Privacy Protection and Security in eHealth Cloud Platform for Medical Image Sharing

Johanne Vincent, Wei Pan, Gouenou Coatrieux

Privacy Protection and Security in eHealth Cloud Platform for Medical Image Sharing

Johann VINCENT
Institut Mines-Télécom
Télécom Bretagne
CNRS Lab-STICC - UMR 6285
Technopôle Brest-Iroise
CS 83818, 29238 Brest Cedex 3 France
Email: johann.vincent@telecom-bretagne.eu

Gouenou COATRIEUX
Institut Mines-Télécom
Télécom Bretagne
LaTIM - INSERM U1101
Technopôle Brest-Iroise
CS 83818, 29238 Brest Cedex 3 France
Email: gouenou.coatrieux@telecom-bretagne.eu

***Abstract*—**

***Keywords*—Security, Privacy, Cloud Computing, eHealth, Watermarking, Encryption**

I. Introduction

The increased use of new technologies in healthcare practices has greatly modified the traditional ways of dealing with patient information. Nowadays, practitioners want to have access to the relevant patient information on any device at any given time. In particular, the deployment of medical imaging management and exchange with cloud platforms offers an appealing solution to access, share, view and store images. However, medical data and applications are subject to a number of legal and ethical regulations that dictate data security. In addition to that, patients are more and more aware of their privacy and the value that some data may hold for external parties.

The literature often consider three types of eHealth cloud models : private, public or hybrid. Private clouds are the most deployed as data and applications remain under the control of a well defined entity and its users. The public clouds on the other hand, offer all the advantages of cloud computing in terms of service and computing power but at the expanse of reduced native security and privacy protection mechanisms. The eHealth clouds also deal with two different types of health records : Personal Health Records (PHR) and Electronic Health Records (EHR). The formers are directly managed by the user, she can upload her own health record and share them with the practitioner of her choice. Example of this kind of PHR cloud provider include Microsoft Healthvault. EHR on the contrary are managed by Healthcare Providers (HCP) and share the user's records only to trusted HCP third parties.

In this paper, we propose to address the issue of the privacy of medical images in a public cloud platform. Our approach is based on previous work done by Pan et. al [1], where the authors proposed a secure cloud platform. In fact, we specifically address the problem of linkability of image records to a single user from an honest but curious (HBC) public cloud provider. The rest of the paper is organized as follow, the first section define the common public ehealth cloud entities and the linkability issue that is addressed. The second section presents the state of the art of security and privacy techniques for this type of cloud. Our approach to solve the privacy issue is given in section three and some implementation guidelines are proposed. Finally, the paper is concluded and some future works are presented.

II. Linkability of medical records

A. Definitions

In [2], Pfitzmann and Hansen give the following definition for linkability: "Linkability of two or more items of interest (IOIs, e.g., subjects, messages, actions, ...) from an attacker's perspective means that within the system (comprising these and possibly other items), the attacker can sufficiently distinguish whether these IOIs are related or not".

B. Application to the medical records

In a typical public eHealth cloud scenario, an healthcare provider that we denote Producer Hospital (PH) would acquire some medical images of patients. It then would send them to the cloud provider (CP) to make them available for other healthcare provider. A Consumer Hospital (CH) would then request relevant images from the CP to perform an extended diagnostic. Such a scenario can be summed-up through two scenarios we consider thereafter :

- *Outsourcing medical images*: where an image is sent to CP. Entities involved correspond to: one physician, PH and CP.
- *Consultation of the medical images*: where one user of CH request to PH the images of a given patient and retrieve them at CP.

A security analysis of such sharing architecture based on security risk assessment can be found in [1]. In this paper we only recall the common security threats that are being considered. Namely, **T1-** Illegitimate access, **T2-** Operation error, **T3-** Unauthorized modification, **T4-** Loss, **T5-** Unavailability of process/services, **T6-** Information without guarantee of origin and **T7-** Denial of actions. For example, a possible **T1** threat could be a hacker intrusion into the server of the PH.

In addition to these security threats we claim that there can be some privacy threats as well. In fact, in many healthcare cloud solutions the CP may learn some information about the patient that may lead to privacy breach. Here the Honest but Curious model is applied to the CP. If we recall the two scenarios, the CP is responsible of the indexes of images and can easily log the uploads made by a particular HP as well as the accesses by the CH. By doing so, the CP is allowed to track a patient and even possibly identify him if we consider the CP malicious. More formally the above attacks can be described in terms of linkability where the CP is the attacker.

- *Outsourcing medical images*: linkability of two or more images from the CP perspective, means that within the system, the CP can sufficiently distinguish whether these images are related to the same patient.
- *Consultation of the medical images*: linkability of two or more image requests from the CP perspective, means that within the system, the CP can sufficiently distinguish whether these requests are related to the same patient.

