A flexible web oriented Telehealth platform using a RIM-HL7 Based Model

César Sánchez, Edwin Triana and Eduardo Romero
Grupo de Investigación BioIngenium
Centro de Telemedicina
Universidad Nacional de Colombia
Bogotá, Colombia
[cesasanchezb,emtrianag,edromero]@unal.edu.co

ABSTRACT
This article presents a web oriented telehealth platform adapted to the social and economic conditions of a developing country like Colombia. The platform aims to satisfy health care needs integrating modules for telemedicine, where medical processes are modelled following the HL7 Reference Information Model which has allowed easy inclusion of many specialities such as dermatology, radiology, cardiology, pathology and infection diseases, among others. The system implements many security mechanisms such as Digital Signature and Zero Knowledge Proof for authentication. A telecare real-time module measures patient's vital signs such as blood pressure, electrocardiogram, oxygen saturation and sends them over the network to monitor patient's health. After 19 months of service, the system processed 4.751 actual telemedicine cases from 31 remote stations with an average response time of 1,3 days, showing flexibility, security and scalability.

Categories and Subject Descriptors
H.4 [**Information Systems Applications**]: Miscellaneous; C.5 [**Computer System Implementation**]: Miscellaneous

General Terms
Design, Security

Keywords
HL7, Information systems, telemedicine, telehealth, zero knowledge proof, real time telecare

1. INTRODUCTION
Telemedicine has come to be a health tool which allows the access for some underserved regions to highly specialized medical services. Specialities such as dermatology, radiology or infection diseases are nowadays available for such regions thanks to new communication networks, capable to support great information traffic. Challenges with this new brand activity comprise efficient service offers through information systems, an opportune clinical history access, implementation of new functionalities, maintenance of integrity and data confidentiality and easy scalability. Such requirements are difficult to meet and many commercial solutions have failed because of the usual entity-relation database model need not be an appropriate choice or because the technological solution is quite limited concerning the problem requirements.

Telehealth networks that rely on custom built systems are expensive because they are made for specific users operating in specific settings and lack of open connectivity [9]. The developed system may be deployed and used in many operational systems with different software and hardware configurations.

First formal developments in telemedicine followed a store and forward model. They were based on a standalone application in the remote station, which locally saved patient information along with images or support files, and sent it to the reference center when the bandwidth for transmission reached a certain pre-defined level. This model presents some limitations:

- Patient information is only accessed either at the remote station or at the reference center. Therefore, information is highly scattered and difficult to recover.
- Any modification results in a change in the software code for the remote stations, a requirement which is difficult to achieve.
- Any input to the system i.e. a new specialist, or speciality produces an individual database replication for each local database station.

To deal with some of these inconvenients, different variations on this model have been proposed. For instance, once a new patient is introduced into a local database, this is automatically replicated into the other network nodes, that is to say, into the other local databases. The main drawback with this approach is that a failure probability increases with each new remission center, but also the consumption of network and storage resources result inadequate. Another partial solution was based on dedicated storage systems, where a software is responsible to archive the existant information

EATIS '08, September 10-12, 2008, Aracaju, Brazil

in the different local databases and to gather it together into a central database, whereby a complete clinical history is available. Nevertheless this approach duplicates the work and demands additional applications for consulting this information.

In the present work, a conventional telemedicine network is made up of several remote stations and a reference center. In the remote station a general physician checks out a patient and uses an application to register both the patient and relevant clinical information. These data are sent to the reference center where a specialist reads the case and provides diagnosis and treatment, which are sent back to the remote station so that the general physician receives the specialist feedback. For real time telecare, data are sent to the reference center where a server broadcasts signals to the specialist work station.

Practices covered by the system such as teleradiology can bring many advantages to healthcare organizations such as cost savings, access speed, availability and patient information confidentiality [2]. The current telemedicine network has been able to attend many cases of underserved communities in the Amazonian, Orinoquian and Caribbean rainforest where access and resources like bandwidth are limited.

Telemedicine provides services such as diagnosis, consultation, medical treatment, transmission of a medical information, and health education by using different technology for the communication network [7]. Regardless of the technology used, many telemedicine projects lack of continuity, permanent feedback and many others are only short experiments. Here is presented an interdisciplinary work immersed in a telehealth project covering not only a real and continuous telemedicine network, but investigation and administrative tools.

