Digital Healthcare Empowering Europeans
R. Cornet et al. (Eds.)

doi:10.3233/978-1-61499-512-8-251

Secure Public Cloud Platform for Medical Images Sharing

Wei PAN[a], Gouenou COATRIEUX[a,1], Dalel BOUSLIMI[a] and Nicolas PRIGENT[b]

[a] *Institut Mines-Télécom, Télécom Bretagne, LaTIM - INSERM U1101, Technopôle Brest-Iroise, CS 83818, 29238 Brest Cedex 3 France*
[b] *Supélec, Avenue de la Boulaie, CS 47601, Cesson Sévigné Cedex, France*

Abstract. Cloud computing promises medical imaging services offering large storage and computing capabilities for limited costs. In this data outsourcing framework, one of the greatest issues to deal with is data security. To do so, we propose to secure a public cloud platform devoted to medical image sharing by defining and deploying a security policy so as to control various security mechanisms. This policy stands on a risk assessment we conducted so as to identify security objectives with a special interest for digital content protection. These objectives are addressed by means of different security mechanisms like access and usage control policy, partial-encryption and watermarking.

Keywords. Security, Cloud Computing, Risk analysis, Watermarking, Encryption

Introduction

In healthcare, the deployment of medical image management and exchange with cloud computing provides an efficient solution to access, view, share, and store images online. However, moving to the cloud medical applications (e.g. medical image software and storage) is submitted to strict legal and deontological regulations that dictate data security in terms of availability, confidentiality, integrity and traceability. In healthcare, among the different cloud deployment model (private, public or hybrid), the former is the most developed. Indeed, it offers cloud services while remaining under the control of its users.[1-2] At the opposite is the public cloud model which gives access to all cloud advantages in terms of shared resources and services but it is more vulnerable as it is maintained and controlled by providers the user may not be confident with [3-4]. The main challenge in this latter case is then how to establish the trust between cloud provider and data owner.

In this paper, we propose to secure a public cloud platform devoted to medical image sharing while focusing more particularly on the protection of digital content. Our approach relies on the definition and deployment of a security policy that identifies the entities involved in the transactions, the data and services to be protected and the actions one must conduct so as to protect data before outsourcing them. The policy is derived from a risk assessment which allows identifying security objectives to ensure.

[1] Corresponding Author, e-mail: gouenou.coatrieux@telecom-bretagne.eu.
This work was supported by the Labex CominLabs POSEIDON project.

These objectives are next addressed by various security mechanisms. Among these security tools, we use partial encryption and watermarking so as to achieve a higher degree of security while ensuring image confidentiality, integrity and traceability. Such mechanisms are controlled by a security policy by means of rules that dictate what a user has to do in terms of data protection before communicating them.

The remainder of this paper is organized as follows. In Section 1, we present the basic public cloud platform for medical image sharing. We also describe the methodology we follow so as to secure digital contents exchanged in this platform in Section 2. In Section 3, we present one possible implementation of our platform.

1. Description of the proposed public cloud platform use case

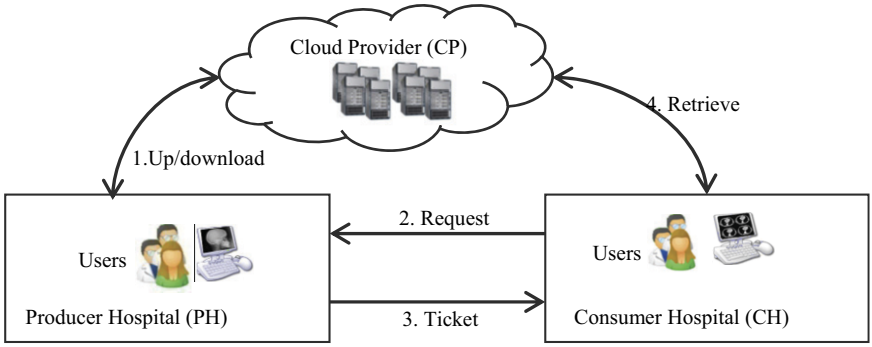

Figure 1. Public cloud platform for medical image sharing.

As shown in Figure 1, the platform allows sharing medical images between three entities: a Producer Hospital (PH), a Consumer Hospital (CH) and the Cloud Provider (CP). PH is the hospital where an image is acquired and interpreted for the first time before being outsourced to CP. Herein, CP is a public cloud that provides storage capabilities and enables image exchange between CH and PH. Such a scenario can be summed-up through two scenarios we consider thereafter:

- *Outsourcing medical images*: where an image and its medical report are sent to CP (*step 1 in Fig.1*). Entities involved correspond to: one physician, PH and CP. Notice that it is CP which assigns an identifier to the image and not PH.
- *Consultation of the medical images*: where one user of CH requests to PH the images of a given patient *(step 2 in Fig.1)*. The request response is a ticket with the image links CH should send to CP so as to access data *(step 3, 4 in Fig.1)*.

