IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Vol. 05, Issue 01, January 2015, ||V1|| PP 58-62

Efficient Control of Information Brokerage Systems in Distributed Networks

[1]Mrs. Sindhuja M, [2]Mr. S. Niresh Kumar, [3]Mrs. Thaiyalnayaki S,
[1]*Dhanalakshmi Srinivasan College of Engineering and Technology*
[2]*Dhanalakshmi Srinivasan College of Engineering and Technology*
[3]*Dhanalakshmi Srinivasan College of Engineering and Technology*

Abstract: Information brokering systems (IBSs) are planned to connect many data sources via a brokering edge, that the brokers route their decisions to direct client queries to the requested data servers. Most of the prevailing brokering systems like global organization agency shares data through brokers and conjointly assumes that brokers square measure sure so exclusively agree server-side access control for information privacy. However, privacy of information location and client data can still be collected from information modified among the IBS. In this paper, we propose an approach to preserve privacy of multiple stakeholders involved at intervals in the data brokering system by using Personal Health Records as the case study. In the proposed system an encryption scheme known as Jasypt to provide the strong encryption and also providing the Load Balancing algorithm to avoid data loss and finally a new technique known as Proxy Re-Encryption to provide the double Encryption for the Sensitive data.

I. INTRODUCTION

1.1 OVERVIEW OF NETWORK SECURITY

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information and programs within their to the authority.

Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions. It does as its title explains: It secures the network, as well as protecting and overseeing operations being done. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Network security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name i.e. the password, this is sometimes termed one-factor authentication. For Homes & Small Business, basic firewall or a unified threat management system. For Windows users, basic Antivirus software. An anti-spyware program would also be a good idea. There are many other types of antivirus or anti-spyware programs available. When using a wireless connection, use a robust password. Also one could try to use the strongest security supported by their wireless devices, such as WPA2 with AES. TKIP may be more widely supported by their devices and should only be considered in cases where they are not compliant with AES.If using Wireless: Change the default SSID network name, also disable SSID Broadcast; as this function is unnecessary for home use. (Security experts consider this to be easily bypassed with modern technology and some knowledge of how wireless traffic is detected by software). Enable MAC Address filtering to keep track of all home network MAC devices connecting to one's router. (This is not a security feature per se; However it can be usedto limit and strictly monitor one's DHCP address pool for unwanted intruders if not just by exclusion, but by AP association.)Assign Static IP addresses to network devices. However it may be used, in conjunction with other features, to make one's AP less desirable to would-be intruders.)Disable ICMP ping on router. Review router or firewall logs to help identify abnormal network connections or traffic to the Internet. Use passwords for all accounts. For Windows users, Have multiple accounts per family member and use non-administrative accounts for dayto-day activities.

Raise awareness about information security to children. For Medium businesses, a fairly strong firewall or Unified Threat Management System .Strong Antivirus software and Internet Security Software. For authentication, use strong passwords and change them on a bi-weekly/monthly basis. When using a wireless connection, use a robust password. Raise awareness about physical security to employees. Use an optional network analyzer or network monitor. An enlightened administrator or manager. Use a VPN, or Virtual Private

Network, to communicate between a main office and satellite offices using the Internet as a connectivity medium. A VPN offers a solution to the expense of leasing a data line while providing a secure network for the offices to communicate. A VPN provides the business with a way to communicate between two in a way mimics a private leased line. Although the Internet is used, it is private because the link is encrypted and convenient to use. A medium sized business needing a secure way to connect several offices will find this a good choice. Clear employee guidelines should be implemented for using the Internet, including access to non-work related websites, sending and receiving information. Individual accounts to log on and access company intranet and Internet with monitoring for accountability. Have a back-up policy to recover data in the event of a hardware failure or a security breach that changes, damages or deletes data. Disable Messenger. Assign several employees to monitor a group like cert which studies Internet security vulnerabilities and develops training to help improve security. For Large businesses, A strong firewall and proxy, or network Guard, to keep unwanted people out. A strong antivirus software package and Internet Security Software package. For authentication use strong passwords and change it on a weekly/bi-weekly basis. When using a wireless connection, use a robust password. Exercise physical security precautions to employees. Prepare a network analyzer or network monitor and use it when needed. Implement physical security management like closed circuit television for entry areas and restricted zones. Security to mark the company's perimeter. Fire extinguishers for fire-sensitive areas like server rooms and security rooms.