The rest of the paper is organized as follows: In section 2 main system requirements are presented, section 3 presents technical issues related to the fulfillment of requirements, section 4 shows how the system has grown and how has it helped to improve the health care of favored regions. Finally, section 5 mentions main contributions of the work.

2. REQUIREMENTS

An ideal health information system must guarantee the quality of medical information, following criteria about integrality, sequentiality, scientific rationality and clinical history availability and opportunity. Main issues are described hereafter:

- The clinical history must register patient information as well as clinical information about medical procedures on the patient. This document must be chronologically organized and also be continously updated.
- The clinical history must assure consultation at any time and from any place, but the access must be restricted to health professionals or other authorized personnel.
- At the time of information storage, the used application must provide security mechanisms for identifying the personnel responsible and also avoid later modifications of data.
- The specialist answer must be integrated into a digital signature procedure, which assures the information consistency at any time.
- Consultation must support any kind of required file such as dermatology images in tiff or JPEG formats, radiology images in DICOM format, electrocardiogram files or any relevant case file.
- As long as new telemedicine services are included, the system must support scalability regarding specialities, patients and specialists.

For the telecare case, there exists new requirements about the use of network resources and multiple patient care of a remote point.

1. General Telecare Requirements
   - The Specialist monitors remote patients, optimizing network resources
   - A module for vital measurements must be provided. These measurements include systolic, mean, and diastolic blood pressure; pulse rate; oxygen saturation, pletismography and electrocardiogram
   - The vital signs must be stored in a central server in order to check the patient status in any time
2. Remote Requirements
   - Medical hardware should be medically certified
   - The system must take status signs and send them to the central server
   - A remote point can have one or more care patients
   - The monitoring process must be independent of the network connections
3. Reference center requirements
   - The specialist checks the status patient in real time
   - Devices must be controlled and configured remotely
   - The module shows the devices status (i.e. non-connected)

3. METHODOLOGY

Environment integration, acceptance doctors and technical standards, are fields of telemedicine in which many innovations may be developed in the near future [6]. An initial phase of requirements analysis and review of standards was firstly carried out. A list of requirements was obtained by an extensive poll with both future users and specialists in order to gather together their observations about the expected system functionalities. The database model was adapted from the information model (RIM) proposed by the HL7 organization. This model was implemented on a PostgreSQL server, along with the needed functionalities for searching and data operation. The system was developed in Java, under a J2EE architecture and using the JBoss application server.

3.1 Teamwork organization

The whole development was divided in three groups: first group was responsible for system analysis, design, development, installation and documentation; second group was dedicated to evaluation and planning and the last group was focused on validation. The first group determined the initial requirements, as well as the HL7 based data model design. Development was accomplished under the extreme programming philosophy [3] (in an increasing manner), given the high variability requirement. This group comprises both, hardware and software development. Maintenance of different production versions was carried out through an open-source revision control tool (subversion), applying a branching technique for keeping the different versions.

3.2 Multi tier Architecture

To provide scalability and flexibility, the system was implemented under a service based architecture, which guarantees low coupling between components. The system architecture is made up of four layers: the GUI layer, which comprises JSP pages, applets and servlets; the Business Logic layer, where the application directives are defined; the Data Access layer, which provides and coordinates data transmission between the Storage and the Business Logic layer; and the Storage layer, composed basically by the database. Figure 1 shows the system layers with their core components, the Business Logic layer shows a Service Oriented Architecture (SOA) [8, 4], where the component granularity provides loose joint.

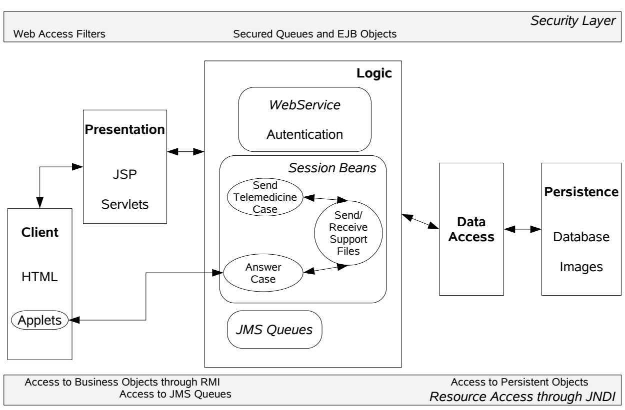

Figure 1: Architecture by Layers.

