CONF-IRM 2019 Proceedings

International Conference on Information Resources Management (CONF-IRM)

5-2019

PRIVACY-AWARE CLOUD-BASED ARCHITECTURE FOR SHARING HEALTHCARE INFORMATION

Fadi Alhaddadin
Auckland University of Technology, fadi.alhaddadin@aut.ac.nz

PRIVACY-AWARE CLOUD-BASED ARCHITECTURE FOR SHARING HEALTHCARE INFORMATION

Fadi Alhaddadin
Auckland University of Technology
Fadi.alhaddadin@aut.ac.nz

Abstract

Cloud computing appears to be the dreamed vision of the healthcare industry; it matches the need of healthcare information sharing directly to various healthcare-related parties over the internet, regardless of their location and the amount of data being shared. There have been various attempts and efforts found in the literature to adopt the technology of cloud computing in the healthcare domain, however, challenges related to information privacy and security remain unresolved. This paper presents the key design elements of a cloud-based architecture that enables sharing healthcare information amongst disparate parties in a privacy-preserving manner.

Keywords:

Cloud Computing, Data sharing, Information management, Information privacy, Access Control Management

1. Introduction

The healthcare industry has generated large amounts of information, driven by record keeping, compliance and regulatory requirements, and (of course) patient care. Information about patients' health generates special value when it is exchanged and collaboratively used among different parties involved in the healthcare area (Kitamura, et al., 2016). Several researchers and interviewed individuals consider immediate access to previously generated medical records during healthcare service delivery as highly important (Fabiana, Ermakovab, & Junghannsa, 2015). Healthcare information systems in healthcare organisations such as hospitals are required to collaborate with each other by exchanging information among medical staff and practitioners for medical care betterment purposes (Gaboury, Bujold, Boon, & Moher, 2009).

In the healthcare domain, patients usually acquire medical care from a wide range of caregivers based on their proximity, quality of care received, cultural attitudes and bedside manner. Medical care may be received from various caregivers such as hospitals, pharmacy, laboratory, physician group, nurses, school clinics, and public health places (Thompson & Brailer, 2004). This has led to fragmentation of patients' information in heterogeneous systems. The majority of this collected information is stored in heterogeneous distributed health information systems which are mainly proprietary (Kokkinaki, Chouvarda, & Maglaveras, 2006), and as a consequence, health-related information stored in these systems cannot be easily accessed to present a clear and complete picture of an individual patient when needed.

Several attempts have been made by researchers to allow the exchange of medical information among medical practitioners / data analysts in a privacy preserving manner. In healthcare, the availability of information regardless the location of patient and the clinician is a key driver towards patients' satisfaction and healthcare service betterment. For that, there is a stressing need for having a decentralized design of architecture for healthcare information systems that allows for asynchronous interactions among parties involved in the healthcare domain with respect to privacy regulation (Casola, Castiglione, Choo, & Esposito, 2016).

Cloud computing appears to be the dreamed vision of healthcare industry; it matches the need of healthcare information sharing directly to various healthcare-related parties over the internet, regardless their location and the amount of data being shared (Guo, Kuo, & Sahama, 2012). It is a computing paradigm in which resources of the computing infrastructure are provided as a service over the internet (Yu, Wang, Ren, & Lou, 2010). However, the protection of information privacy is a major challenge that hinders the adoption of cloud computing in the domain (Yüksel, Küpçü, & Özkasap, 2017). Information privacy protection is very essential to build users' trust in order to reach the full potential of cloud computing in the healthcare domain. For that, an important characteristic in healthcare cloud-based information systems is the ability to assure patients that their data is protected in the cloud, and their private information will only be disclosed to responsible parties.

This research aims to propose a cloud-based architecture design for managing and sharing healthcare information in privacy-preserving manner. The intention is to design an architecture that meets the main privacy requirements for sharing healthcare information amongst disparate parties. These requirements include (1) storing patients' information on the cloud with assurance that cloud provider cannot read it, (2) providing access to medical practitioners to the needed information in every incident of medical treatment and preserves the privacy of the other irrelevant information, (3) allowing the use of patients' information for research purposes without breaching the privacy of individual patients.

