

# CyclopsDistMedDB. - A Transparent Gateway for Distributed Medical Data Access in DICOM Format

Leonardo Andrade Ribeiro  
*The Cyclops Project,  
Telemedicine Laborator,  
University Hospital (UFSC)  
Florianópolis – SC – Brazil*  
lar@inf.ufsc.br

Paulo Roberto Dellani  
*The Cyclops Project,  
Telemedicine Laboratory,  
University Hospita (UFSC)  
Florianópolis – SC – Brazil*  
dellani@inf.ufsc.br

Aldo von Wangenheim  
*The Cyclops Project  
Computer Sciences  
Department (UFSC)  
Florianópolis – SC – Brazil*  
awangenh@inf.ufsc.br

Michael M.Richter  
*The Cyclops Project,  
Universität Kaiserslautern,  
Germany*  
richter@informatik.uni-kl.de

Kerstin Maximini  
*The Cyclops Project,  
Universität Kaiserslautern,  
Germany*  
k\_maximi@cs.uni-hildesheim.de

Eros Communello  
*The Cyclops Project,  
Universität Kaiserslautern,  
Germany*  
eros@informatik.uni-kl.de

## **Abstract**

*The image diagnosis area is the most propense medical field to Telemedicine, because it does not obligate a direct contact of the patient with the responsible radiologist during the building of the report. The persistent lack of specialists on places distant from urban centers makes the Telemedicine an important tool for improvement of healthcare services. In this work we present a framework, called CyclopsDistMedDB, for the integration of distributed DICOM medical record databases over wide areas. The present system has a central module that is responsible for receiving the clients requests about patient data (images, waveforms), performing the querying and retrieval of images, patient records etc. from the specific DICOM databases containing the data requested and delivering them to the clients. The data communication protocols adopted are DICOM, for retrieval of objects directly from DICOM data servers and CORBA (Common Object Request Broker) for the delivery of DICOM data to client applications.*

## **1. Introduction**

The need of storing and making available digital medical examination data containing images and biological signals, like computed tomography, magnetic resonance and electrocardiography, is increasingly present in the hospital and clinics environments. The “filmless radiology” represents a solution to improve accessibility, quality and quantity and, at the same time constrain the healthcare costs. In this scenario, the DICOM standard has become an effective international standard and the most important protocol used in Radiological Information Systems (RIS).

The Telemedicine is one of the most important supporting technologies to bring the healthcare services closer to citizens. In order to achieve this, the Telemedicine services need to become more global and ubiquitous; in particular a standardized communication is necessary. Isolated and self contained systems must move toward an integration and sharing of information throughout hospitals, increasing their interoperability and providing more general services.

The transparent interchange of medical image and signal data through the Internet by medical organizations is essential in order to eliminate completely the necessity of the physician's presence on the site where the images are produced. A deeper integration of image and signal databases between different, distant hospitals is necessary for a better follow-up of the patient's health history, enabling a drastic reduction of duplicate examinations in emergency and outpatient situations and also supporting the providing of second opinions and even other not so obvious benefits like better scheduling of work between clinics who operate on different places.

The main goal of this work is to provide a framework that allows hospitals of any size which have DICOM image and signal databases running in their Intranet environments to share studies among them under secure and functional conditions.

## 2. Problem Description

The DICOM standard has become a *de facto* world standard, but its use in an Internet wide context is still very limited. The transfer and storage of radiological images between peer entities is done mostly in Intranet environments. In order to build a general and transparent mechanism for sharing images between different clinics and hospitals, it is necessary to deal with two main issues: a strong support for secure access control to individual studies and the ability of uniquely identify patients among different domains, which are both not yet supported by the DICOM standard.

Any system working with sensitive information has to guarantee the security of transmission and a rigid access control over its data. On part 15 of the DICOM standard [6], there is specified the support for connections over Secure Socket Layer (SSL), but access control is still defined on database level, not patient or study levels. Currently, there is a proposal to the DICOM standard based on encryption within the application layer, which consists in new attributes for DICOM objects where the sensitive information about a person will be ciphered. This approach requires less time expenditure than the transmission over SSL/TLS.

