Healthcare Data Supervision and Secrecy in Cloud Computing

알 아민 후세인, 모하메드 마타하리 이슬람, 모하메드 아잠, 이승진, 허의남
경희대학교 컴퓨터공학과
e-mail : {alamin, motahar, aazam, seungjin, johnhuh} @khu.ac.kr

Healthcare Data Supervision and Secrecy in Cloud Computing

Al Amin Hossain, Md. Motaharul Islam, Mohammad Aazam, Seung-Jin Lee and Eui-Nam Huh
Dept. of Computer Engineering, Kyung Hee University

Abstract

Medical data sharing is increasing due to treatment duplication which increases the cost of medication. Medical healthcare system has been improved to combine with cloud computing. It reduces treatment delay and the medical data error. However, the concern about the privacy protection of medical information is also significant. Medical information is more sensitive than other information because involuntary disclosure can affect in both personal and social life. Privacy cloud brokerage has conquered great attention for solving these problems. Our method provides a security model in the cloud computing environment that facilitates the exchange of medical records between assigned custodians. 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 method offers a trustworthy solution against the privacy violence.

1. Introduction

Information is an important ingredient in good health care. The digital revolution has enabled new ways to gather and accumulate health information to ensure it is available to health professionals when they require it. Actually patient demands are very simple, they want to achieve the ability to record medical history as well as current medical data, including health events, test results, vital status, medications, ideally also supplemented by doctors, medical facilities, and the ability to communicate this data to health care providers. However, paper-based documents are clumsy for several reasons, it's difficult to make available in different places at a time and sometimes duplication is very common problem, and that make information more expensive. Information technology allows health professionals to retrieve information about a patient, and to monitor the patient's progress.

Medical data is very much sensitive, and it unexpectedly needs in anytime anywhere. Therefore, 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 difficult of systems assimilation which is one of the core challenges in sharing medical record between medical healthcare suppliers. Nowadays web services in cloud environment are distributed technologies that successfully solve integration problems between heterogeneous systems [1]. Clearly, Cloud Computing is important to streamline healthcare whether it is for maintaining health records, monitoring of patients, collaboration with peers, even analysis of data, etc. In fact, more than half of all health care organizations have already moved some of their computing activities into the cloud computing. What's more, the health care cloud computing market is expected to grow from $1.7 billion in 2011 to $5.4 billion by 2017 and is expected to be an attractive alternative for organizations seeking to qualify for incentive funds. Cloud computing improved the quality and availability of data and increases the ability to link the data.

However, most significantly computerized data collection, storage and dissemination can give augmentation to significant privacy concerns. The delivery of health care can also raise complex questions about how to reconcile privacy and confidentiality with the need to share information for the benefit of the patient, or for the benefit of the wider society. Therefore, it is raising the concern about the new demand for information privacy. It has become common over the past decade to portray privacy as being under threat. Most significantly, authorized access of medical data is noticeably important. It may generate massive problem even though very small portion of privacy violation of medical data. Privacy is an important and indispensable value in modern society, but it is not an absolute right. It has to be weighed and reconciled with other values, including values that have to do with the public awareness. In different areas of human activity, different weighting may be appropriate. Health information may be in a quite different category from others. Therefore, privacy is notoriously difficult to define, so it is little wonder that there are many competing definitions of, and ways of thinking about, this elusive concept. Privacy in the health system raises a lot of difficult issues. A majority of people express concern about privacy, and a desire to keep their personal information private. There are much higher levels of concern about with internet security and medical confidentiality. We aim to develop new healthcare information privacy approach to facilitate the exchange medical information without concerning about the privacy

threat. The proposed model will be able to response any healthcare organization requests according to the user search criteria. Our contribution can be summarized as follows:

- A service brokering system that can enable the exchange of information between healthcare providers that permits custodian (e.g., doctors) to retrieve complete patient medical records before treatment.
- A service broker that can ensure to avoid duplication of diagnostic data.
- Privacy broker who endeavors to reduce privacy violation threat and enforce privacy strategy in health care information system, and Data privacy monitoring system to ensure that data is not leaking to third party.