In this design, client accesses services through interfaces so that the implementation of services is independent of the specific service definition. Therefore, required changes in the GUI, only affect the Web application, not the core components. Likewise, changes in the WebService implementation or in any EJB (Enterprise Java Bean) need not affect the GUI.

3.3 Data Model

HL7 (*Health Level 7*)[1] is an organization who is responsible for developing standards in health care and who is accredited by the ANSI (*American National Standards Institute*). HL7 efforts are focused on administrative and clinical data management. An important initiative proposed by this organization is called the Reference Information Model (RIM), an abstract model for medical information management and whose backbone classes comprise:

- Act: All the actions performed in a health care context, which must be recorded and documented.
- Entity: Represents things and beings which are allowed to change very little or nothing that are of interest to, and take part in health care.
- Role: Establishes the roles that entities play when they participate in health care acts.
- Participation: Represents the context for an act, such as who performed it, to whom and where it was done.
- Act Relationship: Represents links between acts, defined by composition, sequentiality, precondition or postcondition.
- Role Link: Represents relationships between roles, such as dependencies or hierarchies.

Each backbone class inherits to many subclasses which provide more specificity to the data model. Also, this structure permits to add new subclasses, based on the RIM's classes, whereby it is quite easy any adaptation of the reference model to the particular needs of health entities. Overall, classes are related with the others such as figure 2 illustrates.

3.3.1 RIM adaptation to telemedicine

The RIM proposes a general framework for health care applications, which must be adapted for telemedicine applications. Information about the entities that are part of several acts were stored using the Living Subject, Person and Organization classes. Each entity may play roles such as Patient, Physician, Specialist, User, Agent and Service Delivery Location. Possible acts are: Patient Encounter, Observation, Diagnostic Image, Diagnosis, Clinical Document and Control Act.

Each telemedicine case, sent from the remote stations, is composed of the patient data, information about the medical institution, medical measurements, specific data for each speciality, images and support files. This information is structured as the acts associated by a hierarchical scheme. First, an instance of the Patient Encounter class stores the very basic medical information, along with the case number. Each measure (general or specialized) is stored as an individual act, and related to the principal act through the class Act Relationship. This scheme allows easy inclusion of new specialities or any additional data input to the system, with no changes at all in the data model. Each image or support file is stored as a Diagnostic Image act, and is related to the principal act as it is done for measurements. Finally, a Control Act registers that this new telemedicine case is created.

When the specialist checks out the case and answers (a diagnosis), another Control Act records that the case was read and answered. The diagnosis and treatment info is stored in a Diagnosis act, along with a ICD code (International Classification of Diseases). This act is related to the principal case act through an instance of the Act Relationship. A

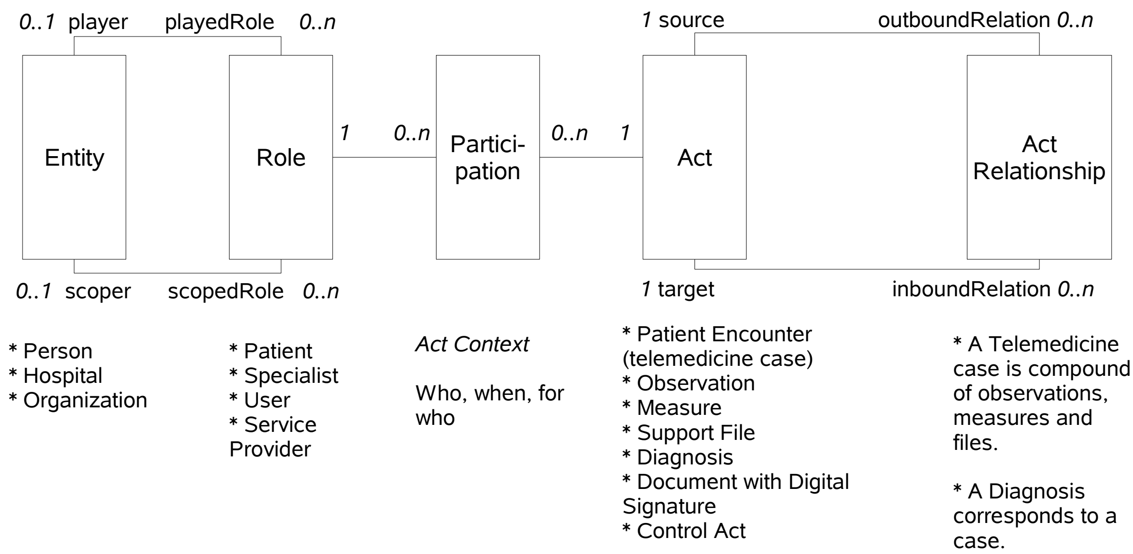

Figure 2: Reference model adapted to Telemedicine Information System.

