

# A New Approach for a Healthcare Network Architecture and Security

MIHAI SCUTARU, RADU ȚOEV, MIHAI ROMANCA, MARIAN ALEXANDRU

Department of Electronics and Computers

Transilvania University of Braşov

29 Eroilor Blvd., ROMANIA

scutaru.mihai@gmail.com, radutoev@gmail.com, romanca@unitbv.ro, alexandrum@vega.unitbv.ro

**Abstract:** - The paper presents an original approach for organizing a network that allows hospital actors to manage and have access to databases remotely and in a secure manner. The architecture, based on the concepts of SONA (Service Oriented Network Architecture) is designed taken into consideration some important characteristics: scalability, integration with other existing hospital networks, remote and secure resource access, user friendliness, and complete data security. This was achieved using two main approaches. The first one was concerned with internal security, being implemented through user permissions and smartcard token based authentication. The second approach was concerned with attacks originated outside the network. In order to prevent system penetrations or data interception VPN tunnels and traffic filters were configured at the edge of each structural component.

**Key-Words:** Hospital network security, smartcard, Hospital information systems, System architecture

## 1 Introduction

Due to the fact that medical institutions all over the world are implementing computer networks and hospital information system (HIS) technology, the need for data security and secure access to centralized and standard databases has become increasingly high. Also, nowadays, Internet technology can facilitate the remote access and the distribution of medical data to the medical community. This fact, combined with the continuous development of software and hardware devices, now provides the means of managing and controlling these databases, therefore increasing the efficiency of companies and institutions. The use of ICT in medical institutions offers great potential for improving the quality of provided services, and also reduces organizational expenses.

In the past years more and more healthcare institutions have adopted HIS integrated information systems to manage all the administrative, financial and clinical documents of a hospital. This trend began when the need for efficient resource management, high availability and security of information had become critical. These types of systems have been implemented with success in various medical institutions, but the health system has yet to adopt a standard solution, a lot of different medical information systems being used, from different vendors, and usually with incompatible structures. The need for centralized and compatible resources is imperative because of factors such as slow retrieval or loss of critical information, illegible documentation by clinicians, too much time spent on tedious menial tasks like searching through hospital records etc.

Such a system can enable: national sharing of information, improve patient doctor relationship, care provision and offer time, cost savings and convenience. The sharing of information between hospitals, clinics and private practices facilitates better treatment administration, thus improving patient care. This improvement is also based on access to comprehensive, up-to-date, accurate clinical data and through efficient collaboration between specialists, critical decisions faster for the benefit of the patient. Another important factor is the economical aspect, and by having an accurate patient medical history, expenses can be reduced. For example, this can be achieved by not having to repeat certain tests of which records have been lost and thus reducing the utilization of hospital resources.

This paper presents an original approach for organizing a network that allows hospital actors to manage and have access to databases remotely and in a secure manner.

In [1], the author proposes a three layer client-server architecture to be used in a HIS implementation for a Radiology Information System. The server resolves the problems of authentication, authorization, data security, privacy of access and protection. The author proposes as authentication method the use of a Secure Sockets Layer (SSL) Protocol, based on TCP/IP.

The paper [3] suggests the application of PKI (public-key cryptography infrastructure) and certificates to verify the authenticity of mobile users in the context of e-business and e-health information transactions.

The paper [4] discusses the main consideration for integration of data, functions and workflow, among

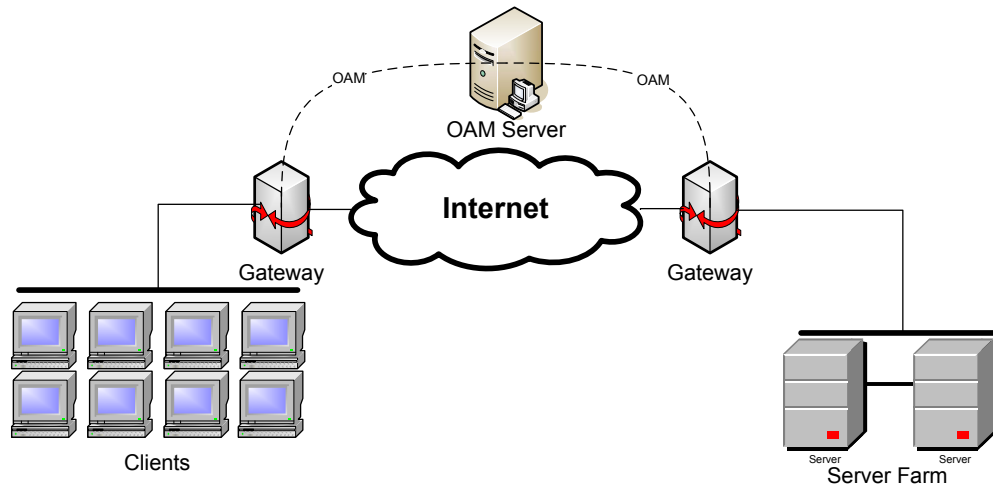


Fig.1 Network Architecture Concept (OAM = Operation, Administration and Management)

different and heterogeneous medical information systems in order to establish an enterprise hospital information system, and propose an architecture design system using digital neural network system in hospital, implemented at a Chinese hospital. No aspects regarding the secure access and security of data are introduced.

