Towards an Information Infrastructure for Medical Image Sharing

Gustavo H. M. B. Motta¹ · Danilo A. B. Araújo¹ · Juracy R. Lucena-Neto¹ · Paulo M. Azevedo-Marques² · Saulo S. Cordeiro² · Severino A. Araújo-Neto³

Published online: 13 June 2019

© Society for Imaging Informatics in Medicine 2019

Abstract

Information infrastructures involve the notion of a shared, open infrastructure, constituting a space where people, organizations, and technical components associate to develop an activity. The current infrastructure for medical image sharing, based on PACS/DICOM technologies, does not constitute an information infrastructure since it is limited in its ability to share in a scalable, comprehensive, and secure manner. This paper proposes the DICOMFlow, a decentralized, distributed infrastructure model that aims to foment the formation of an information infrastructure in order to share medical images and teleradiology. As an installed base, it uses the PACS/DICOM infrastructure of radiology departments and the internet e-mail infrastructure. Experiments performed in real and simulated environments have indicated the feasibility of the proposed infrastructure to foment the formation of an information infrastructure for medical image sharing and teleradiology.

Keywords Digital imaging and communications in medicine (DICOM) · Information infrastructure · Medical image sharing · Picture archive and communication systems (PACS) · Systems architecture · Teleradiology

Introduction

Information infrastructures involve the notion of a shared and open infrastructure, constituting a social space where people, organizations, and technical components may spontaneously form associations in order to develop certain activities [1–3]. The concept of sharing is understood as an infrastructure as a common good [1], which does not belong to one single organization, but that may be used by multiple communities in a variety of manners, and not provided for in its original conception [4]. Open is understood as the capacity to include an increasing number of entities, whether technological components (e.g., software, devices, standards), communities (e.g., users, developers), and organizations (e.g., companies), as well as governance and standardization (e.g., IEEE, W3C,

ISO). Sharing and openness, therefore, result in increasing technical and social heterogeneity [4].

It is emphasized that in information infrastructures, control is generally distributed and episodic, the only manner in which to coordinate their evolution, since they are not modified from the top down [4, 5] because they have no central authority. Thus, they do not result from the execution of a specified a priori project, but rather evolve as they emerge from the continuous interaction between people, organizations, and technical components in a process of continuing design [2, 6]. The Internet is a typical example of an information infrastructure. It was formed through an evolutionary process, which, contrary to the traditional “design from scratch” approach, followed an approach that “cultivated” an installed base (e.g., the web used the installed TCP/IP base) in order to foment its dynamic growth through bootstrapping and adaptive growth [4]. This signifies that an information infrastructure occurs when an infrastructure is bootstrapped from an installed base and continuously supports its growth (adaptation) so as not to be paralyzed due to the inertia of the installed base itself [4, 5].

In the currently installed base for sharing medical imaging exams, widely used by radiology departments, the main technical components are PACS (Picture Archiving and Communications Systems) [7] and the DICOM (Digital Imaging and Communications in Medicine) standard [8]. However, this is not an information infrastructure since it

✉ Gustavo H. M. B. Motta
gustavo@ci.ufpb.br

¹ Center of Informatics, Federal University of Paraíba, João Pessoa, PB 58058-600, Brazil

² Center of Imaging Sciences and Medical Physics, Ribeirão Preto Medical School, University of São Paulo, Ribeirão Preto, SP 14049-900, Brazil

³ Center of Medical Sciences, Federal University of Paraíba, João Pessoa, PB 58051-900, Brazil

has a limited ability to meet the growing demand for sharing such exams amongst the stakeholders in a scalable, comprehensive, and secure manner. Although the PACS/DICOM-installed base does not offer major barriers to sharing when access is made locally to radiology departments, there are nonetheless serious barriers to sharing them on a global scale (teleradiology). For instance, the static point-to-point connectivity upon which DICOM relies, that is simple to manage and configure to connect devices in a same network domain, is not feasible to be used to connect remote devices dynamically over the Internet [9]. In addition, DICOM lacks the ability to instruct a device to relay received data [9]. Hence, the PACS/DICOM-installed base does not establish a common infrastructure for exchanging examinations between organizations and health professionals.

This thereby leads to the establishment of bilateral agreements between the parties, characterized by the adoption of ad hoc integration solutions [10], generally based on point-to-point communication at network level and cloud-based repositories [11]. The point-to-point network solution directly connects parties that wish to share exams via virtual private networks [11]. Because this requires point-to-point configurations, it is not scalable and is therefore unsuitable for providing a common means of exchanging images between multiple parties [12]. On the other hand, solutions based on cloud computing [12–16] depend on central elements, for example, for storage or communication purposes (e.g., the use of brokers). In addition, even considering the benefits of enabling clients to access data and services with minimal infrastructure, cloud computing solutions bring the risk of depending on a single provider, coupled with data security, privacy, and availability issues. Therefore, solutions [17–20] based on IHE integration profiles [21] for image sharing between multiple parties also presuppose authority or central elements, either for coordination, control, or operation.

In short, solutions typically used to share imaging exams do not provide an infrastructure, which is shared, open, without authority, or central elements and is scalable, i.e., capable of establishing a global social space of interaction, characteristic of information infrastructures. This article, therefore, proposes the DICOMFlow, an infrastructure model that aims to foment the formation of an information infrastructure for medical image sharing and teleradiology. The proposed infrastructure does not presuppose central authority or elements, and its control and coordination are distributed. The installed base it uses is the PACS/DICOM infrastructure from radiology departments and the infrastructure of internet e-mail.