2. Fundamentals of the proposed architecture design

There are number of fundamental requirements that enable the proposed system architecture to meet the requirements for sharing information about patients in a privacy-preserving manner. Structuring patients' information and encrypting it using hierarchical encryption approach are corner stones in the proposed system architecture.

2.1. Structuring Patient Information

The main goal of structuring patients' information is twofold; firstly to limit the exposure of information in cases when it is not needed. Secondly, structuring patients' information can lead to efficient searching mechanisms which is explained further in the paper.

Patients' information in the proposed system design is stored as collection of files contained in 3 different combinations referred to as documents. The 3 documents -when combined- comprise the entire record of a patient. From users' point of view, information about a patient is categorised according into number of categories. Each category comprise number of documents. Information categories are: Information required for every patients visit (All_V), Information required for emergency visits (Em_V), and information required in out-patient clinical visits (OutP_V). Users have access to patients information according to their roles in the healthcare sector, for example, a nurse in emergency department may only access Em_V category, while a doctor in out-patient clinic is allowed to access OutP_V category.

Figure (1) illustrates how patient information is structured into documents, as well as how these documents comprise information categories for users to access.

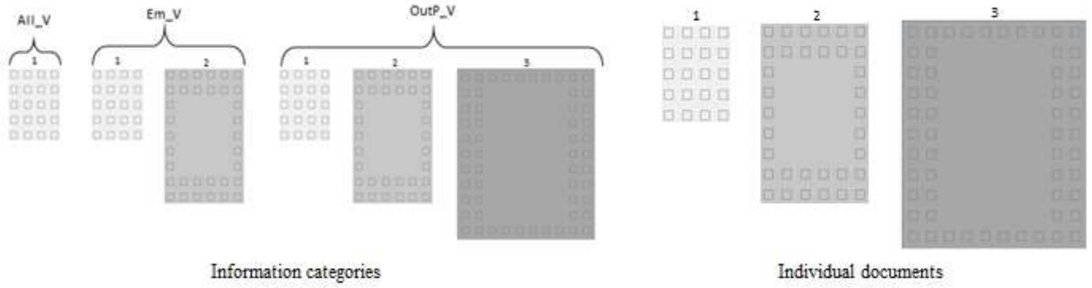


Fig 1: Information structure and categories for patient record

2.2. Hierarchical encryption scheme

The proposed system employs a hierarchical encryption approach called Symmetric Key for Patient controlled Encryption (Symmetric Key PCE) proposed in (Benaloh, Chase, Horvitz, & Lauter, 2009). In Symmetric Key PCE approach, patients' information is partitioned into a hierarchical structure. For every patient, there is a Root Secret Key (S_{kR}) from which number of Sub-secret keys are derived. The Sub-secret keys refer to the secret keys for decrypting documents that belong to the patient. Trapdoors are generated to selectively decrypt documents.

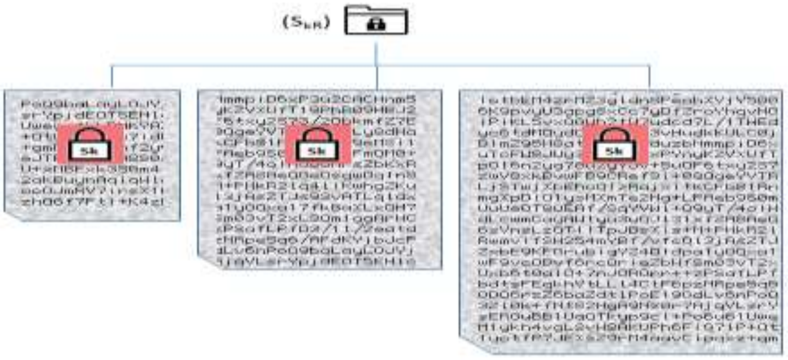


Fig 2: Hierarchical encryption of patient's information

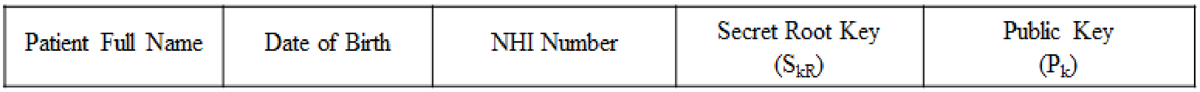
The main goal of employing the Symmetric Key PCE approach is to store patients' health information on the cloud in a searchable manner and only authorized parties can access it upon their requests. The idea of the employed encryption approach is that each patients' information is encrypted using a secret root key. This secret root key is used to generate a secret key for every document included in the patient's information. Each document can only be decrypted using its corresponding secret key. Figure (2) illustrates how patients' information are hierarchically structured and how secret keys are distributed in the employed encryption approach.