On the other hand, the access control specified in the DICOM standard is entirely delegated to the Application Entities (AEs). It is assumed that the AEs involved in a DICOM data interchange are implementing appropriate security policies, as access control, audit trails and mechanisms to identify users and their rights to access information. Unfortunately, most of the DICOM database server implementations only follow the security levels specified in the standard, with access control based on the context of applications and hosts with no user-based authentication. Another important point to be taken into account is the subject of distribution of access rights. For a more strict access control, the access right distribution must be based on studies and not on database level. In spite of the fact that the process of managing authorization decisions on fine grained resources is an expensive action, a rigid control over the information interchanged is a critical requirement in regional healthcare network-compatible applications.

The unique patient identification among database objects located at different systems is still another issue that must be addressed to enable the sharing of those images and signal data between different locations in a regional healthcare network. The patient's moving or a change of healthcare provider will lead to a same person to have studies stored at different places. Historically, health care providers dealt with this issue by creating a Master Patient Index (MPI) that used a limited set of

demographic data (for example, name, gender, date of birth, etc) to help retrieve the disparate elements of a patient's records. In order to gain access to information about a person stored in DICOM databases from heterogeneous systems, it will be necessary to create a centralized MPI service able to identify correlated data and to provide links between them.

### 3. Distributed DICOM Database Gateway

This work presents a model for a transparent access gateway for distributed medical data in DICOM format called *CyclopsDistMedDB*. This solution is based on a centralized approach, with a module managing transactions between clients and the DICOM databases. This module is responsible for receiving the client requests about patient data (images, waveforms), performing the querying and retrieval of these objects from the specific DICOM databases containing the data requested and delivering it to the clients. The data communication protocols adopted are DICOM, for retrieval of objects directly from DICOM data servers and CORBA (Common Object Request Broker) for the delivery of DICOM data to client applications. Both communications are performed over a secure channel using SSL. The choice for CORBA for the communication with the clients provides more flexibility to the system and allows the use of the system together with commercial Internet providers. The multi-language feature of CORBA allows easily applications written in different languages to use the services of our approach. Figure 1 describes the CyclopsDistMedDB communication model.

