Healthcare Information Protection through Cloud Brokerage

Kafe Ul Alam
Human Computer Interaction
Umea University Sweden
kaul0011@student.umu.se

AL AMIN HOSSAIN
Department of Computer
Engineering
Kyung Hee University, Global
Campus,
SOUTH KOREA
johnhuh@khu.ac.kr

Dipak Surie
Senior Research Engineer,
Department of Computing
Science
Umea University Sweden
dipak@cs.umu.se

Abstract

Healthcare system has been improved to combine with computer technology. Cloud Computing reduce treatment delay and the data error. The demand for medical data sharing is increasing due to treatment duplication between healthcare organizations which increases the cost of medication. However, the concern about the protection of medical information is also significant. Medical information is more private than other information because involuntary disclosure can affect in personal life. Cloud brokerage has attained great attention for solving these problems. This paper aims to provide a security model in the cloud computing that facilitates the exchange of medical records between a large variety of providers such as hospitals, laboratories and healthcare institute It allows doctors to obtain a complete patient medical records which can help to avoid duplication, reduce the medical error and healthcare cost as well. In addition our solution is crackdown against the privacy violence.

Keywords: Cloud Computing, Broker, Healthcare system, Privacy and Security.

1 Introduction

Now a days cloud computing has enormous effect on health care service. Basically, in the Cloud Computing model customers plug into the cloud to access IT resources which are priced and provided on-demand. Essentially, IT resources are rented and shared among multiple tenants much as office space, apartments, or storage spaces are used by tenants. This paradigm moved the location of this infrastructure to the network to diminish the costs related with the management of the hardware and software resources [1].

Currently, Cloud brokerage technologies are best considered in the context of supply, demand and delivery. Cloud broker is a type of cloud service provider that plays an intermediary role in cloud computing. Cloud broker help us to detect the best and most cost-effective cloud services from cloud provider according to our needs. In fact, Cloud brokerage has enormous effect while we need to access data frequently. Cloud brokers may provide dynamic access to different cloud providers based on cost and performance data, and they could use different cloud providers at different times, based on what best serves their clients.

Medical data is the most significant issue in cloud computing, thus data security is the top most priority in all the data operation of cloud. Exchanging data between healthcare provider turn out to be an important field for many reason, it decrease the waste of medical resources, medical inaccuracy as well as reduce the cost of treatment. Practically healthcare systems are deployed using various programing language, diverse system platform and different databases. Therefore, it leads to the difficulties of systems assimilation which is one of the core challenges in sharing medical record between medical healthcare suppliers. The Privacy Broker proposed by Bhattacharya and Gupta [3] provided automated support for enforcing privacy policies related to purpose, limited retention, safety and compliance. However, this Privacy Broker is based on a modification of P3P [4]. Cloud brokerage improved the quality and availability of data and increases the ability to link the data, but it is raising the concern about the new demand for information privacy.

This project aims to develop a new cloud broker approach to facilitate the exchange medical information without concerning about the privacy threat. The broker will be able to response any healthcare organization requests according to the user search criteria (e.g., services or patient's information).Our main goal is to provide a Service broker that can enable the exchange of information between healthcare providers that permits doctors to retrieve complete patient medical records before treatment, and offer a service brokerage system that can ensure to avoid duplication of diagnostic data, and endeavors to reduce privacy violation threat and enforce privacy strategy in health care information system.

2 Related Works

The data security and user privacy in health care system has not been discussed widely. Whenever sensitive information needs to exchanged, it must be transmitted through secure channel. *Hussain et. al* [2] proposed context-based adaptations to guide the interaction between end users. Privacy specification language such as Privacy Preference Project (P3P) provides the syntax and semantics of privacy policies, but it does not support implementation of the stated privacy policies. Sometimes, it's difficult to enforce organization policies even if an organization uses P3P to specify its own privacy policies.

Bhattacharya et. al. [8] proposed Enterprise Privacy Authorization (*EPAL*), a formal language to provide privacy middleware architecture based on privacy broker. It has better performance than P3P. However, *EPAL* needs to modify in order to fulfill the capability transfer requirement of the capability certificates.