3. Components of the proposed architecture

3.1. Requesting agent

The requesting agent is a server that is responsible for receiving requests from users and forwarding them to both Cloud Provider and Secret Key Agent after users are authenticated. The requesting agent is the point of contact that users send requests to in order to store or access information stored on the cloud. Users are authenticated and their access rights are identified before requests are forwarded to both cloud provider and secret key agent. The Requesting Agent has one-way communication channel with the users, one-way communication channel with both cloud provider and secret key agent, and two-way communication channel with the cloud service registry for users' authentication.

The requesting agent stores the information required for identifying patients whose information is stored on the cloud presented in Figure (3). Information stored on the requesting agent is also useful for facilitating access to patients' information that is stored on the cloud. It receives requests from users, and forwards them to both; cloud provider and secret key agent.



Patient Full Name	Date of Birth	NHI Number	Secret Root Key (S_{kR})	Public Key (P_k)

Fig 3: Information permanently stored on the Requesting Agent

3.2. Standard user application

The proposed system architecture requires having a standard application that is installed and run locally on users' machines. Accessing patients' information stored on the cloud can only happen through this application. This application plays an important role in the system in terms of encrypting and decrypting the data stored on the cloud. The main functions of the application include encrypting information and sending it to the cloud, as well as decrypting information when it is received from the cloud provider. Moreover, as part of the application functions, it assures that the information downloaded from the cloud for research purposes are prepared to be read in privacy-preserving manner so that individual patients cannot be identified by reading information related to their health. More information about the functionality of the application is provided further in the instantiation of the proposed system architecture design.

3.3. Cloud service registry

The cloud registry provisions access to information according to users' privileges (SLAs). Services in the context of the proposed architecture include providing access to the information categories. The access is granted for documents that form these categories. The cloud service registry stores the names of categories and their comprising documents' tags. A list of registered users and corresponding SLAs is stored on the cloud registry.

3.4. Secret key agent

The Secret Key Server is a server that stores the required information for decrypting information stored on the cloud. All secret keys are stored together with encrypted indexes and trapdoors for all documents related to one patient (under S_{kR}). The main functions of the secret key server is to receive a request from the requesting agent, and send the required decryption information directly to users. Secret key server has one-way communication with the requesting server which is to receive requests, and one-way communication with user.

3.5. Cloud service provider

The cloud service provider serves by storing and releasing encrypted information related to patients upon users' requests. The cloud service provider has one-way communication channel with the requesting agent, and one-way communication channel with users. It receives requests from authenticated users through the requesting agent and releases the required information in encrypted manner to users.

4. Target Architectural Design

Having outlined and discussed the fundamentals and components of the proposed architectural system design, figure (4) illustrates the relationships of the architectural components involved in the design. The requesting agent plays the role gate person for both cloud provider and secret key agent. It is the only way through which communication with both cloud provider and secret key agent can happen. Moreover, storing encrypted information on a location (cloud) and their corresponding decryption keys on different location (secret key agent) protects the information stored. If cloud server is compromised, information stored on it is meaningless to any disparate party, and similarly, if secret key agent is compromised, keys are of no use without their corresponding information. No communication between the secret key agent and the cloud provider at any stage, they both receive requests from requesting agent through one-way communication channel and send information to users through one-way communication channel.

