ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 11, November 2014

Secure and Dynamic On-Demand Access to Distributed Information through Information Brokering System

K.P.Karthik[1], C.Vasumurthy[2], S.NG.Nawaz[3]

Student, Computer science, S.K.D Engineering College, Gooty, Anantapuramu, India[1]

Asst professor, Computer science and Engineering, S.K.D Engineering College, Gooty, Anantapuramu, India[2]

Assoc professor, Computer science and Engineering, S.K.D Engineering College, Gooty, Anantapuramu, India[3]

Abstract: 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. Recently Li et al. proposed an approach for privacy preserving information brokering. 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, privacy, information brokering, and access control

I. INTRODUCTION

Data plays an important role for every organization or business or government. 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. By the same token it is understood that information brokering systems came into existence. 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.

Recently Li et al. [19] 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. The work done in [19] 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. The remainder of this paper is structured as follows. Section II presents review of literature. Section III presents proposed system and prototype. Section IV presents experimental results while section V concludes the paper

II. RELATED WORKS

Data sharing problem has attracted significant research efforts. The systems like publish-subscribe and peer-to-peer is used for file sharing. Many such systems came into existence as explored in [1], [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. To protect data from untrusted brokering encrypting metadata is also used. For searchable encryption towards that end was discussed in [10], [11] and [12]. Keyword based search and the information retrieval and sharing was explored in [13].

Relaying information from sender node was focused in [14] and [15]. Such approaches were used for privacy preserving information brokering. There are a host of challenges to achieve this other than the anonymity problem. Access control mechanism were explored in [16] in a distributed environment for collaborative data processing. Access control approaches that are view based are provided in [17] and [18]. They incurred high storage and maintenance costs. Thus they were not feasible in the real world applications. For perfect information brokering with security and privacy to data and data owners, NFA based approach is followed by Li et al. [19] which proved to be more efficient when compared with prior approaches that came into existence on view – based schemes.

III. PROPOSED SOLUTION AND THE PROTOTYPE

We built a prototype application for secure and privacy preserving information brokering. Our system is based on the insights from Li et al. [19] which explore two kinds of attacks such as inference attack and attribute –correlation attack in distributed environment. Our application was built using Microsoft .NET platform using Web Forms. The application is able to demonstrate various layers of security with privacy preserving information brokering.

A healthcare application is taken as case study. Many users interact with system with given access rights. The information flow is as per the business rules and the security is provided to the information dissemination process. Some of the important screens used by the players of the application are provided here.

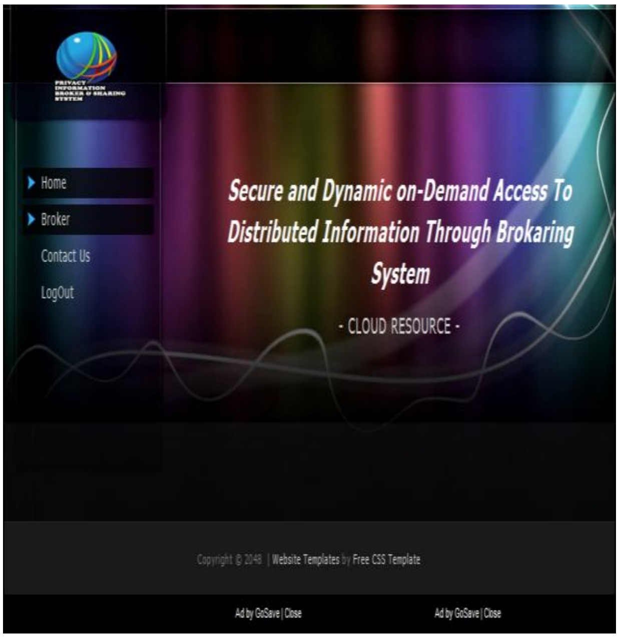

PRIVACY INFORMATION BROKER & SHARING SYSTEM
Home
Broker
Contact Us
LogOut
Secure and Dynamic on-Demand Access To Distributed Information Through Brokaring System
- CLOUD RESOURCE -
Copyright © 2048 | Website Templates by Free CSS Template
Ad by GoSave | Close
Ad by GoSave | Close

Figure 1 – UI for data provider

As can be seen in Figure 1, it is evident that the data provider can give information required. In this case the data provider is the patient in hospital. This information is used for sharing with other users as per the business rules. Data provider can perform other operations as specified in the menu.