In this paper, a new solution as to provide unlinkability for these two cases is proposed in section IV and some related works are presented in section III.

III. Related Works

Numerous approaches have been proposed to secure and enforce privacy protection of patients in eHealth clouds. In [3], Abbas and Khan propose a taxonomy of these approaches which they classify in two mains categories : cryptographic approaches and non-cryptographic approaches. In the former, most of the solutions are based on well known encryption schemes such as Public Key Encryption (PKE) and Symmetric Key Encryption (SKE). However, there are also several other cryptographic primitives that are also used to preserve the security and privacy. They includes : searchable encryption [4], (Hierarchical) identity based encryption (HIBE) [5], proxy re-encryption (PRE), Predicate Encryption (HPE) [6] and (Fully) Homomorphic Encryption (FHE) [7]. This taxonomy is represented on figure 1 and the reader is invited to check the aforementioned article for a full review of security and privacy approaches. However, among the literature, only a portion of approaches are trying to solve the linkability issue that we consider.

In [8], Zhang an Liu present a reference model for preserving privacy in public eHealth cloud. Their proposal rely on group signatures to ensure the unlinkability of a medical record to a given practitioner. They also propose that the patient record indexes should not leak any information on the patient and should allow efficient search. However the authors do not give any practical solution as to achieve this last goal and while group signature protect the anonymity of a signer it does not prevent an honest but curious CP to log the accesses.
Percarina et al. [9] present the SAPPHIRE solution to protect the user privacy. They heavily rely on public key cryptography and on a semi-trusted cloud. In their solution however, the medical record is a PHR under the responsibility of the patient which is not the case for the issue at hand.

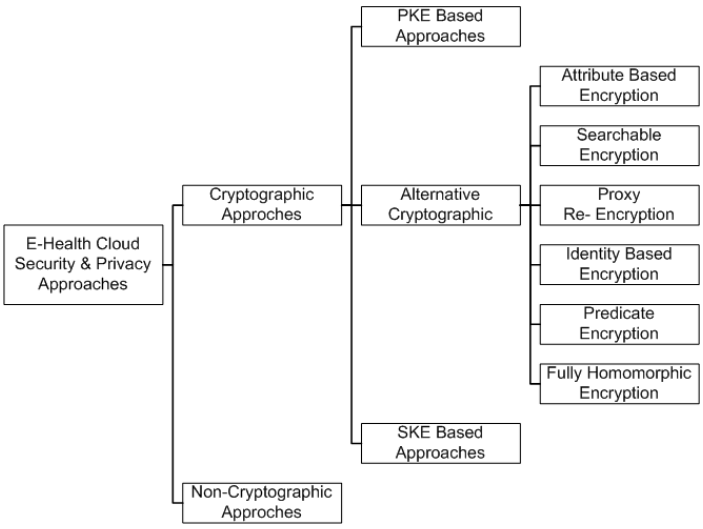

Fig. 1. Taxonomy of security and privacy approaches in eHealth clouds (from [3])

In [10], Lin et al. propose a cloud assisted mobile solution that rely on advanced cryptographic primitives such as Identity Based Encryption to protect the identity of the client, Homomorphic encryption of records, and moreover proxy re-encryption to protect the privacy of all parties. The solution is mainly built for multi dimensional range query which does not really fit our simple $index, image$ database scheme. Moreover, timing attacks can still occur.

In [11], Haas et al. propose a solution for that last requirement. In their public cloud solution, a component called data pseudonimity service is responsible for the anonymization of record before they are sent to a public CP. This service consist in a policy enforcement point and a local cache that allows the randomization of the order in which records are sent to the CP. This solution provides unlinkability of images when they are sent to the CP.

However, to our knowledge, there is no solution for when medical records are accessed by the CH to enforce unlinkability. In the next section, our proposal for that later issue is given.

IV. Proposed approach

As exposed, the problem that our solution is trying to solve is the linkability of medical image records to a specific patient by an honest but curious public cloud. In this section, the following hypothesis are taken regarding the security aspect of such cloud platform. We assume that the **T1** to **T7** security threats are taken into consideration by mean of specific access control policies, encryption and watermarking techniques (such as the one mentioned in [1]).

As showed in section III, our architecture can not let the CP chose the indexes of the EHR. The first addition

that is proposed is then a trusted third party that will be in charge of that tasks. This third party can also acts as the Policy Enforcement Point (PEP), serve as a Policy Definition Point (PDP) and act as Certification Authority as mentioned by [1]. Finally, the use of that element masks the origin of the record to the CP. In fact, every records come from that third party regardless of the HP and practitionner that have made the acquisition. In order to address the problem of linkable records due to the time of upload we use the same cache mechanism as proposed by [11]. This cache relies on a randomization point that creates a random index as well as a random caching time that will decide when the image is uploaded.