II. SYSTEM ANALYSIS

EXIXTING SYSTEM

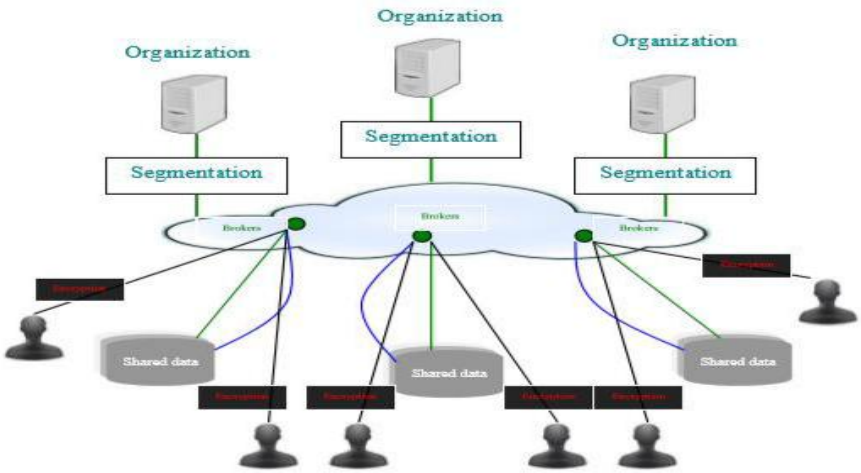
Databases of different organizations are connected through a set of brokers, and metadata are pushed to the local brokers, which further advertise the metadata to other brokers Queries are sent to the local broker and routed according to the metadata until reaching the right data server.

First, at present, site distribution and load balancing in PPIB are conducted in an ad-hoc manner. Our next step of research is to design an automatic scheme that does dynamic site distribution. Several factors can be considered in the scheme such as the workload at each peer, trust level of each peer, and privacy conflicts between automaton segments. Designing a scheme that can strike a balance among these factors is a challenge. Second, we would like to quantify the level of privacy protection achieved by PPIB. Finally, we plan to minimize the participation of the administrator node, who decides such issues as automaton segmentation granularity.

PROPOSED SYSTEM

A main goal is to make PPIB self-reconfigurable. Finally server sends the particular data for the Meta-data by adopting the re-encryption technique, thus the data send from the server will be double Encrypted. This is the way a large number of information sources in different organizations are loosely federated to provide a unified on-demand data access. In the current paper, we present two efficient protocols, one of which also supports the private update of a generalization-based anonymous database. Security proofs and experimental results for both protocols have also been proposed. So far no experimental results had been reported concerning such type of protocols and this results show that both protocols perform very efficiently.