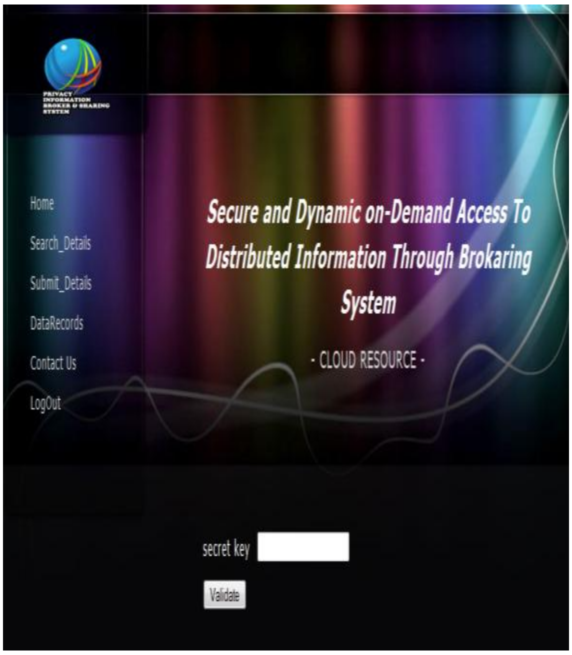
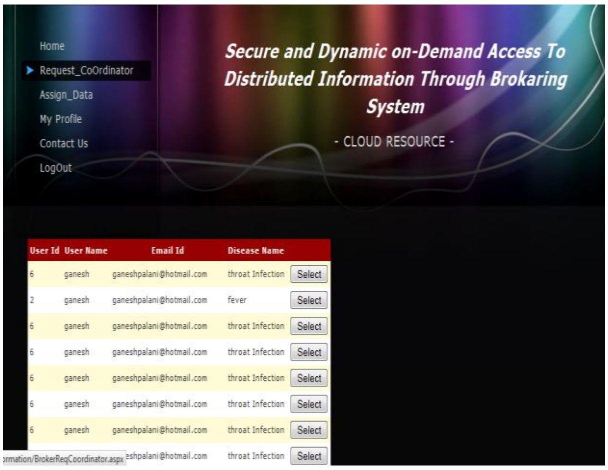

PRIVACY INFORMATION BROKER & SHARING SYSTEM
Home
Search_Details
Submit_Details
DataRecords
Contact Us
LogOut
Secure and Dynamic on-Demand Access To Distributed Information Through Brokaring System
- CLOUD RESOURCE -
secret key
Validate

Figure 2 – UI for broker

As can be seen in Figure 2, it is evident that the broker can perform intended operations. In this case the broker can request coordinator to grant permissions. As per the permissions provided by the coordinator, the broker can share information to authorized users of the application.


Home
Request_CoOrdinator
Assign_Data
My Profile
Contact Us
LogOut
Secure and Dynamic on-Demand Access To Distributed Information Through Brokaring System
- CLOUD RESOURCE -
ormation/BrokerReqCoordinator.aspx