2. Securing digital contents in the proposed platform

Our proposal is built on a three stage process starting by a security risk assessment for security objective identification followed by the definition of security rules that security mechanisms will have to respect. Due to space limitation, we only provide a short view of each of these stages essentially focusing on digital content protection.

2.1. Risk evaluation and security objectives for digital content

Based on the above use case, we identify four assets to be protected: Medical Images (MI), Hospital Information System (HIS), Cloud Information System (CIS) and Interconnection Network (IN). Depending on the system architecture and data workflow, each asset has security needs which can be expressed in terms of Availability, Integrity, Confidentiality and Traceability (AICT). Herein, a need is measured on three levels: Low (L), Medium (M) and High (H). Table 1 provides AICT levels we defined for the previous assets considering the framework given in Figure 1 and the potential platform risks. All needs of "High" level should be considered.

Table 1. Level of needs in terms of AICT.

	A	I	C	T
MI	H	H	H	H
HIS	H	M	H	M
CIS	H	M	H	M
IN	H	M	H	M

In this paper, we focus on the protection of Medical Images. As seen in Table 1, we fixed its AICT levels as "High". Indeed, MI should be available for all relevant uses at any time (e.g. emergency), it should be traced so as to detect improper usage or communication, its integrity should be preserved so as to avoid medical errors and its confidentiality should be ensured. The next risk analysis step consists in evaluating the threats the system may be concerned by. In this use case, we have identified seven classes of threats for digital content (i.e. MI):

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.

The final determination of security needs and objectives for all assets are revised depending on a threat analysis. Due to the fact MI AICT are already of high level, security objectives to consider have to cover all identified threats. In our platform, we defined five security objectives, *Oi*, *i*=1…5, such as:

- ***T1*** ➔ ***O1***: any access to MI should be controlled,
- ***T2*** & ***T3*** ➔ ***O2***: integrity of MI should be guaranteed,
- ***T4*** & ***T5*** ➔ ***O3***: MI should be available for use,
- ***T6*** & ***T7*** ➔ ***O4***: MI should be able to authenticate and ***O5***: traces of operations should be usable even when they are generated by different systems.

2.2. Security mechanisms and digital content security objectives

In order to respond O2 and O4, we use reversible watermarking so as to insert into an image the proofs of its integrity (i.e., a digital signature of the image) and of its authenticity (i.e., patient, sender and recipient identifiers).[5] O5 is also be satisfied by inserting within the image the identifier of the user who consulted it. The interest of the reversibility property ensures that it is possible to exactly reconstruct the original image by inverting the distortion induced by the watermarking process. It allows also the watermark update without introducing more distortion.

O1 is carried out by: cryptography mechanisms, a Central Authority (CA), an access and usage control policy. In order to provide MI confidentiality and traceability at the same time, we combine symmetric partial encryption with reversible

watermarking. The solution we implemented combines a block cipher algorithm (e.g. AES, the Advanced Encryption Standard) that is applied to the most significant bit planes of the image while proofs of image integrity and authenticity are reversibly embedded in its least significant bit planes. In this way, one can easily trace and verify the integrity and authenticity of the image while it is encrypted or not. Notice that the entity that updates the watermarked message has to digitally sign it so as to ensure non-repudiation. In our framework, a Central Authority (CA) is used as a trusted third party that authenticates certified hospitals, i.e., hospitals that are allowed to communicate and exchange data through the cloud while providing watermarking and encryption key management. In order to conduct access and usage control, organization based access control model (OrBAC) can be used to express the corresponding security policy rules.[6] One of the main OrBAC advantages is that it can specify authorizations and obligations contextually. A "context" can be viewed as a set of conditions to be satisfied before activating a given authorization or obligation. For instance, the update of a watermark in an image by the PH or the CP can be controlled by an access and usage rule R1 with the dynamic context "*WatermarkUpdate*" that should be satisfied, e.g., "*the identifier of the requester should be inserted into the image before granting the image access*". The access and usage authorization request of PH, CH and CP are addressed to a monitor. This latter is centralized with CA.

Finally, O3 is treated by means of a backup service PH and CP systems should provide and maintain.

2.3. Securing other assets and data ticket

Other assets' security needs are covered by various security mechanisms. For example, one use antivirus and firewalls to mitigate HIS and CIS confidentiality threats, Virtual private network (VPN) are appropriate to mitigate IN availability and confidentiality threats. Notice that these mechanisms are also controlled by the security policy in OrBAC and are be used to reinforce MI security objectives. For instance, audit logs enhance the response to O5 (traceability) especially if it is combined with an OrBAC rule R2 like "*PH should log each image request*".