The remainder of the paper is organized as follows: The “[Background: Information Infrastructure](#)” section presents an overview of the characteristics of information infrastructures and the main challenges facing their formation, followed by a section providing a summary of related work. “[The DICOMFlow](#)” section presents the proposal of this work,

followed by the section that describes the experimental evaluation of the proposal. The final section discusses and concludes the paper.

Background: Information Infrastructure

Information infrastructures comprise a diversity of sociotechnical entities and digital services, arranged extensively in a network, and are capable of forming a complex system to support a work activity or practice [1]. Their construction is not derived from a traditional top-down development process, which emphasizes initial detailed planning and inflexible designs, with a centralized, rigidly hierarchical control structure [22]. In contrast, they are constructed through a composition of heterogeneous entities that integrate to form a scale-free network in an evolutionary bottom-up process. These entities have their own formation and operational processes and are autonomous in relation to the evolution of the network, i.e., they are free to join or withdraw from the information infrastructure, and to use its resources and services or even to design them [4].

Typically, technical entities include devices, software, and standards, while social entities include users, developers, organizations, and governance bodies. By linking these sociotechnical entities in networks, an interactive space is created, which is capable of supporting the accomplishment of activities and work practices, thereby forming the information infrastructure. Hence, information infrastructures emerge in practice, based on the relations between technological solutions (technical entities) and users, communities and organizations with their policies and cultures (social entities), establishing rules for the use of these solutions [5, 6].

However, the question that arises is how to foment its formation and evolution. Through studying the formation and evolution of infrastructures such as the internet, the web, and the global telephony system [4, 23], it was observed that an infrastructure is always formed on a pre-existing infrastructure, called an installed base [3]. For example, at the beginning of the Internet, the telephony communications infrastructure was used as an installed base to leverage its growth, making it easy to reach locations already connected to the existing communications infrastructure. However, for such growth to be sustainable, it must be able to adapt to the sociotechnical heterogeneity that exists between the installed base and the new infrastructure that is formed, as well as between the new entities that make up the new infrastructure [4]. The great capacity to adapt therefore favors the integration of new entities into the infrastructure, which may not only take advantage of the strengths of the installed base, but also overcome its weaknesses, thereby reinforcing its growth.

It has been observed in the evolution of infrastructures that adopting gateways is a key aspect in achieving a greater

capacity to adapt and integrate [4, 23–25]. Gateways are elements that act as adapters in order to integrate heterogeneous entities to promote the growth of the infrastructure. Gateways can be simple elements such as an AC/DC converter, which integrates direct current equipment into alternating current power supply networks, or more elaborate elements such as the Domain Name System (DNS), which made it possible to integrate a new network, based on names, the World Wide Web (WWW), to an already installed network, the Internet, based on numerical IP addresses [4]. In short, the function of the gateway is to overcome pre-existing incompatibilities in an installed base in order to facilitate the entry of entities to form a new infrastructure on this basis, thus obtaining an economy of scale [25].

Another key aspect is to modularize the information infrastructure with the weak coupling of its components so as to allow them to be altered in an incremental, autonomous, decentralized manner [4, 26]. The idea is to recursively decompose it into separate application, transport and service sub-infrastructure, exploring gateways to connect them [4]. This enables the coordination and distributed control of the infrastructure. For example, on the Internet, this allows the governance of the WWW (the application layer), conducted by the W3C, to occur autonomously in relation to the governance of the transport layer, which is the responsibility of the Internet Engineering Task Force (IETF). In addition, such modularization offers both flexibility, in order to allow local changes to occur without impacting the infrastructure as a whole, and a high composition capacity of its components, which favors adaptation for use by heterogeneous entities [4, 26].

Security in an information infrastructure is an aspect that emerges during its evolution in order to meet adaptation demands from its sociotechnical entities. For instance, the Internet and the WWW were not originally designed having security as a main concern, but during its evolution, a set of security standards and protocols were incorporated to attend adaptation demands to make e-commerce feasible. The public key infrastructure based on X.509 [27] standard for digital certificates was incorporated into the Internet as a reliable base to authenticate subjects and data, enabling secure e-mail and HTTP communication with S/MIME [28] standard and HTTPS/TLS [29] protocol, respectively. It is worth to note that these security standards and protocols establish only a common mechanism to secure communication, but each entity in the Internet is autonomous to make its own security policies. For example, a cloud storage provider has its own access control policies and is responsible to keep stored data safe but needs to use the common security mechanisms of the Internet to communicate with partners and clients.

Therefore, the formation of information infrastructures is associated with a permanent effort involving its sociotechnical components, as part of an innovation process based on

continuous design [2, 6], i.e., it is able to replace or change elements whenever necessary, without radically changing the architecture, and to expand the information infrastructure by adding new entities in modular increments, with the aim of evolving into a common working environment [3]. During this process, the infrastructure continues to operate and never stops to redesign.

Related Work

In this section, the related work is organized into solutions based on cloud computing, IHE integration profiles, peer-to-peer (P2P) networks, and e-mail. The aim is to identify the technologies and standards used and their contributions to the formation of a teleradiological information infrastructure.