The previous mechanism, however, does not enforce the unlinkability of records when the consumer hospital accesses the file. To do so, our architecture relies on Oblivious Transfer (OT). Especially, 1-out-of-N and k-out-of-N oblivious transfer are interesting for the problem at hand.

•

V. Conclusion

The conclusion goes here.

Acknowledgment

The authors would like to thank...

References

[1] Wei Pan, Gouenou Coatrieux, Dalel Bouslimi, and Nicolas Prigent. Secure public cloud platform for medical images sharing. *Studies in health technology and informatics*, 210:251–255, 2014.

[2] Andreas Pfitzmann and Marit Hansen. A terminology for talking about privacy by data minimization: Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management, 2010.

[3] Asad Abbas and Samee U Khan. A review on the state-of-the-art privacy-preserving approaches in the e-health clouds. *Biomedical and Health Informatics, IEEE Journal of*, 18(4):1431–1441, 2014.

[4] Dan Boneh, Giovanni Di Crescenzo, Rafail Ostrovsky, and Giuseppe Persiano. Public key encryption with keyword search. In *Advances in Cryptology-Eurocrypt 2004*, pages 506–522. Springer, 2004.

[5] Dan Boneh and Matt Franklin. Identity-based encryption from the weil pairing. In *Advances in Cryptology-CRYPTO 2001*, pages 213–229. Springer, 2001.

[6] Jonathan Katz, Amit Sahai, and Brent Waters. Predicate encryption supporting disjunctions, polynomial equations, and inner products. In *Advances in Cryptology–EUROCRYPT 2008*, pages 146–162. Springer, 2008.

[7] Craig Gentry et al. Fully homomorphic encryption using ideal lattices. In *STOC*, volume 9, pages 169–178, 2009.

[8] Rui Zhang and Ling Liu. Security models and requirements for healthcare application clouds. In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, pages 268–275. IEEE, 2010.

[9] John Pecarina, Shi Pu, and Jyh-Charn Liu. Sapphire: Anonymity for enhanced control and private collaboration in healthcare clouds. In *Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on*, pages 99–106. IEEE, 2012.

[10] Huang Lin, Jun Shao, Chi Zhang, and Yuguang Fang. Cam: cloud-assisted privacy preserving mobile health monitoring. *Information Forensics and Security, IEEE Transactions on*, 8(6):985–997, 2013.

[11] Sebastian Haas, Sven Wohlgemuth, Isao Echizen, Noboru Sonehara, and Günter Müller. Aspects of privacy for electronic health records. *International journal of medical informatics*, 80(2):e26–e31, 2011.

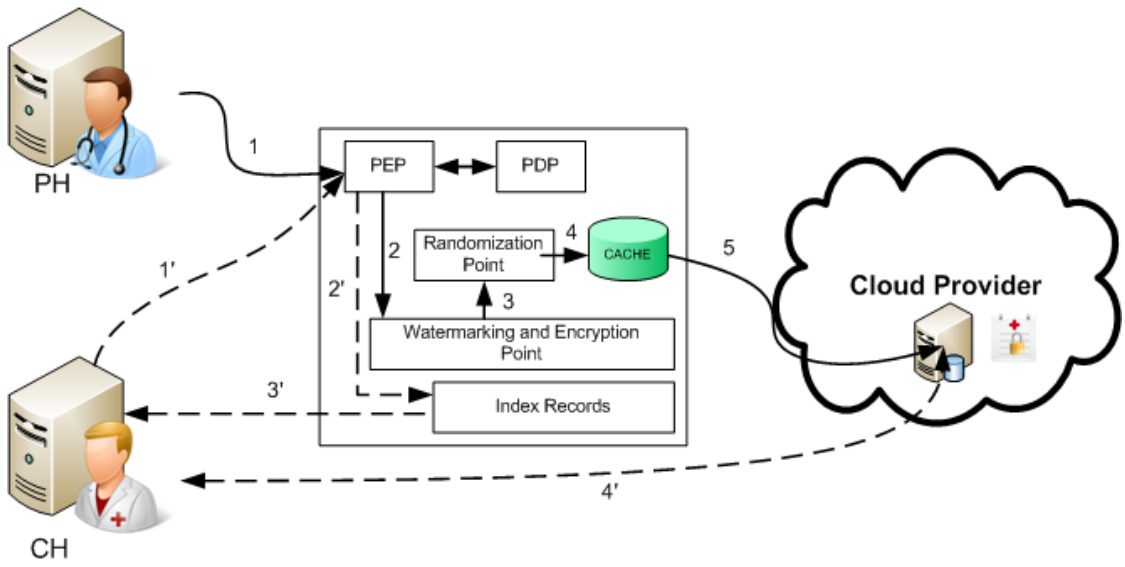

Fig. 2. Proposal for a privacy enhanced public cloud platform