III. SYSTEM ARCHITECTURE

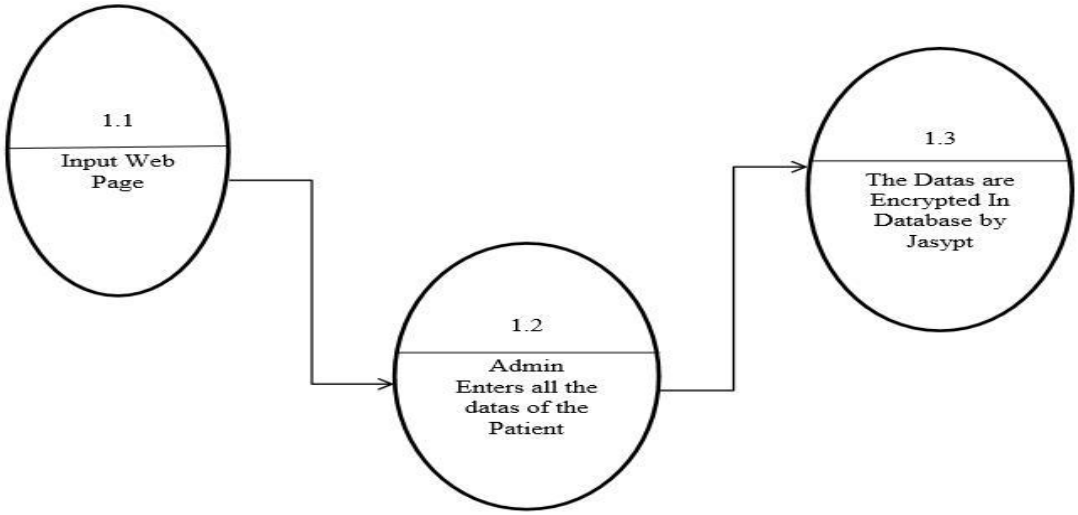


3.1. MODULE DESCRIPTION

3.1.1 Administrator
3.1.2 Information Request and Response
3.1.3 Proxy Re-Encryption
3.1.4 Load Balancing

3.1.1 ADMINISTRATOR

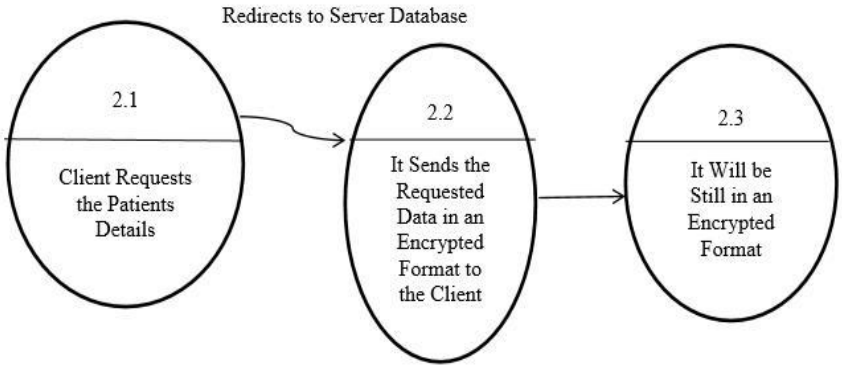
Admin can collect the information of Demographics, Emergency contact, Allergy table, Labs and test table, Lab result, Insurance, Health report this information can be collected in centralized server that is health care administration server then it can be loaded in the encrypted format. It means the data can be encrypting using the jasypt. Jasypt is a java library which allows the developer to add basic encryption capabilities to projects. High-security, standards-based encryption techniques, both for unidirectional and bidirectional encryption. Encrypt passwords, texts, numbers, binaries etc…, the information can loaded and saved in the main centralized server of health care admin in encrypted format using jasypt.



ADMINISTRATOR

3.1.2 INFORMATION REQUEST AND RESPONSE

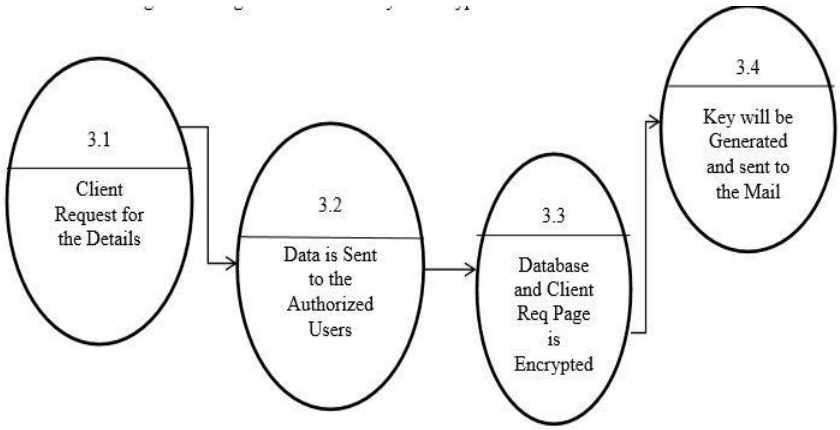
This module requests arises from Patient, Doctors, Insurance Company, National Center for Disease Control (NCDC), friends and family to the centralized server that means healthcare admin. Health admin was receive the request then match the information to it then send the requested information to the requester with encrypted format using jayspt. The receiver can receive the encrypted information then decrypt the information using jayspt algorithm. So this process makes security to that information stored in the health care administration.