Cloud-based solutions for image sharing across PACS/DICOM infrastructures [12–16] typically use a central storage repository and maintain gateways at the edge of the infrastructure, which serve as DICOM message relays via the Internet. Communication adopts a transmission protocol (e.g., HTTP, XMPP [30]) and messages are structured in a standard format (e.g., XML). In addition, the repository, besides storing images, acts as an intermediary in the exchange of messages between infrastructures. Thus, the main advantage of using the cloud is the possibility of accessing data with a minimum change in the original infrastructure [12]. However, the central element for storing information limits the ability of being scalable, because an increase in the volume of trafficked information in the central element decreases the performance of the response time. Finally, because there is no guarantee that providers will not apply mining to customer data, there are legal policies and regulations that prohibit the use of third-party repositories or require privacy preservation guarantees regarding such data. This leads to the development of security mechanisms (e.g., cryptography) to impose centralized access control, which hinders the spontaneous association between two or more infrastructures and the arbitrary growth of the infrastructure as a whole.

The IHE framework, an initiative formed to help ensure interoperability between healthcare organizations, has developed integration profiles to enable electronic medical records and medical imaging to be shared [31]. The purpose of these profiles is to ensure that information needed for medical decisions is both correct and available to health professionals [21], thereby enriching the use of existing standards (e.g., DICOM, HL7, ISO, IETF) and establishing an approach to readapt the flow of PACS for the exchange of data between institutions [15]. The XDS-I profile [32], adopted in interoperability solutions for exchanging medical imaging exams [17–20], regulates the publication, search, and retrieval of imaging exams amongst affinity domains. The profile provides guidelines to establish a centralized discovery mechanism for these images,

composed of actors and transactions between these actors. However, compliance with the recommendations contained within the IHE XDS-I profile represents a technical challenge needing to be considered in the solutions. As presented, the XDS-I profile only establishes guidelines for transactions between entities in the same affinity domain.

On the other hand, P2P solutions [33–35] do not use central control elements, and thereby bring advantages. For example, content and resources may be shared either from the center or from the edge of a P2P network, unlike the client/server network, where content and resources are generally only shared from the center. Furthermore, this type of network is more reliable, since it does not require a central server subject to being a single point of failure or to being a bottleneck in times when network utilization is high. Moreover, the solutions give significant autonomy to the network nodes [33]. However, communication between two points requires synchronism, and it is necessary for both nodes to be active during communication. Also, because there is no open specification in the communication pattern of the solutions, autonomy becomes a limiting factor for the formation of an infrastructure, because as the network grows, groups of nodes may establish particularities, forming isolated networks, requiring different communication configurations to be maintained for each group, and thereby compromising scale and growth.

Finally, [36, 37] seek to benefit from the high connectivity and the asynchronous, decentralized nature of the Internet e-mail infrastructure in order to distribute medical images. The Dicoogle [36] proposes a P2P network and uses e-mail as the central repository of communication messages between nodes, making the P2P network asynchronous. On the other hand, DICOM e-mail [37] is a standardized protocol for exchanging medical imaging exams through a secure connection between two partners that do not need to be known a priori (ad hoc teleradiology connection) [37]. Specified by the IT Working Group (@GIT) from the German Radiological Society (DRG), it uses the specifications of e-mail message transmission protocols (SMTP [38]) and DICOM object attachment in e-mails (Supplement 54: DICOM MIME-Type) to share imaging exams with e-mail attachments, applying PGP/GPG encryption to ensure the security of the trafficked information. Weisser et al. [39] presented different applications of teleradiology with DICOM e-mail, such as for issuing reports and emergency consultations. The asynchronous transmission of imaging exams provided by e-mail enables DICOM e-mail to integrate different service infrastructures in various ways to compose teleradiology applications in the workflow of more than 240 institutions in Germany. As an example, in 2013, Mannheim University Hospital received more than 6000 imaging exams and passed more than 3700 exams to 36 network partners, with a send/receive flow of more than 2,550,000 images [40].

The DICOMFlow

The DICOMFlow is an architectural model that aims to foster the formation of an information infrastructure for sharing imaging exams and teleradiology based on the PACS/DICOM infrastructures of radiology departments and Internet e-mail. In order to build on an installed base, it is essential to obtain information on it so as to take advantage of its strengths and overcome its limitations [5].

The strengths of the PACS/DICOM infrastructure include the widespread use of the DICOM protocol as a communication standard between devices encountered in radiology departments; and it is the basic support for radiology workflow. One limitation related to the PACS/DICOM infrastructure is that it was designed between the mid-1980s and 1990s [7], in a context of local networks, a fact that in practice makes it impossible to transmit images with the DICOM protocol via Internet, both through the presence of firewalls, amongst other security issues, as well as communication overhead.

The idea, therefore, has been to take advantage of the strengths of the PACS/DICOM infrastructure and overcome its limitations. Thus, it is necessary to obtain a solution that acts as a gateway between the PACS/DICOM-installed base and the Internet, capable of safely transporting information in DICOM standard via the Internet using protocols accepted by the access policies contained in firewalls. All this needs to be carried out without significantly altering the local PACS/DICOM structure, while making it possible to transpose the radiology workflow from a local to a global context, i.e., to achieve image sharing and teleradiology.