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* [5] 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. [7] 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.

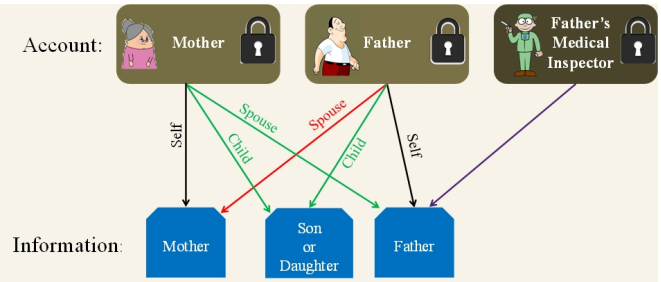
To reduce treatment delay and data error *Bin et. al*. [6] proposed Cloud resource broker technology that applied goal based resource allocation within the cloud environment. Still they failed to determining similarity between entity class from goal based request and also best available resources. Privacy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

The two major initiatives, Google Health and Microsoft *Healthvault* received a lot of attention, most of it focusing on technology, security and privacy issues. Even though the progress on both Google Health and Microsoft *Healthvault* services are disturbingly slow.

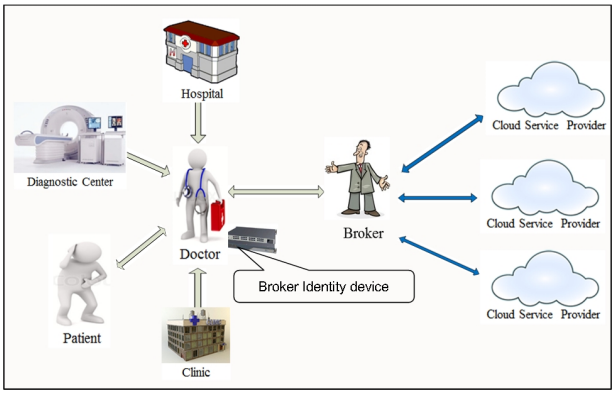
Google Health had several cruxes. There was no facility to upload documents directly. Although, it had a text box where user can paste some information, but that was not the right way to handle a multi-page surgery report. In Google Health test results forces put a uniform value / units / date structure, which was completely inappropriate for more complex medical data e.g. EKG, Ultrasound, MRI, etc. There had no facility whatsoever for ongoing monitoring of vital stats like blood pressure, blood glucose, etc. The test results section was way too rudimentary; this area needs better data entry, charts, averages etc. An MRI scan is likely more important than a two-year old lab test, and your Cardiologist, Dermatologist or Urologist will likely want to see different sets of data. Due to these drawbacks Google Health is not having the broad impact that they hoped it would. Therefore, Google Health has been decided to discontinued [3], and most importantly Google Health (retired January 1, 2012; data was available for download through January 1, 2013). However, Microsoft(R) HealthVault(TM) is still alive. It's a vault only to store user data, and facilitate working with other service providers. In fact, permit authentications are the key features in HealthVault. HealthVault entirely depends on using partner's services. It doesn't have faithful clue about the needs of real patients, for example a blood sugar monitoring service that does not ask whether your values are fasting or after a meal, and a blood pressure monitoring site that does not record whether it's early morning, daytime or evening.