PDF file that contains the diagnosis is generated and its filename is stored in a Clinical Document act, related directly to the Diagnosis act.

This model versatility provides us with a proper management of associated events as well as an useful modeling of every telemedicine situation. Particularly, to control session logins and logouts, a Control Act is used for assigning roles to connected users. Thus, data model allows to audit each performed act, maintaining a register of participating entities and roles.

3.4 System Modules

According to the pre-defined user's role, the interface displays the available modules for this user.

3.4.1 Remissions

The module used for telemedicine remissions is only accessed by users who have the role "Agent". Here, the user chooses an speciality and then a form is displayed; the user may then introduces the Patient info, anamnesis, some vital or any other specific measurement, depending on the chosen speciality, and the associated support files.

3.4.2 Diagnosis

This module is used by specialists to make diagnosis based on remissions. In this module, a form shows the whole case information. Diagnosis is sent through an applet with the following functionalities:

- To allow the expert to deem the image quality following a pre-defined scale, and introduce the final diagnosis and treatment.
- A list of Diagnosed Diseases according to the International Classification of Diseases (ICD) is integrated into the system so that the user selects the disease associated to the consultation.
- A specific java panel allows to add the speciality form. For example in mammography, a field allows to select the BI-RADS (Breast Imaging-Reporting and Data System) Category.
- A security mechanism such as a digital signature is also integrated in order to ensure data integrity of the document.
- A security mechanism is provided to start the transmission of data between java clients and the server. This is accomplished using a Zero Knowledge Proof Mechanism. This mechanism is better explained in section 3.6.3.
- A PDF file is generated together with information of the patient, the remission center and the answer of the case. This document is digitally signed using a security certified system which is within a personal USB which is needed at the time the diagnosis must be sent.
- Secure data transport is provided through a RMI+SSL socket for data input and PDF report file.

3.4.3 Queries

Both users of remote stations and specialists access the query information module. Here, some criteria for searching cases and diagnoses are presented: patient identification, number of case, speciality, specialist who gave an answer and the responsible user (the one that sent the case). In this module all information concerning a case or to a patient can be retrieved including the sent files and the answer in PDF format. For specialists, this module also gives the opportunity to give a new opinion about a case already attended, redirecting to the Diagnosis module.

3.4.4 Videoconference

Thinking on the patient interaction with the specialist, the videoconference module was incorporated to the system.

Once the remote doctor has sent patients cases, the specialist, the patient and remote doctor meet in the videoconference.

In order to adapt this module to the low bandwidth conditions, the developed system offers the possibility of configure the used bandwidth in the video and sound parameters in an independent way, making efficient use of the network resources, by reducing the video to 1 frame per second (1 Kbps) and the voice to 3 Kbps, without affecting the communication between patient and specialist. The video quality is less important because the videoconference is not used to show patient's images, but only for physicians dialogue.

3.4.5 Statistic Tool

This administrative tool allows the administrative personnel to obtain some statistics about the system. For this purpose, a separated database is used for the OLAP module. An automatic daily updating of the datamart has been set up from the transactional database. In the star schema the dimensions used are Remote Station, Speciality, Time and Diagnosed Disease according to the International Classification of Disease (ICD) codes. The table of Facts registers the number of cases, the number of images, the disk usage and the response time. Figure 3 shows the datamart model.

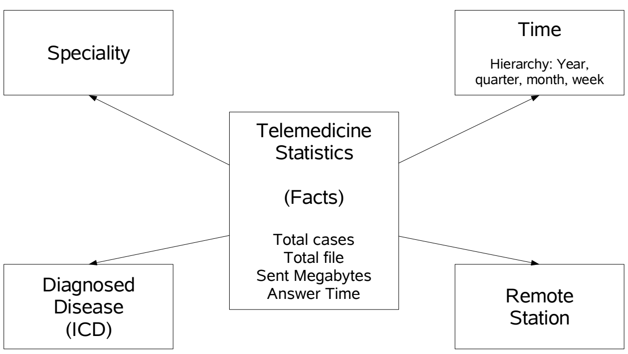

Figure 3: Statistics tool's star schema

3.4.6 Real Time Telecare

The Telecare module was developed for patients requiring real-time monitoring in a remote place, while the specialist team can be at the reference center or in different cities

