLUSIONS

We proposed a new system approach in privacy information brokering application for information sharing. Our system reduce time complexity and provide high security to information.

REFERENCES

[1] Fengjun Li, Bo Luo, Peng Liu Dongwon Lee and Chao-Hsien Chu, *"Enforcing Secure and Privacy-Preserving Information Brokering in Distributed Information Sharing"*, IEEE TRANSCATIONS ON INFORMATION FORENSICS AND SECURITY, 2013.

[2] 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 ACM CCS '07, pp. 508–518, 2007.

[3] 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.

[4] W. Bartschat, J. Burrington-Brown, S. Carey, J. Chen, S. Deming, and S. Durkin, *"Surveying the RHIO landscape: A escription of current RHIO models, with a focus on patient identification,"* Journal of AHIMA 77, pp. 64A–D, January 2006.

[5] X.Zhang, J. Liu, B. Li, and T.-S. P. Yum, *"CoolStreaming / DONet: A data-driven overlay network for efficient live media streaming,"* in Proceedings of IEEE INFOCOM, 2005.

[6] M. Franklin, A. Halevy, and D. Maier, *"From databases to dataspaces: a new abstraction for information management,"* SIGMOD Rec., vol. 34, no. 4, pp. 27–33, 2005.

[7] R. Agrawal, A. Evfimivski, and R. Srikant, *"Information sharing across private databases,"* in Proceedings of the 2003 ACM SIGMOD, 2003.

[8] A. C. Snoeren, K. Conley, and D. K. Gifford, *"Mesh-based content routing using XML,"* in SOSP, pp. 160–173, 2001.