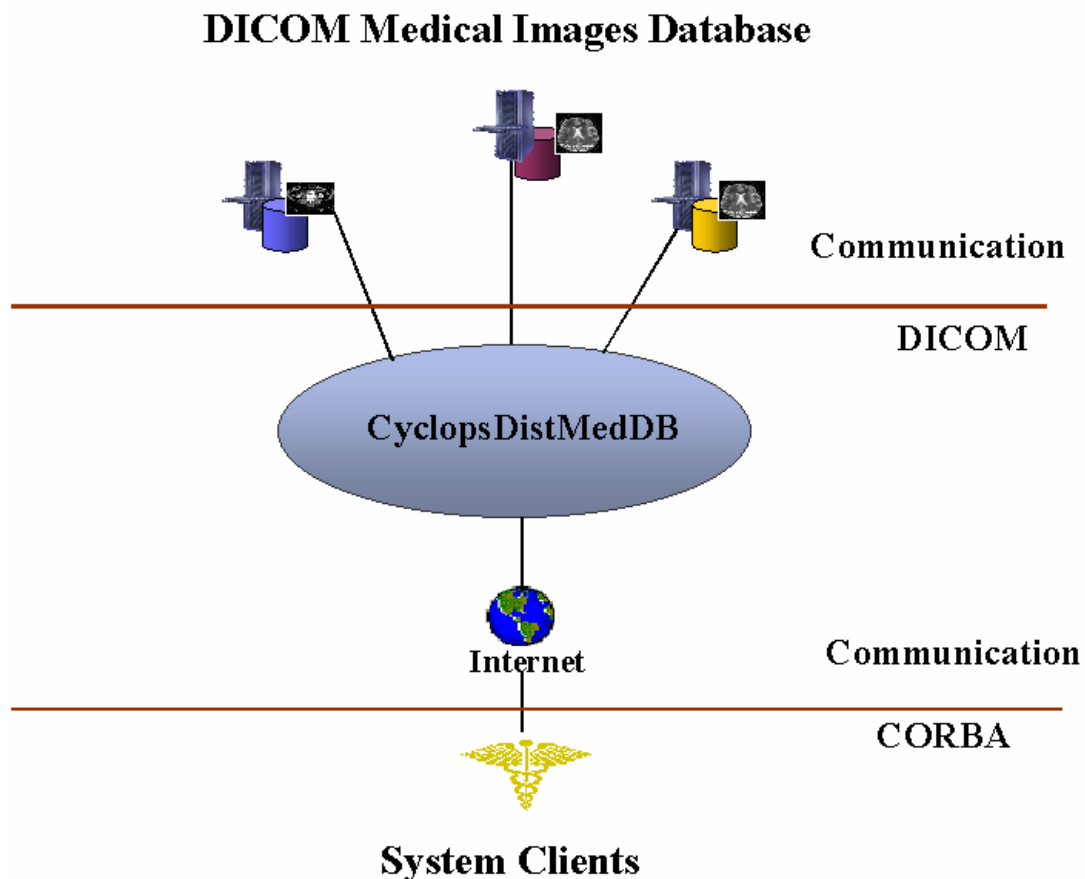


Figure 1. Communication model among CyclopsDistMedDB clients and DICOM servers

The use of a centralized intermediary instance to interchange image and waveform objects among the servers and clients provides facilities for the easier configuration of both entities. The client applications just need to keep CORBA data like IDL interfaces and object references for request services. On the image servers side, it is necessary only to enable the connection with CyclopsDistMedDB as a DICOM Application Entity. The configuration of the whole system is performed on the central module, and the addition or removal of one participant does not pose the need of the reconfiguration of all the others. Additionally, this approach allows dial-up and DSL clients to gain access to images on DICOM databases, which is difficult in traditional DICOM configurations because these clients have temporary IP addresses, and DICOM servers request pre-knowledge about the IP address of their clients and callback enabling. A table of metadata in the gateway module contains information about patients, their studies and their places of origin and storage. This information is kept updated by the nodes containing the DICOM servers through a daemon which retrieves local information from the DICOM database through C-FIND message service [5] and sends information about new studies to the central gateway.

To be able to identify some amount of information from different places as concerned to a same patient, the system employs a MPI which is executed each time new data from the DICOM database demons arrives, correlating information related to the same patient but originated from different places. An implementation of a MPI system based in the probabilistic approach of [3] will be deployed on second stage of the development of CyclopsDistMedDB.

## **4. Security, Ethics and Access Control**

Medical ethics and sensitive information protection against unauthorized access are a key issue in this field and addressed in this work through connection security policies and a special access control strategy.

### **4.1. Security for Data Interchange**

The support of secure channels during the data transmission is provided through TLS, both on the CORBA and DICOM side, providing for encrypted connections. In spite of the loss of generality because there are many DICOM databases which do not employ TLS, this requirement is essential to use DICOM network services on Internet/WAN level. A DICOM server that is not conformant with DICOM Secure Connection Transport Profile should not be used on public networks.

During data transmission from DICOM servers to CyclopsDistMedDB, the TLS communication employs host authentication of both sides. CyclopsDistMedDB allows DICOM connections only from hosts registered as DICOM data suppliers and with known public keys.

### **4.2. Access Control Strategies**

The present work does not intend to provide security for each participant individually. It is assumed that each Application Entity insures that its own local environment is secure before even attempting secure communications with the system. Thus, access policies of the system are extending the Intranet secure context, that each clinic or hospital must have implemented, toward the Extranet environment.

To enable a fine-grained access control at study level, the system provides identification of all the interested parties involved in patient care, providing user-based and role-based authorization controls.

The main objective is provide an essential guarantee for privacy of sensitive patient data, keeping the doctor-patient trust relationship during Telemedicine practice.

Implementing the basic precepts of the medical ethics in the Telemedicine field, is although not an easy task. The non-existence of international rules and mediator associations able to provide well-defined ethical rules, makes the building of a specific access policy hard. One of the common sense rules for the practical Telemedicine is the one that the patient must have pre-knowledge of any transmission of his/her studies. Emergency conditions, with eminent danger of life should constitute an exception, but without exempting the physician of any responsibility for the handling and the correct use of the sensitive information of the patient. Another requirement, recently highlighted by the rules defined by U.S. Health Insurance Portability and Accountability Act (HIPAA), is that the patient must have extensive access to any kind of medical studies about him [4].