A key aspect of this solution, which acts as a gateway, is to use the installed base of Internet e-mail, the strong point of which is the high connectivity. In practice, it is able to exchange messages between a wide diversity of professionals and health organizations, without the need to modify their firewalls, thereby enabling the integration of the radiology workflow to a global scale. Furthermore, e-mail is asynchronous and allows the content of messages to be safely transmitted (with confidentiality, integrity, and authenticity), making it possible to implement protection policies on clinical data. The limitation is the compulsory receipt of the raw data from the imaging tests and the difficulty in transporting them as e-mail attachments, as occurs in DICOM e-mail [37]. Due to the large size (> 30 MB), an examination in DICOM e-mail is fragmented into multiple e-mails in order to be transmitted.

To overcome this difficulty, the DICOMFlow was chosen for an asymmetrical approach. E-mail is used to notify the recipient with a message on the availability of an exam in order to perform some action (e.g., issue a report), based on a service request protocol incorporated in the e-mail itself. In addition to the request, the e-mail only includes light data, such as metadata, a summary of relevant clinical information, and information on accessing the exam (URL and access

credentials), i.e., the raw data of the images are not transmitted as e-mail attachments. The receiver retrieves the images (the DICOM object) via the transmission content protocol (e.g., HTTP/REST [41]) specified in the URL and meeting part-by-part security.

Service Protocol

The service request protocol specifies the content of messages transmitted by e-mail notifying the recipient to perform an action involving a management or transport service on a medical imaging exam. Table 1 describes the DICOMFlow services and the main actions.

Service Certificate actions are used to exchange public key certificates to enable confidential and mutual authentication between parties. The storage service notifies the recipient to perform storage actions for one or more image exams available for download from the sender. For example, this service may be used by small clinics to request the long-term archiving of exams at a data storage company.

The Sharing service shares the URLs and the access credentials for one or more exams with the recipient. In a network of hospitals, such sharing will allow patients at one hospital to access imaging exams they performed at another, i.e., in principle, from one hospital, it is possible to access exams from other hospitals in the network and vice versa, without needing to duplicate the raw data (DICOM objects). The Request service notifies the receiver to perform an action on one or more of the exams. For example, notifying a radiologist to write a report or a medical image processing company to perform a specific processing. Once the action has been completed, the recipient returns a message with the result to the sender. In this case, either the written report or the URL to download the exam after processing. Finally, the Discovery service is used so that the sender may know which services the recipient supports. For example, to discover to which modalities and specialties a specific radiologist is interested in issuing reports.

Figure 1 illustrates the e-mail structure with a message requesting the execution of the storage service for an examination. The top part contains the usual information regarding the source, destination, subject, and formatting scheme. Below are the control data used to aid the pre-processing of the message by DICOMFlow clients. After this, comes the message encoded in the XML language with the following structure: (1) the request with service name and respective action, (2) a unique identifier of the message and timestamp, and (3) the URL to download the exam (DICOM object) and credentials that authorize this access to the recipient.

In order to meet safety standards for the transmission of and access to clinical information, XML service messages are encrypted in the S/MIME standard using X.509 digital certificates exchanged via the Certificate service. Before being sent, each message is encrypted with the sender's private key, to ensure authenticity, followed by encryption with the recipient's public key, to ensure confidentiality. Downloading exams, in turn, requires user authentication and credential validation in order to authorize the transfer via HTTPS protocol (HTTP communication on a TLS-encrypted connection [29]).

DICOMFlow Architecture

The proposed protocol enabled the organization of a macroarchitecture (Fig. 2) capable of interconnecting a diversity of entities related to the practice of radiology. The architectural organization complied with the principles of building information infrastructures, with the services protocol integrating heterogeneous infrastructures of entities from different domains for exchanging exams and teleradiology. For this to occur, entities that wish to integrate must have a DICOMFlow adapter on the edge of their infrastructures acting as a gateway, so that pre-existing heterogeneities become compatible. The function of the DICOMFlow adapter is therefore to interpret the messages of the service protocol transmitted via e-mail

Table 1 DICOMFlow services and the main actions. Each message sent contains only one service and one action. For each request action (Request, Put, VerifyServices) there is a result action (Result, Confirm, VerifyResult)

Service	Action	Description
Certificate	Request	Request for digital certificate
	Result	Response containing the digital certificate.
	Confirm	Confirming receipt of the digital certificate.
Storage	Save	Request for storage of the study.
	Result	Result of the storage operation.
Sharing	Put	Signaling that the study is available for sharing.
	Result	Result registering information on sharing metadata.
Request	Put	Request to perform an operation on an study (e.g., written report).
	Result	Result of action (e.g., written report completed and returned to requester).
Discovery	VerifyServices	Requesting lists of available services.
	VerifyResult	Result containing a list of services.

Fig. 1 Storage request message. In addition to the control data and service specification, the URL for the exam is included and the credential for access clearance. The encrypted information is indicated in the figure

(IMAP [42]/SMTP [38]) and actions are executed in the local infrastructure.

A typical example of a DICOMFlow adapter is one located in Imaging Centers or Hospitals with local PACS/DICOM infrastructures. It is responsible for monitoring the local PACS so that, for each new exam, service request messages are sent to

the e-mail boxes of the interested parties based on some locally established policy. Other DICOMFlow adapters, located in the recipient infrastructures, access the e-mail boxes to receive requests for execution. Requests, for example, may be sent to (1) archive exams in an image storage service, (2) archive exams in the PACS of a partner hospital to keep them synchronized, (3) issue a report from a specific radiologist or from a teleradiology service, or (4) process images from a specialized service. In addition, requesting physicians and patients themselves may be notified by the Sharing service of the availability of the exam and its written report. It should also be emphasized that the adopted approach offers the receiver the option to retrieve the exam immediately or at a future moment, thus maintaining the point-to-point connectivity between the infrastructures.