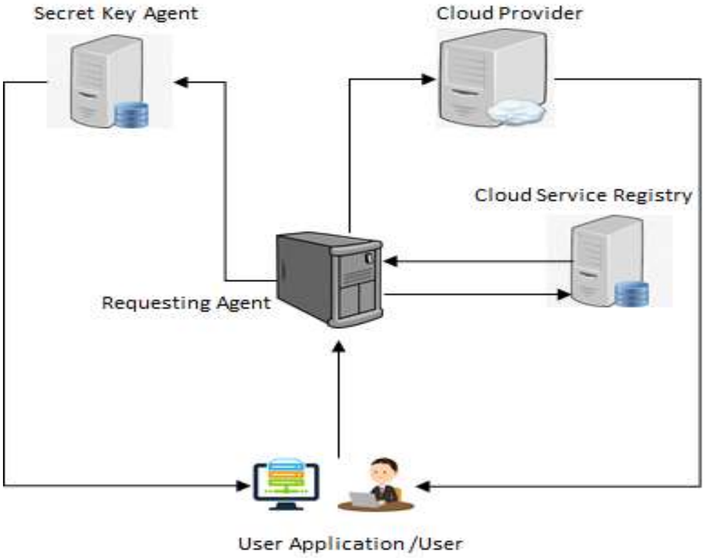


Fig 4: Target Architecture Design

To briefly explain the protocol of the target system, Bob is an example of a patient who is seen by a nurse (Julia) in an emergency department of a hospital. Julia requests Bob’s information by sending a request to the requesting agent using her application. The requesting agent authenticates Julia by sending her information to the cloud service registry. Julia is then authenticated and information about documents she can access is given to the requesting agent. In this example, Julia is allowed to access 2 documents namely doc-1 and doc-2. Julia’s request then is forwarded to both cloud provider and the secret key agent. The cloud provider searches for Bob’s information using his public key and sends information to Julia directly, and secret key agent searches for secret keys for doc-1 and doc-2 using the secret root key associated to Bob and sends them to Julia directly. Julia’s application is responsible of decrypting the information received from the cloud provider using the secret keys, indexes and trapdoors received from the secret key agent.

Conclusion

Sharing patients’ information and using it collaboratively in the healthcare domain generates significant advantages towards improving the medical treatments provided to patients and enables for research purposes. Cloud computing offers the essentials characteristics to meet the need of sharing and using shared patients records in the healthcare field. However, the privacy of information has been a barrier to the adoption of the technology for the healthcare domain. This paper presented a design of cloud-based architecture that enables sharing healthcare information in privacy-preserving manner. Fundamentals of the proposed design were presented, the roles of components comprising the system design were explained. The implementing the proposed system design will grants significant benefits in the healthcare domain.

References

Benaloh, J., Chase, M., Horvitz, E., & Lauter, K. (2009). Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records. *Microsoft Research, Redmond, WA, USA.*

Casola, V., Castiglione, A., Choo, K.-K. R., & Esposito, C. (2016). Healthcare-Related Data in the Cloud: Challenges and Opportunities. *IEEE Cloud Computing*.

Fabiana, B., Ermakovab, T., & Junghannsa, P. (2015, March). Collaborative and secure sharing of healthcare data in multi-clouds. *Information Systems, 48*, 132-150. doi:10.1016/j.is.2014.05.004

Gaboury, I., Bujold, M., Boon, H., & Moher, D. (2009). Interprofessional collaboration within Canadian integrative healthcare clinics: Key components. *Social Science & Medicine, 69*(5), 707–715. doi:10.1016/j.socscimed.2009.05.048

Guo, Y., Kuo, M.-H., & Sahama, T. (2012). Cloud computing for healthcare research information sharing. *IEEE 4th International Conference on Cloud Computing Technology and Science (CloudCom).* IEEE.

Kitamura, T., Kiyohara, K., Matsuyama, T., Hatakeyama, T., Shimamoto, T., Izawa, J., . . . Iwami, T. (2016, March 5). Is Survival After Out-of-Hospital Cardiac Arrests Worse During Days of National Academic Meetings in Japan? A Population-Based Study. *Journal of Epidemiology , 26*(3), 155-162. doi:10.2188/jea.JE20150100

Kokkinaki, A., Chouvarda, I., & Maglaveras, N. (2006). Integrating SCP-ECG files and patient records: an ontology based approach. Greece: University of Thessaloniki.

Thompson, T. G., & Brailer, D. J. (2004). The Decade of Health Information Technology: Delivering Consumer-centric and Information-rich Health Care: Framework for Strategic Action . *Department of Health & Human Services* .

Yu, S., Wang, C., Ren, K., & Lou, W. (2010). Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. *INFOCOM, 2010 Proceedings IEEE.* IEEE.

Yüksel, B., Küpçü, A., & Özkasap, Ö. (2017). Research issues for privacy and security of electronic health services. *Future Generation Computer Systems*, 1-17.