The proposed architecture was based in a Messaging Schema where applications can create, send, receive and read messages in a distributed enterprise system [5]. In our case, the remote station (sender) shows and sends signs (message) through the network to the Application Server (AS). Then, the AS re-directs the signal to specialists (Subscriptors). Likewise, doctors can send control messages to configure or to operate devices (i.e taking blood pressure), and the process results are notified to all terminals using a normal sign message, figure 4.

In a standard execution environment, a patient is monitored from Bogota, the vital signs are sent to the server and then are broadcasted to the specialists. If a control message must be sent (i,e take blood preasure), this is added to a FIFO message queue, then this control message is received and executed in the patient side (remote application) and finally the results are notified to the server in order to report it to the specialist. In case of two or more specialist sending different control messages, these are placed in the queue in a consecutive way, however, any operation (control message) can be canceled by a specialist in any moment.

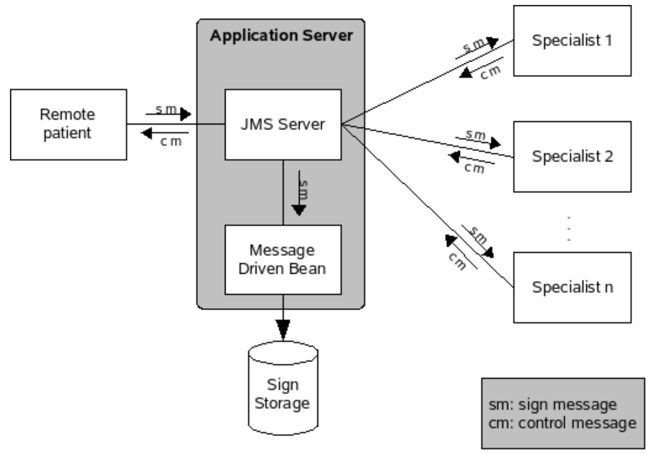

Figure 4: General Telecare Architecture

The module is composed of a physical part, sensor devices, station computers and server machines, and a logical part, the software module and the application server. The used sensor devices were the non-invasive blood pressure, three-channel EKG and pulse oximeter. The software was developed in Java and the application server was JBoss 4.2.2 with Java Message Services enabled.

Data Acquisition and Transmition.

Devices acquire patient's signs every millisecond (ms). This information has to be shown and sent to the reference center. In our case, this transmission spend between 150 Kbps y 200 Kbps per patient, a harsh value in environments where the bandwidth varies between 100Kb and 250Kb. Therefore was designed a transmission strategy, where a new acquired sign is saved in a temporal buffer, and it is sent embedded in a packet every 150 ms, so the bandwidth consumption is reduced to 7Kbps.

In difficult access environments with small bandwidths (smaller than 56Kbps), doctors could increase this period up to 1000 ms, getting a reduction of the used resources up to 2Kbps, but losing quality in the EKG and Pletismography diagram.

3.5 Physical System Architecture

The Physical System Architecture is composed of a group of centralized servers, as shown in figure 5. The servers manage a storage system, built up on top of two storages of 3 Terabytes configured on RAID 5. The first storage is used to save all the data related with each case, namely the transactional database, support files and digitally signed documents; the second one holds a daily backup of the database. Three additional machines are used, one for the application server used for basic telemedicine, another for the Java Message Service (JMS) server used for telecare and the last one server for the database management system with the Datamart.