From a modular point of view, the macroarchitecture is weakly coupled, with a separation between service, transport, and application. The proposed protocol specifies the services, and the infrastructures of the e-mail and the web (HTTP) provide the transport/communication, on which applications may be developed. The DICOMFlow adapter acts as a gateway, by connecting them. Because it is situated on the edge of infrastructures, the DICOMFlow adapter reduces the need for local changes, thus facilitating its integration into the installed base, regardless of the existing heterogeneity. On the other hand, by offering basic services, it allows the creation of services and applications from the composition of these simpler services, which favors the capacity of adaptation required in the process of forming information infrastructures. In addition, weak coupling is a necessary feature for the incremental growth of information infrastructures [4].

Fig. 2 Macroarchitecture of the DICOMFlow integrating entities from distinct domains with DICOMFlow adapters located on the edge of heterogeneous infrastructures

It may also be observed that in the macroarchitecture (Fig. 2), there is no need for central elements, either to control or to operate the infrastructure. Each entity is free to join the infrastructure and to offer or consume services and is autonomous in relation to the entities with which it wishes to interact. Hence, the infrastructure is open and may grow in a manner that is not limited in the number of its members thanks to the scalability of the Internet e-mail infrastructure.

Infrastructure members are also free to implement or deploy implementations of DICOMFlow adapters that best meet their needs, as well as client applications. What is important is that such implementations conform to the service protocol. The architectures of the DICOMFlow adapters are called microarchitectures. The following subsection presents a reference microarchitecture (Fig. 3) for a typical DICOMFlow adapter, followed by a subsection describing its implementation.

DICOMFlow Adapter Microarchitecture

The microarchitecture of the DICOMFlow adapter is organized into two main modules: DICOMMessage and DICOMMove. The DICOMMessage deals with the communication and security aspects of sending and receiving messages, while DICOMMove manages the transmission of medical images (DICOM objects) and their safety aspects.

In the internal organization of the DICOMMessage (Fig. 3), the Process Manager component coordinates the flow of

sending and receiving messages and the configuration flow of the services. The ParserXML component standardizes and encrypts information in XML services, and the Sender and Receiver modules send and receive messages via e-mail, respectively. The module provides an API to allow the execution of its functionality using pre-established default settings. It is also possible to execute the API independently, through command line scripts, which allows the module to be used in other microarchitectures, with different programming languages, thereby providing flexibility in the use of the protocol.

In the DICOMMove module (Fig. 3), the Repository component monitors the local PACS infrastructure to request the Registry component to register the metadata of the new exams as they are stored in the PACS. The Repository component is also responsible for retrieving DICOM objects from PACS, in response to an e-mail request to download exams via HTTP/REST [41]. The Registry stores metadata and responds to queries regarding exams. It is up to the Controller component to coordinate the activities of the module, monitoring the arrival of exams in the PACS via the Repository, registering them in the Registry, and the respective signaling to the DICOMMessage to send messages. Considering the possibility of working with multiple PACS in the same domain, DICOMMove is based on XDS-I integration profile guidelines to find and index image studies locally. The module still controls the transmission of the image exams, ensuring the authenticity and authorization of access for clients to download the exams, acting as a web application.

Fig. 3 Reference microarchitecture of the DICOMFlow adapter. The DICOMMessage deals with the safe communication of messages, and the DICOMMove handles the safe transmission of the medical imaging exams (DICOM objects)

Implementation

The DICOMMessage module was developed in the Java programming language and each of its components implements an API, so that a greater capacity of composition is obtained between them. The ParserXML component was based on the implementation of the XML processing Java code generated by the JABX framework from the XML Schema Definitions (XSD) of the DICOMFlow services protocol messages. The protocol XML messages were encrypted with the BouncyCastle library, which implements the security guidelines specified in the S/MIME standard. The JavaMail, a library that supports SMTP and IMAP e-mail protocols, was used to implement the Sender and Receiver components. In this way, the sending of a message may be described as follows: (1) the sender creates a message of multiple contents (MIMEMultipart), (2) includes a content (MIMEBodyPart) with the XML structure of a DICOMFlow service and defines the type of content (Content-Type) as XML (text/XML; charset = UTF-8), (3) optionally includes other content (MIMEBodyPart), containing the digital certificate of the sender and defines the type as an attachment (application/octet-stream), (4) the sender signs the message with the private key associated with the public key present in its digital certificate, (5) encrypts the message with the public key present in the recipient's digital certificate, and (6) defines the message type as encrypted in the message header (application/pkcs7-mime; name = "smime.p7m"; smimtype = enveloped-data).

The DICOMMove module uses Java Internet technology (J2EE) in its construction. The Repository and Registry components employ Hibernate technology to manage a database that stores metadata and to monitor the PACS server(s) database. Interfaces are implemented in the module that make it possible to construct database connectors for several types of PACS servers (e.g., DCM4CHE and CONQUEST). The Repository uses the DICOM communication tools of the DCM4CHE technology to retrieve and store images in DICOM objects on the PACS server. In addition, the Controller, besides managing the other components, transmits the medical images through HTTP/REST WebServices implemented with the Jersey software framework. Security while transferring imaging exams is based on the documentation of Amazon Web Services [43] and occurs as follows: (1) the receiver prepares an HTTPS request with the URL contained in the received message; (2) the verification signature is calculated with HMAC-SHA1 [44] using the access credential, also received in the message; (3) the signature is added to the request, which is sent to the sender of the service message for the purpose of downloading the exam, (4) the sender receives the request and locates the receiver's credential locally; (5) after locating it, the verification signature is calculated with HMAC-SHA1; (6) compares the calculated signature with that received in the

request; and (7) transmission of the compressed images to the receiver is initiated.