INFORMATION REQUEST AND RESPONSE

3.1.3 PROXY RE-ENCRYPTION PROXY-RE-ENCRYPTION

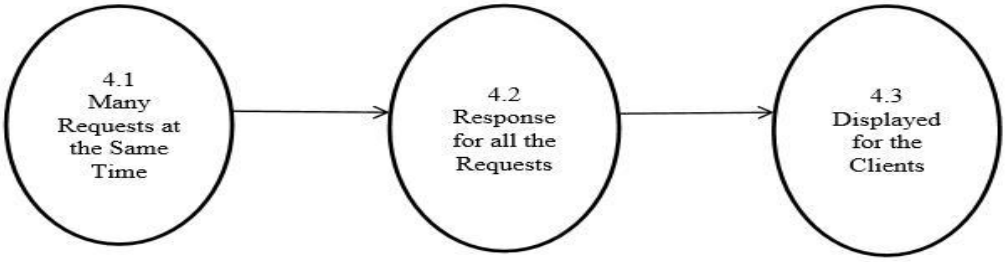
It is used to encrypt the message from the user due to the travelling the encrypted message was re-encrypted then the message was decrypt at the receiver side. It was due the travelling the message was automatically re-encrypt the information.



PROXY RE-ENCRYPTION

3.1.4 LOAD BALANCING DISTRIBUTING

Processing and communications activity evenly across a computer network so that no single device is overwhelmed. Load balancing is especially important for networks where it's difficult to predict the number of requests that will be issued to a server. A load balancer is a core networking solution responsible for distributing incoming traffic among servers hosting the same application content. By balancing application requests across multiple servers, a load balancer prevents any application server from becoming a single point of failure, thus improving overall application availability and responsiveness. For example, when one application server becomes unavailable, the load balancer simply directs all new application requests to other available servers in the pool. Load balancers also improve server utilization and maximize availability. Load balancing is the most straightforward method of scaling out an application server infrastructure. As application demand increases, new servers can be easily added to the resource pool and the load balancer will immediately begin sending traffic to the new server.



LOAD BALANCING

IV. 4CONCLUSION AND FUTURE ENHANCEMENT

4.1 CONCLUSION

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.

4.2 FUTURE ENHANCEMENT

In Future this technique can be used for the transmission of more number of data by eliminating the maximum number of brokers and also by analyzing advanced techniques for encryption and transmitting the data more securely.

REFERENCES

[1]. Alexandra Boldyreva, Mihir Bellare, Adam O'Neill, (2007)"Deterministic And Efficiently Searchable Encryption", in Proc.Crypto.
[2]. Fengjun Li Bo Luo Peng Liu Dongwon Lee Prasenjit Mitra Wang-Chien Lee Chao-Hsien Chu. (2006)"In-Broker Access Control: Towards Efficient End-To-End Performance Of Information Brokerage Systems", in Proc. IeeeSutc.
[3]. 3. L. M.Haas, E. T. Lin, andM.A. Roth, (2002) "Data Integration Through Database Federation" IBM Syst.
[4]. N. Koudas, M. Rabinovich, D. Srivastava, and T. Yu,(2004)" Routing Xml Queries" in Proc. ICDE.
[5]. H. Y. S. Lu, (2004)"Commutative Cipher Based En-Route Filtering In Wireless Sensor Networks", in Proc. VTC.
[6]. Ming Li, Shucheng Yu, Ning Cao and Wenjing Lou, (2011) "Authorized Private Keyword Search Over Encrypted Data In Cloud Computing", in Proc. ICDCS.
[7]. Ming Li, ShuchengYuy, Ning Cao and Wenjing Lou, (2011) "Authorized Private Keyword Search Over Encrypted Personal Health Records In Cloud Computing", in Proc. ICDCS.
[8]. Praveen R. Rao, Member, IEEE Computer Society, and Bongki Moon, (2009) "Locating Xml Documents In A Peer-To-Peer Network Using Distributed Hash Tables", IEEE Trans. Knowl. Data Eng.