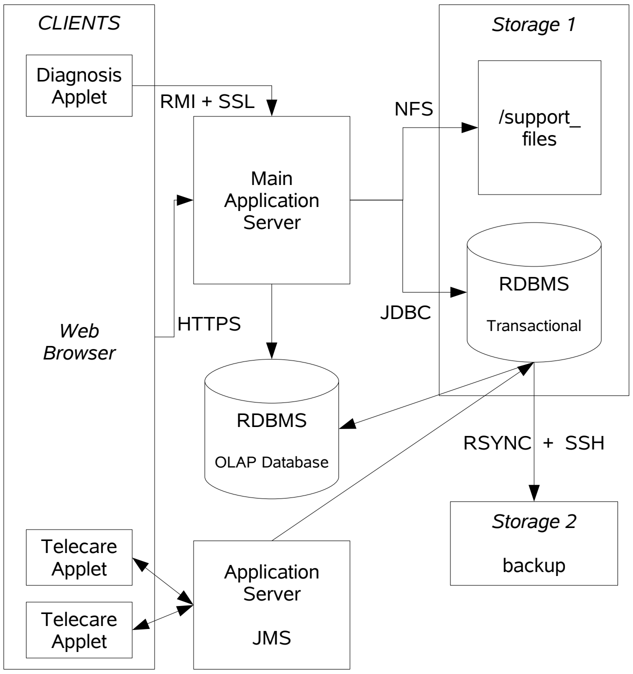

Figure 5: Physical Architecture.

3.6 Security mechanisms

3.6.1 Data Transmission over SSL

The clients plug into the application server through a web browser, using the HTTPS protocol, whereby the integrity and confidentiality of the medical information transmitted is assured. The Java applet used for specialists to answer each telemedicine case, uses a different network connection. To secure this new socket, it performs remote invocations (RMI - Remote Method Invocation) through SSL (Secure Sockets Layer). Each client must have the server certificate to be able to open the secure connection.

3.6.2 Role based Filters

The application uses the Intercepting Filter Pattern to ensure that the accessed data and services may be displayed or used for the user connected, according to his associated roles. Thus, for example, a remote doctor user cannot access to the java applet, a specialist cannot access to the module for sending a new case, and a user that is not a health professional can only access to the statistics datamart.

3.6.3 Zero Knowledge Proof Authentication Mechanism

Restricted access generally demands identification with username and password, a mechanism which is far from being secret. This situation can even worsen because password for someone else's benefit.

The system requires possession of a little personal USB device that contains a secret password (unknown even for the user) that is never revealed to any of the involved entities in the information system. This device uses a variant of a cryptographic method called Zero Knowledge Proof or ZKP, which uses an undetermined sequence of mathematical questions and answers so that the algorithm allows the device to demonstrate to the system that the user is in possession of a valid password, but without revealing it.

In contrast to RSA and ElGamal systems, ZKP requires small numbers for an appropriate operation i.e. of the order of 64 bits. A ZKP is a dynamic method carried out for an entity to prove to another that a declaration (usually mathematical) is true, revealing nothing but the veracity of the statement [10]. One entity proves its identity to another by demonstrating that it has a secret, but without disclosing it. A zero knowledge proof must satisfy the next properties [11]:

- Completeness: if the declaration given by the prover is true, the honest verifier will be convinced of this fact.
- Soundness: if the statement is false, no dishonest prover will be able to prove the verifier that it is true, except with a very low probability.
- Zero-knowledge: if the declaration is true, none of the verifiers can learn anything else from this fact.

A typical zero knowledge proof begins when the prover sends a random commitment and then a random challenge is provided by the verifier. The answer given by prover depends on both, the commitment and the challenge. This protocol can be performed several times and, depending on the obtained answers, the verifier can either accept the proof or decline it [10].

Certainly, this protocol could be infringed but it can be made safer through repetition. With repetition in execution the probability of fraud reduces to half of last probability. Therefore, with only 10 executions the probability of fraud is less than 0.097%, resulting in a security level higher than 99.9%.

FIAT-SHAMIR, a variation of the ZKP, was the selected algorithm to implement in a microcontroller with an USB interface. The Microcontrollers used have the enough memory size (An 4 KB EEPROM) required for the storage of the personal encrypted information used for the digital sign (See section 3.4.2), a clock frequency up to 8 Mhz, a 128 KB flash memory and an 8 bit ALU (Arithmetic Logic Unit) to easily make operations with 64 bit variables, which supports standard computational platforms.

A library (DLL) was developed to make the communication between the microcontroller and the computer client. Methods in the DLL are acceded from the Java applet using JNI (Java Native Interface). Technically, this is possible because the applet is digitally signed and the user's java policy file allows the load of libraries to applets digitally signed with the key associated with the telemedicine certificate. The server sends challenges and receives commitments and proves from the clients through RMI. Then, the java applet serves as communication bridge between the prover (the microcontroller) and the server (the verifier). The user can send the medical report once the authentication is executed, and the delivery of the document to a server (with the digital signature, in pdf format) becomes effective.

The figure 6 summarizes the logic architecture used for communicate the honest verifier and the prover.