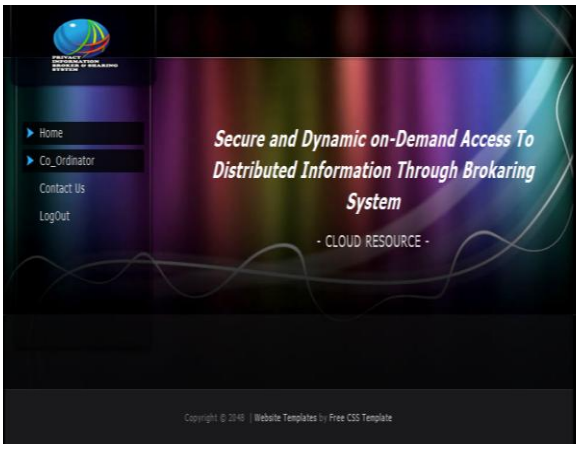
User Id	User Name	Email Id	Disease Name	
6	ganesh	ganeshpalani@hotmail.com	throat Infection	Select
2	ganesh	ganeshpalani@hotmail.com	fever	Select
6	ganesh	ganeshpalani@hotmail.com	throat Infection	Select
6	ganesh	ganeshpalani@hotmail.com	throat Infection	Select
6	ganesh	ganeshpalani@hotmail.com	throat Infection	Select
6	ganesh	ganeshpalani@hotmail.com	throat Infection	Select
6	ganesh	ganeshpalani@hotmail.com	throat Infection	Select
		eshpalani@hotmail.com	throat Infection	Select

Figure 3 – Other UI for broker

Here the broker can request for the required information which he needs to share to users in distributed environment. The requests given by broker can be viewed and processed by the coordinator with underlying secure procedures fulfilled.

As can be seen in Figure 4, it is evident that the coordinator can perform intended operations. In this he can grant privileges to broker to share information to users. As per the permissions provided by the coordinator, the broker can share information to authorized users of the application.

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940



Secure and Dynamic on-Demand Access To Distributed Information Through Brokaring System

- CLOUD RESOURCE -

Figure 4 – UI for coordinator

IV. EXPERIMENTAL RESULTS

Experiments are made with the prototype application in terms of system scalability using simple path rules, XPath rules and wildcards, XPath queries, rules with wildcards, rules with 5% wildcards probability, and wildcards with 5% probability. Other aspects considered are number of access control rules, number of coordinators, number of queries in unit time, and number of total segments.

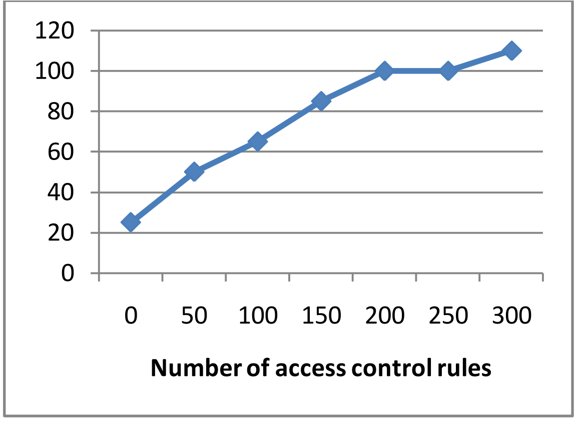


Figure 5 – System scalability using simple path rules

As can be seen in Figure 5, it is evident that the horizontal axis represents number of access control rules while the vertical axis represents number of coordinators. The results reveal the scalability dynamics of the system in terms of simple path rules.

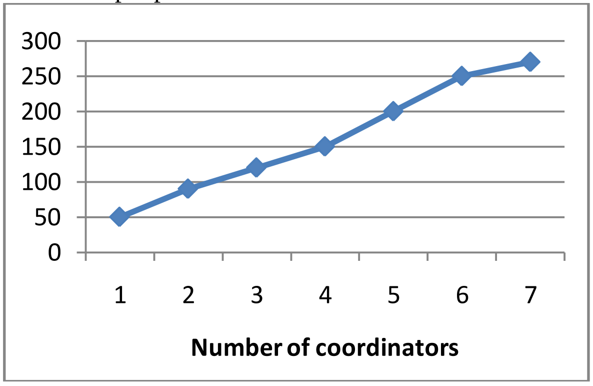


Figure 6 – System scalability using XPath rules with wildcards

As can be seen in Figure 6, it is evident that the horizontal axis represents number of access control rules while the vertical axis represents number of coordinators. The results reveal the scalability dynamics of the system in terms of XPath rules and wildcards.