A last point to address is to secure the ticket that allows CH to access the data. To do so, a "blind ticket"[7] is generated such as: $[K_{pr\_PH}(K_{pub\_CP}(ID_i), K_{pub\_CP}(W_{trace})), K_{pr\_PH}(K_{pub\_CH}(K_i))]$ where: K_{pub_CP} and K_{pub_CH} are the public keys of CP and CH, respectively; K_{pr_PH} is the private key of PH; ID_i is identifier of the image i; W_{trace} is the traceability message (i.e., the identifier of the requester) to be inserted by CP into the image (i.e., when updating the watermark); and, K_i is the symmetric encryption key CH needs to decrypt the image. Notice that some metadata are also exchanged so as to provide contextual elements for access authorizations.

3. Implementation of the proposed platform

A prototype of the proposed platform was implemented with java and SQLite for database management. Four servers were developed so as to act as a PH, a CH, a CP and a CA. The block cipher and reversible watermarking algorithms we used are AES and the method proposed by Ni *et al.* in [8]. The choice of the AES stands on the fact it is recommended by the medical image standard DICOM. As stated above, security mechanisms and servers are controlled through access and usage rules we specified by

using OrBAC. Moreover we took advantage of the OrBAC application programming interface (API) and used it as system monitor. It can thus supervise partial-encryption/decryption and watermarking operations on images, controlling if they are conducted at the right time in the data workflow. We especially implemented the two use-case scenarios of Section 1 in their secured form:

1) Once a medical image *i* is acquired in PH, its encryption (O1) and watermarking are obliged before it is outsourced (imposed by R1) via VPN to CP. The watermarked message corresponds to the: image digital signature (O2), patient ID (O4), physician ID (O5). At the reception, CP generates ID_i and sends it back to PH.

2) In the image consultation scenario, one authenticated user in CH requests an image sending all the necessary pieces of information to PH. On its side, PH logs the requests (R2 rule) and checks with CA if CH is part of the hospital group of confidence (O1). If yes, it generates the corresponding blind ticket and sends it to CH. CH then just has to send the blind ticket obviously without K_i to get images. Before sending the image, CP is obliged to update and digitally sign the watermarked image (see O5).

Herein, if an image is disclosed by a CH user, he will not be able to deny (T7) due to the presence of W_{trace} into the image and of the recorded log.

4. Conclusion

In this work, we defined and deployed a security policy so as to control different digital content protection mechanisms and to secure medical images shared through a public cloud platform. Based on a risk assessment and threat analysis, we identify different security objectives that are achieved through the specification of access and usage rules and the use of partial encryption with reversible watermarking. As next step of the proposed methodology, we cannot present due to space limitations, one can re-evaluate the system robustness against security threats, old and new ones, and include new or more adapted security mechanisms. As example, one can use techniques that are able to watermark fully data encrypted. Through such an iterative process, our solution becomes flexible and scalable.

References

[1] C.T. Yang, L.T. Chen, W.L. Chou and K.C. Wang. Implementation of a medical imaging file accessing system on cloud computing. CSE IEEE Conf. on, Dec. 2010, pp. 321-326.

[2] C.G. He, X.M. Fan and Y. Li. Toward ubiquitous healthcare services with a novel efficient cloud platform. IEEE trans. Biomed Eng., Jan 2013, 60(1): 230-234.

[3] C.C. Teng, J. Mitcell, C. Walker, A. Swan. A medical image archive solution in the Cloud. ICSESS IEEE Conf. on, July 2010, pp. 431-434.

[4] L.A. Bastiao Silva, C. Costa and J.L. Oliveira. A PACS gateway to the cloud. 6th Iberian Conference on CISTI, June 2011, pp. 1-6.

[5] W. Pan, G. Coatrieux, N. Cuppens, F. Cuppens, C. Roux. Medical image integrity control combining digital signature and lossless watermarking. Lecture notes in computer science, 2009, vol. 5939, pp. 153-162.

[6] F. Cuppens and N. Cuppens-Boulahia. Modeling contextual security policies. Int. J. Inf. Secur., 2008, 7(4):285-305.

[7] D. Chaum. Blind signatures for untraceable payments. Advances in Cryptology - Crypto '82, Springer-Verlag (1983), 199-203.

[8] Z. Ni, Y. Shi, N. Ansari, and S. Wei. Reversible data hiding. In Proc. IEEE Int. Symp. Circuits and Systems, May 2003, vol. 2, pp. 912–915.