In order to satisfy the medical ethical issues without loosing the functionality, we propose that a system that distributes patients records over a public network must attend at least the following features:

- The access policies are applied at the study level, which means that each study that belongs to a patient can have its own access policy;
- Studies can have multiple security levels. A radiologist or responsible technician can determine that a study can be accessed only by users with explicit permission to do it (this is the appropriate default behavior), or by users with special rights (i.e., the one responsible for the emergency room of a hospital) or even though allow access to any system user.
- The system provides interfaces for the patient who has studies stored on it, to access its own data. The patient can view and control who has access, who is accessing its information and avoid inappropriate use of that information;
- Users which not are expressively allowed to access some information not must have any access or view to this information;
- A extensive log of the operations must be employed for audit purposes;

Information about other studies in the distributed database is completely filtered out, providing for each user different views about the data managed by system. It is possible for a physician who is participating directly on the treatment to grant access to a study for another physician for second opinion purposes. Each operation of granting permissions is recorded in the system for audit purposes.

In order to deploy the access control stated above, we used the basic lifecycle service provide by CORBA specifications. The client application holds a stringified reference to a CORBA Factory object on CyclopsDistMedDB. First, the only usable interface of this object is the one that receives the user login-password data. After a successfull validation and identification on the system, an instance of the class which holds the session context for this user is created. We use extensively the object-oriented polymorphism feature in order to deploy different user roles. The system objects wrapping DICOM data maintain information about the users who are allowed to access them and which operations could be performed. The object encapsulation enables a good level of security.

## 5. Conclusions

We developed a model for a distributed DICOM-compliant medical database accessible through a central gateway, allowing the creation of regional healthcare networks providing image and signal data. This model solves various security and accessibility problems related to the DICOM Standard, without changing the standard itself, thus allowing the integration of existing PACS systems into a network of connected hospitals of any size.

This work aimed at the development of a technology of a distributed database of images and biological signals, able to be used on high speed networks as a central gateway for access to DICOM databases located in different and possible geographically distant places, providing the security and transparency requested by this kind of application. A first prototype implementation of this model has already been developed and is being tested in the scope of the German-Brazilian Cyclops Project.

## References

- [1] Dellani, Paulo Roberto; Desenvolvimento de um servidor de imagens médicas digitais no padrão DICOM; Dissertação de Mestrado - UFSC - CPGCC– 2001.
- [2] Elmasri, R. Navathe, S. 1994 Fundamentals of Database Systems. Second edition – Addison-Wesley, 1998.
- [3] Fellegi, Ivan; Sunter, Alan; A theory for Record Linkage. Journal of the American Statistical Association, American Statistical Association, December 1969, Vol. 64, N° 64, N° 328, pp. 1183-1210
- [4] Health Insurance Portability and Accountability Act of 1996 <http://www.hcfa.gov/hipaa/hipaahm.htm>. Last Access in November, 10th 2001.
- [5] National Electrical Manufacturers Association. Digital Imaging and Communications in Medicine (DICOM) - Part 15: Message Exchanges. Virginia, 2001. On-line available at: <[ftp://medical.nema.org/medical/dicom/2001/draft/01\\_15dr.pdf](ftp://medical.nema.org/medical/dicom/2001/draft/01_15dr.pdf)>.
- [6] National Electrical Manufacturers Association. Digital Imaging and Communications in Medicine (DICOM) - Part 15: Security Profiles. Virginia, 2001. On-line available at: <[ftp://medical.nema.org/medical/dicom/2001/draft/01\\_15dr.pdf](ftp://medical.nema.org/medical/dicom/2001/draft/01_15dr.pdf)>.
- [7] Object Management Group – <http://www.omg.org>. Last Access in March, 10th 2002.
- [8] Request for Comments: 2437 PKCS #1: RSA Cryptography Specifications Version 2.0 On-line available at: <http://www.rsasecurity.com>
- [9] Siegel Jon; CORBA 3 – Fundamentals and Programming, Second edition, John Wiley and Sons, 2000.
- [10] Stallings, Willian; Cryptography and Network Security. Prentice Hall, 1998.
- [11] Stevens, W. Richard; TCP/IP Illustrated The protocols – Volume 1 – First edition. Addison-Wesley, 2000.