To reduce treatment delay and data error *Bin et. al.* [6] proposed Cloud resource broker technology that applied goal based resource allocation within the cloud environment. Still they failed to determining similarity between entity class from goal based request and also best available resources. Privacy protection within database applied to the statistical database. But, it doesn't support any mechanism to establish negotiation with multiple users.

3 Main Approaches and Methodology

The proposed privacy broker for preserving operation aims to enable the following aspects of privacy without modifying the database. (a) The broker has to accept the agreed privacy requirement and certify faithfulness of the indicated privacy strategies, (b) it needs to enable individuals to permit precise individuals to access their data and (c) it ought to be able to enforce non-repudiation of agreements between visitors and web-sites. The Figure-1 depicted overall works flow of the project. From the figure we can see that the diagnostic center, hospital and clinic are associated with cloud broker. In this system first doctor certify with Capability certificate that allows authorized person to access privacy constrained data. Figure-1 has shown that every user has a broker identity device, and through this device user can ensure about the exact broker from where she is getting the healthcare data by matching with metadata, and alongside cloud broker can also informed about the exact consumer information. Since cloud broker has query log so it can store all information into the query log. Therefore, it is very easy to determine that who and when and under which condition data has been accessed. Following this procedure data security as well as user privacy can be improved tremendously. After examining the patients' medical fault, diagnostic data transformed according to our previous work [5] and upload to the cloud server along with patient's personal information. If doctor has authorization to access those data then connect with the cloud broker to get the healthcare information for the patient.

4 Conclusion

Our privacy broker medical healthcare system can be effective in terms of privacy threat, data availability of medical history, current medication and most recent treatment as well. It has several advantages, such financial
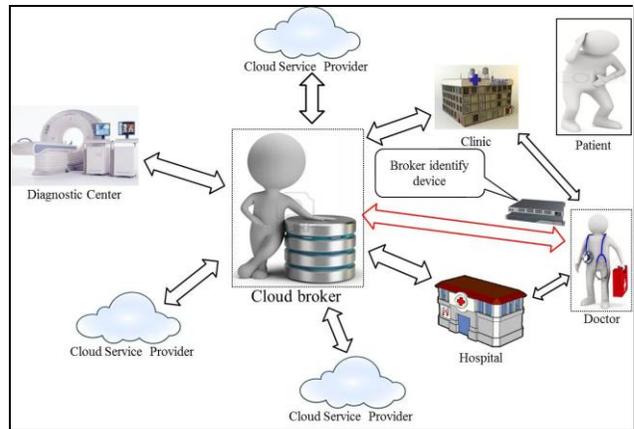

Figure -1: System Architecture

benefit because, it doesn't have data redundancy. It has also effective for healthcare through precise medical care, and social benefit by using capability certificate.

5 References

[1] Brian Hayes. Cloud computing Communications of the *ACM*, (7):9–11, July 2008.

[2] Hussain, Syed Sajid. "Integrating end-user support and negotiations to specify requirements for context-based adaptations in a collaboration environment." *Proceedings of the 2nd ACM SIGCHI symposium on Engineering interactive computing systems*. ACM, 2010..

[3] Bhattacharya J. and Gupta S.K "Privacy Broker for Enforcing Privacy Policies in Databases": *In. Proceedings of Fifth international conference on knowledge based computer systems. Hyderabad, India*, 2004.

[4] The World Wide Web Consortium. The Platform for Privacy Preference (P3P}. Available from http://www.w3.org/P3P/P3FAQ.html (accessed on 27 October, 2012).

[5] Al-Amin Hossain, Hyeong-il Kim, Jae-Woo Chang "A Spatial Transformation Scheme Based on Shear Transformation in Database Outsourcing": *The* 2012 *FTRA World Convergence Conference (FTRA WCC* 2012*) to be held in Jeju, South Korea,* 22-25 *November,* 2012.

[6] Nordin, Mohamad Izuddin Bin, and Mahamat Issa Hassan. "Cloud resource broker in the optimization of medical image retrieval system: A proposed goal-based request in medical application." *National Postgraduate Conference* (NPC), 2011. IEEE, 2011.

[7] Bhattacharya, Jaijit, S. K. Gupta, and Bhurvi Agrawal. "Protecting privacy of health information through privacy broker." *System Sciences*, 2006. *HICSS'06. Proceedings of the 39th Annual Hawaii International Conference on*. Vol. 5. IEEE, 2006.