The DICOMFlow implementation contemplated a common language for communication, with mechanisms for asynchronous, asymmetric, and point-to-point communication between the various entities of the distributed environment. The implementation employed non-proprietary and widely diffused technologies. Finally, we emphasize that the implemented code is open, maintained in a repository in GitHub, which is freely available to use.

Experimental Evaluation

The aim of the experiments was to evaluate the DICOMFlow architectural model with regard to its technical and operational feasibility in both simulated and real environments.

The simulated environment experiment evaluated DICOMFlow's ability to synchronize the content of PACS infrastructures located in different domains. An environment composed of three interconnected computers was set up at the edge of a metropolitan network with a transmission capacity of 5 Mb/s, 5 km apart and protected by firewalls. The machines represented PACS servers commonly found in clinics and hospitals and the following software package was installed in each: the DCM4CHE DICOM manager and its toolkit (tool set for manipulating the exams maintained by DCM4CHE), the DICOMFlow adapter, the PostgreSQL and MySQL database managers, the Java Virtual Machine, and JBOSS and Tomcat application servers as web platforms for DCM4CHE and DICOMFlow, respectively. The DICOMFlow service protocol messages were exchanged through the Gmail e-mail server. There were no changes to the firewall settings because DICOMFlow uses standard ports typically freed for HTTP and e-mail protocols.

The experiment took place in the following manner. Initially, the toolkit was used to store CT scans with a unit size of 32.4 MB in the DCM4CHE of two servers. The DICOMFlow adapters were then configured for the mutual synchronization of the exams. Afterwards, three rounds of PACS synchronization tests were performed involving 20, 40, and 80 exams. The average synchronization and control overhead times observed at the end of the experiment are shown in Table 2.

Following this, two servers were configured in the same manner as the previous experiment, except that they were changed to perform synchronization on a third server. Then, three new rounds of synchronization tests were run involving 20, 40, and 80 exams. The obtained mean synchronization times on the third server are presented in Table 2.

At a later time, the DICOMFlow was evaluated in two experiments performed in different real environments.

Table 2 Mean synchronization time between servers 1 and 2 and mean synchronization time for server 3 with the others. Overhead not measured for server 3

Synchronization time between servers		Time in minutes		
		Server 1	Server 2	Server 3
20 exams	Sync	15.01	15.06	19.06
	Overhead	1.17	1.13	–
40 exams	Sync	16.85	18.87	28.06
	Overhead	1.25	2.17	–
80 exams	Sync	32.18	29.01	53.06
	Overhead	3.80	2.20	–

The first experiment evaluated the distribution of imaging exams for storage in an external repository. This was performed in an environment consisting of a PACS with a CONQUEST server and an instance of the DICOMFlow adapter, part of the information technology (IT) infrastructure at the Centro de Ciências das Imagens e Física Médica at the Faculdade de Medicina de Ribeirão Preto (CCIFM-FMRP), Universidade de São Paulo (USP), Brazil. The external repository was located in the IT infrastructure of the Superintendência de Tecnologia da Informação at the Universidade Federal de Paraíba (STI-UFPB), Brazil, with an instance of the DICOMFlow adapter and a DCM4CHE server for archiving exams. To perform the experiment, the DICOMFlow adapter of the CCIFM-FMRP was configured to monitor the already existing exams and as they had been received, and to send them to the external repository. On the other hand, the DICOMFlow adapter from the repository was configured to store the exams on the STI-UFPB PACS server. The adapters then remained active for 8 consecutive hours and 426 service messages were exchanged between requests and responses to the requests. Finally, a total of 213 ultrasound imaging exams were transferred and archived, with a total traffic of approximately 2.5 GB.

The second experiment evaluated the distribution of imaging exams issuing reports at a distance. This was performed in an environment which consisted of a PACS with a DCM4CHE server integrated into the IT infrastructure of the Clínica Radiológica de Patos, in Paraíba, Brazil. To complement the experimental environment, a client application was developed to support the issuing of reports [45], kept on the computer of a doctor in a remote location. The application, developed with the Javascript React library, did not require the installation of additional software and had its own implementation of a DICOMFlow adapter, supporting encryption and messaging, digital certificate storage, and the downloading of images. Every implementation followed the DICOMFlow service protocol guidelines. Moreover, the application did not require changes to the firewall settings and was independent

of the operating system involved, requiring at least 1.6GHz of CPU and 4 GB of RAM, to be used.

Thus, to perform the experiment, the clinic's DICOMFlow adapter was configured to monitor both the existing and the newly acquired exams and to send report requests to the client application. On the other hand, the client application was configured to process the messages and retrieve the exams. For 12 h of the experiment, 157 messages were sent to the client requesting reports and 157 computerized radiography (CR) exams were transferred, totaling approximately 3.1 GB of traffic.

