ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Ensuring Privacy of Various Stakeholders In Process of Information Brokering

Lavanya Ganji
M.Tech Student,
Auroras Scientific Technological and Research Academy.

A.Bhakiya Lakshmi
Assistant Professor,
Auroras Scientific Technological and Research Academy.

Swapna
Associate Professor,
Auroras Scientific Technological and Research Academy.

Abstract:

An information brokering system collects information, the data is then sold to companies that use it to target advertising and marketing towards specific groups, to verify a person's identity including for purposes of fraud detection, and to sell to individuals and organizations so they can research particular individuals. Distributed information systems emerged as solution for the needs of enterprises that share information via on-demand access. Information Brokering Systems (IBSs) came into existence to leverage usefulness of sharing information among organizations. The IBS is responsible to integrate loosely coupled systems forming a brokering overlay. The existing IBSs believe that the brokers are trusted and data can be shared through them confidently.

However, adversaries can infer information from the metadata available. This is the problem to be addressed by many researchers. They focused two kinds of privacy attacks namely inference attack and attribute-correlation attack. They also proposed two solutions for preventing these attacks. They are query segment encryption and automaton segmentation respectively. With insignificant overhead, their approach provides system-wide security. In this paper, we implemented privacy preserving on-demand access to distributed information brokering system. We built a prototype application that demonstrates the proof of concept.

Keywords:

Security, Encryption, Decryption, Privacy-Preserving, Key-exchange, Information brokering system and access control.

Introduction:

Data is essentially the plain facts and statistics collected during the operations of a business. They can be used to measure/record a wide range of business activities - both internal and external. While the data itself may not be very informative, it is the basis for all reporting and as such is crucial in business. The importance of data cannot be under-stated as it provides the basis for reporting the information required in business operations. The way a business gathers shares and exploits this knowledge can be central to its ability to develop successfully. This doesn't just apply to huge multinational companies but also to smaller organisation.

Information that is obtained from processing data is more useful as it can help in making well informed decisions. In the context of modern organizations that have collaborations with other organizations including supply chain management systems, health care organizations, banks, insurance companies, governments, law enforcement agencies etc. need information sharing for successfully achieving their goals. Businesses cannot standalone or the government organizations.

There is need for information sharing at all levels to be successful and strategic in dealing with issues.Information brokering systems integrated many companies or businesses or organizations that can provide data to other organizations through brokering system. Brokers are the intermediary organizations or people who can provide data to client organizations. In this context, brokers are trusted in the existing systems. In reality when broker has bad intentions, he can steal sensitive information and have monetary gains. To avoid this brokers are to be considered as possible threats to security.

Related Work:

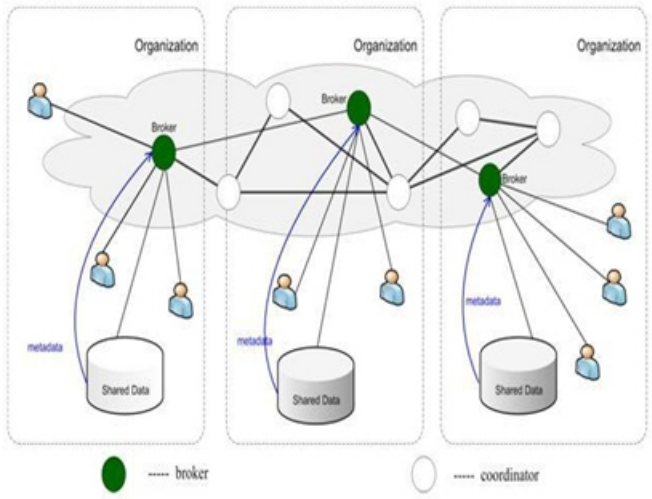
Recently Li et al. [1] proposed information brokering system which is secure and privacy preserving. In this system two attacks such as inference attacks and attribute – correlation attacks are considered. The solutions are given for these two attacks.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

The work done in [1] influenced our work in this paper which focuses on building a prototype that demonstrates the privacy preserving information brokering with an additional layer that coordinates and ensures that brokers can't involve in fraudulent activities.Data sharing problem has attracted significant research efforts. The systems like publish-subscribe and peer-topeer is used for file sharing. Many such systems came into existence as explored in [2] and [3]. For secure information sharing, distributed hash table technology is also widely used [4], [5]. XML publish-subscribe were also explored in [6], [7] that is closely related to the solutions pertaining to privacy preserving information brokering. A robust mesh is used in [8] for routing XML packets with a gab based solution for overlay networks. XPath query related routing [9] is also used in XML databases and content-based routing was also used in P2P systems.