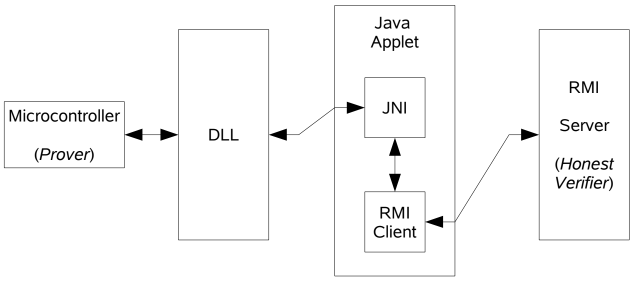

Figure 6: ZKP Mechanism Logic Architecture

4. RESULTS

Currently, 31 hospitals of first and second level complexity use this system for remission of cases, and 20 specialists, working in different third level complexity health institutions, use this system for answering and solving the cases. Internet access for each remote station, is provided by any of the three network hospitals so that connection bandwidths are different for each link. Each of these hospitals are health centers for their respective underserved regions and their action radius covers populations which vary between 200.000 and one million inhabitants. Information about geographic distance of different regions and number of hospitals per region is shown in table 1. The listed areas belong to the Amazonas, Orinoquian and Caribbean rainforest. The channel bandwith speed of the hospitals varies from 128 to 512 Kbps and is shared with other computers in the organization so that effective bandwidth is even smaller in actual operation times.

Remote Region	Number of hospitals	Distance from Reference Center (Km)
Amazonas	6	1.079
Caqueta	15	386
Guajira	1	775
Guaviare	4	281
Sucre	1	597
Vichada	4	534

Table 1: Country regions involved.

After 19 months of service, the system processed 4.751 actual telemedicine cases from 31 remote stations, fulfilling security issues such as data encryption and digital signing of the diagnosis. This successful project stared with a single station in December 2006 and completed 4 in September 2007. Since January 2008 the telemedicine project was extended to 26 additional nodes for a total of 31 points.

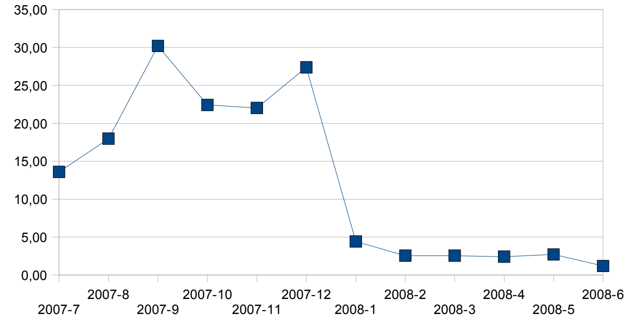

Figure 7: Response time in hours

Since December of 2006 to June of 2008, the average response time is 1,3 days. Response time varies per speciality because each is attended with different frequency due to the schedule of specialists.

Since January 2008, the system allows tracking the arrival of cases and how long they have been waiting for an answer. This has enabled response time improves. Figure 7 shows the response time over time, in the last year. A remission to a specialist consultation could take many days, even weeks, taking in account not only the delay inherent to a citation but the time of displacement of patients; a telemedicine consultation doesn't take more than a few hours.

The integrity of the handled data was maintained through the time span, and no data loss in the transmission process was observed in this period. The system cases accounted for a total of 10.494 images and attached files (3.636 for dermatology, 6.615 for radiology and 243 for others), with an average size of 0,534MB for each file, an average size of 1,181MB for each case, and a total space occupation of 5.613,0716MB.

Access to the system through Internet allows specialists and users to display and send telemedicine cases and diagnoses from remote locations, requiring only a computer and an Internet connection of a proper bandwidth, to be able to access and upload the images of each case in a reasonable frame of time.

Specialists are very satisfied with the facilities that the system offers, because they can access to the clinical information from anywhere at any moment, and they can give their diagnosis from their own PC at home or particular office. Remote users also feel comfortable because they can recover easily sent files and answers by making a single query.

The telemedicine platform has reduced the error rate of diagnosis given in remote stations. This rate is measured using the correlation between the diagnosis given by the specialist and the general physician. The 62.7% of the answers has a negative correlation which means that in the most of the cases, the specialist diagnosis has been really useful to improve patients health care.