Discussion and Conclusion

The experiments enabled us to observe the technical and operational feasibility of the macroarchitecture of DICOMFlow with the construction of adapters for the proposed service protocol. The performance and volume of data trafficked in the experiment in the simulated environment indicated the feasibility of using this implementation in real environments. In turn, the results of the experiments carried out in real environments reinforced this indication. Furthermore, the DICOMFlow adapter may be installed without significantly interfering with the current infrastructure of the participating entities and its operation did not require changes in the existing firewall policies, despite the heterogeneity present in those infrastructures. Nevertheless, it is important to note that to turn DICOMFlow into a product, it required experimenting with exams of greater size, such as computed tomography or digital mammography, in order to improve transference time, making it practical to daily operations. In addition, more work is needed to automate the integration of the workflow of hospitals and imaging centers into DICOMFlow infrastructure.

Compared to other solutions, such as those based on cloud computing [12–16] or in IHE integration profiles standards [17–20], the main factor that distinguishes the DICOMFlow is that its architecture does not presuppose central authority or elements, since its control and coordination are distributed. The presence of central elements hinders the free association of arbitrary entities, generally requiring the satisfaction of policies for federalization. From the operational viewpoint, this limits the large-scale growth of the infrastructure in dealing, for example, with a large number of members with a high technical and social heterogeneity. Furthermore, the DICOMFlow also has advantages over DICOM e-mail [37], which transfers DICOM objects as e-mail attachments, thereby implying the compulsory receipt of large volumes of data, and requiring the use of fragmentation/defragmentation techniques and integrity checks, which overloads the protocol. The model proposed herein overcomes this overload thanks to its asymmetry, which offers the message receiver the option

of deciding the moment to effectively retrieve the imaging exam via download.

It is observed that, at the macroarchitecture level of the DICOMFlow, there are no limits with regard to new entities joining to form an image-sharing network. In order for such entities (typically health professionals and organizations) to join, it is sufficient to become integrated with the installed PACS/DICOM base and Internet e-mail and use DICOMFlow adapters acting as gateways to accommodate heterogeneities. It should also be emphasized that the DICOMFlow gateway acts below the work layer and does not interfere directly with how the work should be performed or how the images exchanged will be used between the parties. On the other hand, at the level of microarchitecture, the entities that make up the infrastructure are free to design, develop, change, or replace their elements whenever necessary. This signifies that there is a stable installed base with high connectivity at the macroarchitectural level to allow the expansion of infrastructure and flexibility with the possibility of making changes at the microarchitectural level thereby allowing it to adapt and evolve.

With this characteristic, the DICOMFlow becomes versatile, with great adaptability in contexts with different working practices. Thus, the high connectivity of the installed base coupled with adaptability has the potential to foment the formation of an information infrastructure for medical image sharing and teleradiology.

References

- Bowker GC, Baker K, Millerand F, Ribes D: Toward information infrastructure studies: Ways of knowing in a networked environment. In: Hunsinger J, Klastrup L, Allen M Eds. *International Handbook of Internet Research*. Dordrecht: Springer, 2010, pp. 97–117
- Monteiro E, Pollock N, Hanseth O, Williams R: From artefacts to infrastructures. *Comput Support Coop Work* 22:575–607, 2013
- Aanestad M, Grisot M, Hanseth O, Vassilakopoulou P: Information infrastructures and the challenge of the Installed Base. In: Aanestad M, Grisot M, Hanseth O, Vassilakopoulou P Eds. *Information infrastructures within European health care: Working with the Installed Base*. Cham: Springer, 2017, pp. 25–33
- Hanseth O, Lyytinen K: Design theory for dynamic complexity in information infrastructures: The case of building internet. *J Inf Technol* 25:1–19, 2010
- Star SL, Ruhleder K: Steps toward an ecology of infrastructure: Design and access for large information spaces. *Inf Syst Res* 7: 111–134, 1996
- Aanestad M, Hanseth O: Implementing open network technologies in complex work practices: A case from telemedicine. *Organizational and Social Perspectives on Information Technology*, Aalborg, Denmark, 2000, 355–369
- Huang HK: *PACS and imaging informatics: Basic principles and applications*, 2nd edition. New Jersey: Wiley-Blackwell, 2010
- National Electrical Manufacturers Association Digital Imaging and Communications in Medicine (DICOM). 2011 Available at: <http://medical.nema.org/standard.html>. Accessed 18 October 2018
- Pianyk OS: *Digital imaging and Communications in Medicine (DICOM): A practical introduction and survival guide*, 2nd edition. Heidelberg: Springer, 2012
- Ribeiro LS, Costa C, Oliveira JL: Current trends in archiving and transmission of medical images. In: Erondy OF Ed. *InTech*, 2011, 89–106
- Chatterjee AR, Stalcup S, Sharma A, Sato TS, Gupta P, Lee YZ, Malone C, McBee M, Hotaling EL, Kansagra AP: Image sharing in radiology—A primer. *Acad Radiol* 24:286–294, 2017
- Silva LAB, Costa C, Oliveira JL: DICOM relay over the cloud. *Int J Comput Assist Radiol Surg* 8:323–333, 2013
- Monteiro EJM, Costa C, Oliveira JL: A cloud architecture for teleradiology-as-a-service. *Methods Inf Med* 55:1–12, 2016
- Yuan Y, Yan L, Wang Y, Hu G, Chen M: Sharing of larger medical DICOM imaging data-sets in cloud computing. *J Med Imaging Heal Informatics* 5:1390–1394, 2015
- Godinho TM, Viana-Ferreira C, Bastiao-Silva LA, Costa C: A routing mechanism for cloud outsourcing of medical imaging repositories. *IEEE J Biomed Heal Informatics* 20:367–375, 2016
- Viana-Ferreira C, Guerra A, Silva JF, Matos S, Costa C: An intelligent cloud storage gateway for medical imaging. *J Med Syst* 41: 141, 2017
- Zhang K, Ling T, Yang Y, et al.: Clinical experiences of collaborative imaging diagnosis in Shanghai district healthcare services. *SPIE Medical Imaging 2016: PACS and Imaging Informatics: Next Generation and Innovations*, 2016, 9789, 97890X
- Langer SG, Tellis W, Carr C, Daly M, Erickson BJ, Mendelson D, Moore S, Perry J, Shastri K, Warnock M, Zhu W: The RSNA image sharing network. *J Digit Imaging* 28:53–61, 2015
- Simalango MF, Kim Y, Seo YT, Choi YH, Cho YK: XDS-I gateway development for HIE connectivity with legacy PACS at Gil Hospital. *Healthc Inform Res* 19:293–300, 2013
- Ribeiro LS, Viana-Ferreira C, Oliveira JL, Costa C: XDS-I outsourcing proxy: Ensuring confidentiality while preserving interoperability. *IEEE J Biomed Heal Informatics* 18:1404–1412, 2014
- Integrating the Healthcare Enterprise (IHE) IT infrastructure technical framework (ITI TF-1), vol. 1, 2017. Available at: http://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_TF_Vol1.pdf. Accessed 18 October 2018
- Paina L, Peters DH: Understanding pathways for scaling up health services through the lens of complex adaptive systems. *Health Policy Plan* 27:365–373, 2012
- Edwards P, Jackson S, Bowker G, Knobel C: Report of a Workshop on History and Theory of Infrastructures: Lessons for New Scientific Infrastructures, Univ. Michigan, School of Information, 2007. Available at <https://www.ics.uci.edu/~gbowker/cyberinfrastructure.pdf>. Accessed 18 October 2018
- Hanseth O: Gateways—Just as important as standards: How the internet won the ‘religious war’ over standards in Scandinavia. *Knowledge, Technol Policy* 14:71–89, 2001
- David PA, Bunn JA: The economics of gateway technologies and network evolution: Lessons from electricity supply history. *Inf Econ Policy* 3:165–202, 1988
- Jensen TB: Design principles for achieving integrated healthcare information systems. *Health Informatics J* 19:29–45, 2013
- Internet X: 509 public key infrastructure certificate and certificate revocation list (CRL) profile, IETF RFC, 2008, 5280
- Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification, IETF RFC 2010, 5751
- Transport Layer Security (TLS), IETF RFC 2008, 5246
- Extensible Messaging, Presence Protocol: (XMPP): Address format, IETF RFC 2015, 7622