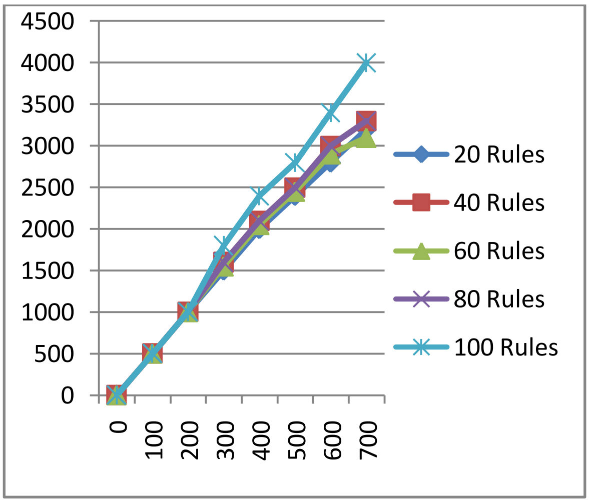


Figure 7 – System scalability using XPath queries and simple XPath rules

As can be seen in Figure 7, it is evident that the horizontal axis represents number of queries in a unit time while the vertical axis represents number of total segments in the system. The results reveal the scalability dynamics of the system in terms of XPath rules and simple XPath rules.

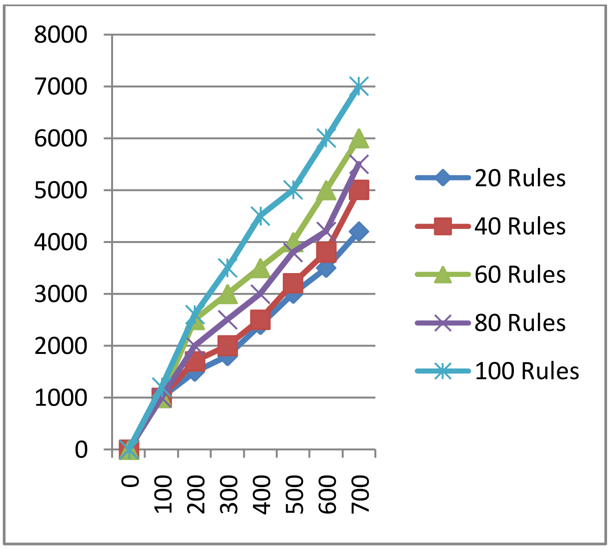


Figure 8 – System scalability using rules with wildcards and XPath queries

As can be seen in Figure 8, it is evident that the horizontal axis represents number of queries in a unit time while the vertical axis represents number of total segments in the system. The results reveal the scalability dynamics of the system in terms of wildcards and simple XPath rules.

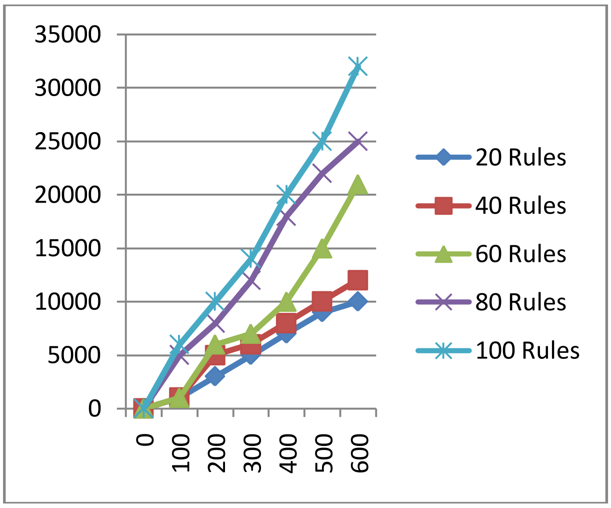


Figure 9 – System scalability with rues and queries using 5% probability

As can be seen in Figure 9, it is evident that the horizontal axis represents number of queries in a unit time while the vertical axis represents number of total segments in the system. The results reveal the scalability dynamics of the system in terms of rules with 5% wildcards and simple queries.