In the ZKP mechanism, the algorithm execution takes 70 milliseconds approximately. After several repetitions, a valid device is always recognized. The digital signature preparation (that is, the capture of memory file) takes about 10 seconds. Compared to flash memory, EEPROM is a slow memory, but 10 seconds is an acceptable time for this kind of application.

New telecare module fulfill expectations, by reducing the used bandwidth from 200 Kbps to 7 Kbps without lose signs quality and giving a new way to help patients in remote places.

5. DISCUSSION

This telemedicine system is very flexible and adaptable because of the RIM data model adaption, and the software architecture used. Flexibility has allowed the addition of new specialities with no changes in the model, and the implementation of new functionalities such as the ZKP mechanism and the real time telecare.

Another contribution of this work is the efficient design, implementation and validation of a Zero Knowledge Proof algorithm in a 8-bit ALU microcontroller, achieving excellent performance at a low price. The proposed device offers a high security level and is also suitable for security applications. Compared to other mechanisms such as a digital certificate in a common USB memory device, the developed hardware is better because it's dedicated to provide security in the authentication process and is immune to virus.

The project has allowed that an interdisciplinary team develop a system that covers topics like security, scalability, datawarehousing and that has permitted that the community benefits of all these when attending patient cases from far away regions, making videoconferences, attending and exploring the use of cases of not very common specialities, providing an administrative statistic tool to make system tracking and keep the quality of the service, and teaching students of some specialities with the telemedicine cases.

Two key aspects for the successful development of the system are the use of a version control system, which allowed the developers to add new functionalities and to handle source code changes in a consistent manner; and the data model used, which complies to the HL7 Reference Information Model Specification, providing flexibility and scalability to the system. The system has shown itself to be scalable; many of the existent functionality has been added incrementally, with minor adaptation efforts.

From the software perspective, a new telemedicine node is now very easy to deploy, because with a standard PC with a web browser and standard ports for connecting digital camera and digitalizer is enough. This is a very important advantage in a country like Colombia where access to some regions may be very difficult to the support engineers, even though it's required a moderately good internet connection to avoid a long waiting while the case with the attached files is sent.

Telecare module gives a new way to take specialized medical services to remote and difficult access places in real time and avoiding the cost and problems of doctors and equipment displacements. Real time telecare module was designed to work in zones where Internet connections have small bandwidth and resources must be reserved to others applications such as the videoconference system, but always ensuring a high quality of patient data

6. REFERENCES

[1] Health level 7. `http://www.hl7.org/`.

[2] A. Alaouia, J. Collmanna, D. Nguyenb, D. Lindischa, R. N. Subbiaha, A. Greena, and S. K. M. Jeffrey Johnsona. Implementing a secure teleradiology system using the internet. *International Congress Series*, 1256:803–808, 2003.

[3] K. Beck. *Extreme Programming Explained*. 2000.

[4] M. Brett. Speed up your rmi transactions with value objects. `http://www.ibm.com/developerworks/java/library/j-ejb0910.html`, IBM 2002.

[5] E. Bruno. *Java Messaging*. Charles River Media, 1 edition, Nov. 2005.

[6] K. Jahn, M. Reiher, and T. Stuhl. Telemedical projects in bavaria - what is the current position and what needs to be done? *International Congress Series*, 1281:180–185, 2005.

[7] S. J. Lee and M. H. Kim. Komips: A web-based medical image processing system for telemedicine applications. In *School of Computer Science & Engineering, Konkuk University*, 2002.

[8] C. Mark. Service-oriented architecture expands the vision of web services. `http://www.ibm.com/developerworks/library/ws-soaintro.html`, IBM, 2004.

[9] E. A. Miller. Solving the disjuncture between research and practice: Telehealth trends in the 21st century. *Health Policy*, 82, Issue 2, July 2007,:133–141, 2007.

[10] C. V. O'Connor. Zero-knowledge-proof, prueba de conocimiento cero. `http://www.dattatec.com/descargas/zero-knowledge-proof.pdf`, NEX IT Specialist online magazine.

[11] C. H. P. Caballero. Protocolos criptogrï¿½ficos. `http://webpages.ull.es/users/cryptull/English/Protocols.pdf`, Universidad de Laguna, Espaï¿½a.

[12] C. Sánchez, A. Rueda, and E. Romero. A granular prototype for telemedicine based on hl7 information model. *Segundo Congreso Colombiano de Computación. Universidad Javeriana*, Abril 2007.