3. Proposed Model

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 [9] 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. In this system every user has to create an account under proposed system, and it identified by a set of credentials. A record contains medical information about an individual. We can see in the figure 1, account and information share a many-to-many relationship. A record may have multiple custodians (e.g., doctor, father).Actually, the person who create a record are designated as a custodian, this is the highest level of security access and gives user full control over the record, including the ability to add and remove health information, view the complete history of changes to the record, share the record with other users and applications and to delete the record. Some of the information stored in the record may be highly sensitive; hence user needs to carefully choose the custodian. When user select a custodian, he must guardian of the records, and then both of users will have complete control over information. Since it is the highest level of access, so guardian can view, modify, and delete everything including, user's role and healthcare information. Therefore, user should grand guardian access to people who is fully trusted (e.g., father, mother, personal doctor).Inappropriate granting of access could allow a grantee to violate user's privacy or even revoke access own records. Through this secure system, users (e.g., patients, doctor medical practitioner etc.) may insert his personal medical data. Even on holiday can put data through smart-



(Figure 1) Information sharing architecture



(Figure 2) Information sharing architecture

Devices such as smart phone, and most importantly his data is more secured. After uploading all medical information, he may ask to his personal medical assistants to see physical condition and provide advices. For example, a patient wishes to know his blood pressure's condition throughout the month. Since doctor can access all that information that patient inserted, so doctor could make a graph [6] by using inserted information and decide what need to do for a particular patient. Doctor might be more efficient. Most significantly, since his partner can access patient's information, therefore it will be very much effective while emergence condition arise.

Watermarking method has been used for the JPEG files (e.g., X-ray report). A watermarking method [2] proposed for cloud computing, to mitigate the risks of insider disclosures. Basically, [2] preliminary implementations are accomplished by exploiting the MapReduce mechanism in the cloudlet they built. Our project aims to develop a graphical library (e.g., watermarking functions) that inserts (encrypted) contents on JPEG files which depend on a selectable key (watermarking key). Our proposed watermark performs as follows:

- *Obscure*: Only authorized person (e.g., doctor) can be able to read the watermark x-ray picture that has watermarking key, even after various disclosures unauthorized person cannot retrieve the images.
- *Robust*: watermark must be difficult to remove from the picture without knowing the watermarking key.

It has several operations such as each disclosure, another watermark is added, which must not affect the other inserted watermarks. Watermarks are easily extractable knowing the watermarking key, in order to reconstruct the disclosure chain. Since it can be extractable, it can also be replaced by a new one if the protocol asks for it.

4. Conclusion

Data availability is one of the core issues in healthcare system. Cloud computing reduced the burden for this issue. However, privacy is one of the most significant issues in cloud computing. All of private data send to the third party cloud service provider. Therefore, if a small portion of medical data changes then it may lead to the massive danger. Our proposed privacy brokerage medical healthcare system is very much effective in terms of privacy threat, data availability for previous and current medical data. It reduces the data redundancy. Patients might be confident about the information security for broker identity device and encrypted data that upload to the server, thus this proposed cloud broker can ensure precise medical care.

Acknowledge

This research was supported by the **MKE**(The Ministry of Knowledge Economy), Korea, under the **ITRC**(Information Technology Research Center) support program supervised by the **NIPA**(National IT Industry Promotion Agency)" (NIPA-2013-(H0301-13-2001)

References

[1] J.K. Zhang and W. Xu, "Web Service-based Healthcare Information System (WSHIS): A Case Study for System Interoperability Concern in Healthcare Field". International Conference on Biomedical and Pharmaceutical Engineering ICBPE 2006, vol, no, pp.588-594, 11-14 Dec. 2006.

[2] Yu, Zhiwei, Clark Thomborson, Chaokun Wang, Jianmin Wang, and Rui Li. "A cloud-based watermarking method for health data security." In High Performance Computing and Simulation (HPCS), 2012 International Conference on, pp. 642-647. IEEE, 2012.

[3] http://googleblog.blogspot.kr/2011/06/update-on-google-health-and-google.html accessed March 19, 2013.

[4] https://ehealth.heartandstroke.ca/heartstroke/bpap.net/?pgSrc=bp_hsfhomepage , accessed March 19, 2013.

[5] 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.

[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.

[8] Al-Amin Hossain, Hyeong-il Kim, Jae-Woo Chang "A Spatial Transformation Scheme Based on Shear Transformation in Database Outsourcing": In. Proceedings of the 2012 FTRA FTRA WCC 2012 Jeju, South Korea, 22-25 November, 2012.