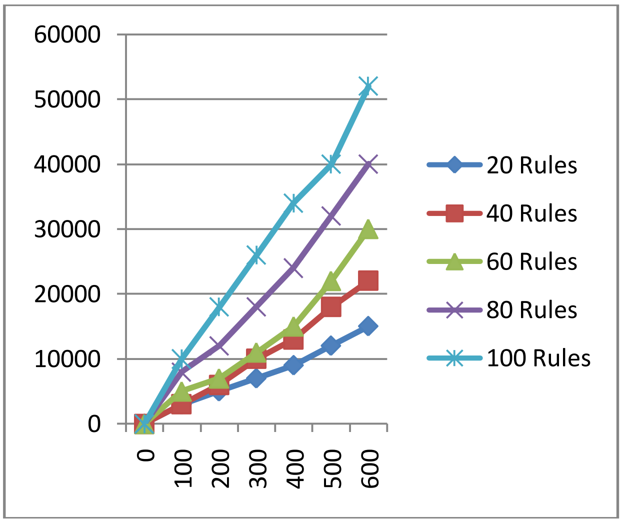


Figure 10 – System scalability using ACR and query with 10% wildcard probability

As can be seen in Figure 10, it is evident that the horizontal axis represents number of queries in a unit time while the vertical axis represents number of total segments in the system. The results reveal the scalability dynamics of the system in terms of ACR with 10% wildcards and queries.

V. CONCLUSIONS AND FUTURE WORK

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 in the real world applications. Later coordinators were introduced to monitor brokers. Li et al. [19] focused on this kind of solution which prevents two kinds of attacks namely inference attack and attribute-correlation 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] J. Kang and J. F. Naughton, “On schemamatching with opaque column names and data values,” in *Proc. SIGMOD*, 2003, pp. 205–216.

[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] C. Wang, N. Cao, J. Li, K. Ren, and W. Lou, “Secure ranked keyword search over encrypted cloud data,” in *Proc. ICDCS’10*, Genoa, Italy, pp. 253–262.

[12] D. Song, D. Wagner, and A. Perrig, “Practical techniques for searches on encrypted data,” in*Proc. IEEE Symposiumon Security and Privacy*, 2000, pp. 44–55.

[13] M. J. Freedman,Y. Ishai, B. Pinkas, and O. Reingold, “Keyword search and oblivious pseudorandom functions,” in *Proc. TCC’05*, Cambridge, MA, USA, pp. 303–324.

[14] P. F. Syverson, D. M. Goldschlag, and M. G. Reed, “Anonymous connections and onion routing,” in *Proc. IEEE S&P*, 1997, pp. 44–54.

[15] M. K. Reiter and A. D. Rubin, “Crowds: anonymity for web transactions,” *ACM Trans. Inf. Syst. Security*, vol. 1, no. 1, pp. 66–92, 1998.

[16] W. Tolone, G.-J. Ahn, T. Pai, and S.-P. Hong, “Access control in collaborative systems,” *ACM Comput. Surv.*, vol. 37, no. 1, pp. 29–41, 2005.

[17] T. Yu, D. Srivastava, L. V. S. Lakshmanan, and H. V. Jagadish, “Compressed accessibility map: Efficient access control for XML,” in *Proc. VLDB*, China, 2002, pp. 478–489

[18] S. Rizvi, A. Mendelzon, S. Sudarshan, and P. Roy, “Extending query rewriting techniques for fine-grained access control,” in *Proc. SIGMOD’04*, Paris, France, 2004, pp. 551–562.

[19] Fengjun Li, Bo Luo, Peng Liu, Dongwon Lee, and Chao-Hsien Chu. (2013). Enforcing Secure and Privacy-Preserving Information Brokering in Distributed Information Sharing. *IEEE*. 8 (6), p888-900.