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, aa 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, endto- 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.

ARCHITECTURE:



Brokers:

It is intercommunicating through coordinators. A local broker functions as the "entry" to the system. It's responsible for authenticates requestors and hides their. It would also permute query sequence to defend against local traffic analysis.

Coordinators:

It is responsible for content-based query routing and access control actuation. With privacy-preserving idea, coordinator cannot hold any rule in the complete form. Instead, a novel automaton segmentation scheme to divide (i.e. metadata) rules into segments and assign each segment to a coordinator. 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 it (each segment)

Central Authority (CA):

It is responsible for key management and metadata maintenance

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 managed by Alice is violated once Bob has access to the contents of the database. 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.

Disadvantages:

1.The database with the tuple data does not be maintained confidentially.
2.The existing systems another person to easily access database.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

PROPOSED SYSTEM:

In the current paper, 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.

Advantages:

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

ALGORITHMS:

A. Automation Segmentation:

The data is share between multiple organizations. Organizations have their own ideas and goals. Global components are divided locally and forwarded to the coordinators. The query must be partitioned into multiple parts and parts are forwarded to the local coordinators. Automation Segmentation includes deployment, segmentation and replication.

B. Query Segment encryption using RC6:

The segmented query is encrypted by the coordinator which is supposed to process. Here the coordinator uses the key to encrypt the query segment. The coordinator used the public key to encrypt. It only sees the slight portion of the query that cannot be inferred. Other than central authority no one knows the global segmentation. Once the query has been encrypted by the coordinator it has been send to the next coordinator. In that case the query must be prevented until it reaches its data server. Thus the post encryption has been handled ad the query has been successfully forwarded to the destination.

C. Key-exchange using Speke:

Password-authenticated key agreement method is an interactive method for two or more parties to establish cryptographic keys based on one or more party's knowledge of a password.

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 Owner 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 request which are all submitted from the data user will be verified and thus it will be passed to the co-coordinator. 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 Depends on the restriction the data will be passed to the Co-coordinator.The co-coordinator pass 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 register and register the Organization and Users Forms.

Conclusion:

In this paper, we studied the problem of privacy preserving information brokering. Information brokering is a distributed approach in which many organizations involve in sharing information through brokers. In the existing solutions, brokers are treated as trusted which is not the case

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

in the real world applications. Later coordinators were introduced to monitor brokers. Li et al. [1] focused on this kind of solution which prevents two kinds of attacks namely inference attack and attributecorrelation attack using solutions such as automaton segmentation, and query segment encryption. In this paper we implement a prototype application that demonstrates the proof of concept. The experimental results reveal that the proposed application has many layers of security where the coordinators monitor the brokers and ensure privacy preserving information brokering. As future work, we focus on the information brokering system with a mobile application.

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]I. Manolescu, D. Florescu, and D. Kossmann, "Answering XML queries on heterogeneous data sources," in Proc. VLDB, 2001, pp. 241–250.

[3]M. Genesereth, A. Keller, and O.Duschka, "Informaster: An information integration system," in Proc. SIGMOD, Tucson, AZ, USA, 1997.

[4]R. Huebsch, B. Chun, J. Hellerstein, B. Loo, P. Maniatis, T. Roscoe, S. Shenker, I. Stoica, and A. Yumerefendi, "The architecture of PIER: An Internet-scale query processor," in Proc. CIDR, 2005, pp. 28– 43.

[5]I. Stoica, R. Morris, D. Liben-Nowell, D. Karger, M. Kaashoek, F. Dabek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup protocol for Internet applications," IEEE/ACM Trans. Netw., vol. 11, no. 1, pp. 17–32, Feb. 2003.

[6]Y. Diao, S. Rizvi, and M. J. Franklin, "Towards an Internet-scale XML dissemination service," in Proc. VLDB Conf., Toronto, Canada, Aug. 2004.

[7]A. Carzaniga, M. J.Rutherford, andA. L.Wolf, "Arouting scheme for content-based networking," in Proc. INFOCOM, Hong Kong, 2004, pp. 918–928.

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

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

[10] M. Bellare, A. Boldyreva, and A. O'Neill, "Deterministic and efficiently searchable encryption," in Proc. CRYPTO'07, Santa Barbara, CA, USA, pp.535–552.

[11] Bhandekar Harika, P. Rajendra Prasad, T.Madhu, Privacy Preserving of Outsourced Data Using AttributeBased Encryption,IJMETMR,http://www.ijmetmr.com/oljuly2015/BhandekarHarika -PRajendraPrasad-TMadhu-22.pdf, Volume No: 2 (2015), Issue No: 7 (July)