31. Noumeir R: Sharing medical records: The XDS architecture and communication infrastructure. *IT Professional* 13:46–52, 2011
32. Integrating the Healthcare Enterprise (IHE), Cross-enterprise document sharing for imaging (XDS-I.b), 2017. Available at: http://wiki.ihe.net/index.php/Cross-enterprise_Document_Sharing_for_Imaging. Accessed 18 October 2018
33. Guo Y, Hu Y, Afzal J, Bai G: Using P2P technology to achieve e-health interoperability. 8th international conference on service systems and service management. *IEEE*:722–726, 2011
34. Urovi V, Olivieri AC, Torre AB et al.: Secure P2P cross-community health record exchange in IHE compatible systems. *Int J Artif Intell Tools* 23:1440006, 2014
35. Figueiredo JFM, Motta GHMB: SocialRAD: An infrastructure for a secure, cooperative, asynchronous teleradiology system. *Stud Health Technol Inform* 192:778–782, 2013
36. Ribeiro LS, Bastião L, Costa C, et al.: Email-P2P gateway to distributed medical imaging repositories. *Proc. HEALTHINF 2010* 310–315
37. Weisser G, Walz M, Ruggiero S, Kämmerer M, Schröter A, Runa A, Mildenberger P, Engelmann U: Standardization of teleradiology using DICOM e-mail: Recommendations of the German radiology society. *Eur Radiol* 16:753–758, 2006
38. Simple Mail Transfer Protocol (SMTP), IETF RFC 2008, 5321
39. Weisser G, Engelmann U, Ruggiero S, Runa A, Schröter A, Baur S, Walz M: Teleradiology applications with DICOM-e-mail. *Eur Radiol* 17:1331–1340, 2007
40. Oliveira MAL: Forming an information infrastructure for teleradiology: A series of case studies based on the design theory for dynamic complexity. M.Sc. Thesis, Dept. informatics, fed. Univ. Paraíba, João Pessoa, Brazil, 2015
41. Fielding RT: Architectural styles and design of network-based software architectures. Ph.D. dissertation, Univ. California, Irvine, CA, 2000
42. Internet Message Access Protocol (IMAP), IETF RFC 2003 3501
43. Amazon Web Services, Inc., Authenticating requests using the REST API. [online]. Available at: http://docs.aws.amazon.com/AmazonS3/latest/dev/S3_Authentication2.html. Accessed 18 October 2018
44. Keyed-hashing for message authentication (HMAC), IETF RFC 1997, 2104,
45. Lucena-Neto JR: DICOMStudio: Multidomain platform for teleradiology. M.Sc. thesis, Dept. Informatics, Fed. Univ. Paraíba, João Pessoa, Brazil, 2018

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.