## 2 Architecture and Components

In response to the above mentioned healthcare system's needs we propose a complete central resource distribution system, aiming to be implemented at a national level. This system ensures secure communications, remote resource access and personnel management.

As a proof of concept the architecture (Fig. 1) is designed in such a way that it can be easily integrated in any existing infrastructure and its scalability characteristics being heavily taken into consideration.

This architecture is based on the concepts of SONA (Service Oriented Network Architecture), [6], therefore being divided in three major structural components: Client level, Infrastructure level and Server farm level. SONA is Cisco's architectural approach to designing advanced network capabilities into an infrastructure.

Every structural component has a specific purpose and topology, the communication between them being done through standardized logical interfaces. The client component has a campus network topology, accommodating a large access network, each of the end terminals having specialized software running. Through the graphical user interface of this software, access to medical resources is granted based on user permissions. The resources are located at the server site. This structural component has a server farm topology and contains a Domain Controller that manages users and a

database server that holds the actual resources. The client and server sites are interconnected through the Infrastructure component that consists of gateways that aggregate outbound traffic from all the sites. This component ensures data security of the traffic passing through either public or private networks.

### 2.1 Server

In order to implement the token based authentication system we needed a central authority that could issue access rights and a mechanism that can define the users' hierarchy. Also there was the need of setting up a database to store patient information from which token clients could access or insert data [2].

Considering the above needs, we studied two implementation possibilities, implying different characteristics and approach methods for each one. The first solution was a SUSE Linux Enterprise Server that used Crypto Server for token management, OpenLDAP for user rights and hierarchy, and a MySQL database. The other solution was Windows 2003 Server using Microsoft Active Directory for user management, a proprietary token management system and a SQL database.

Given the fact that Windows is the most common operating system for PCs we chose the Windows Server 2003 approach. Also, because of software incompatibility issues, the Linux solution was not a viable one.

The first step in configuring the server was setting up Active Directory. This solution assures all the management necessities of a corporation in regard to user control from a central repository that can be globally distributed. The structure of the information contained in this system can match any organization's

structure and type. Active Directory offers a central management system for network administration and administrative authority delegation, thus granting access to all resources in the local domain. By defining Organizational Units we delegated control and management of the data according to the medical staff needs.

An important component of the server structure is the Certificate Authority. This entity manages all the digital certificates throughout the domain. These certificates contain a public key and the identity of the owner. A Digital Certificate makes it possible to verify someone's claim that they have the right to use a certain resource, preventing user impersonation, thus providing a complete security solution, assuring the identities of all parties involved in the transactions. The Certificate Authority has the same flexibility as the Domain Controller at assigning certificates to users depending on their rank in the institution, such as Organizational Units.

In order to provide eToken smartcard [5] authentication, a central management system is needed. The implemented solution involves Aladdin's Token Management System 2.0. This system is directly connected to the Domain Controller and the Certificate Authority in order to provision the necessary information onto the eTokens. Our solution needs to provide the user with the possibility to login into the domain using the smartcards and to have loaded on the devices the individual Digital Certificates of the user profile in order to ensure mobility.

A fundamental component of the server is the database. The main purpose of this database is to hold patient information, ranging from personal details, medical history to insurance plans. It was implemented using SQL Server 2005 and was based on the Romanian health system specifications. It can be viewed as a repository of patient charts containing highly detailed information on topics such as patient evolution, diagnostics or surgical procedures. One must take into consideration the fact that this is a central database handling high amounts of information generated by a large number of health institutions. Therefore its structure was designed to be robust allowing indexing and searching. Furthermore it allows information extraction based on different criteria specified by the user. For example, the medical staff is able to view all the laboratory results of a patient in a desired timeframe. This type of structure also eases the process of statistical analysis of illness' incidences, researchers having the possibility to access very large volumes of patient information in a structured manner.

## 2.2 Client

The user's interaction with the authentication system is represented by an eToken smartcard. By using this solution we ensure the transparency of the security methods and user mobility, thus enabling a doctor to access a certain patient chart from any end-terminal in the network.

The user's authentication in the system is done by entering the smartcard's PIN. Based on the rights of the user's Organizational Unit the interaction with the database is limited by the rank of the user in the institution. Relative to the medical specific legislation we defined several groups of users: administration personnel, head of department, doctors and nurses. Of course, we can imagine new groups to be added, depending on the healthcare system structure. Each of these groups are limited to their own department and based on their rank, they can either edit or visualize the information from the database.

At the client side it's imperative to ensure an intuitive graphical user interface, regardless of the technology used, in order for the medical staff to be able to quickly comprehend all the possibilities that the application provides. Therefore, for the front-end of the application, we have taken into consideration technologies like .NET framework with C# features, the JAVA swing library and PHP combined with Flash. All of them have strong graphical capabilities, but we opted for C# because it is developed by the same company that developed Active Directory and the incompatibility chances are small.

The interface between the user and server starts after the successful login. According to figure 2, there are several options for the client to use, tailored for his permissions and rights in the domain. For example, the administrative personnel can assign and view shifts, nurses can view what treatment should be administered and doctors can view a patient history, prescribe treatment and edit patient details.

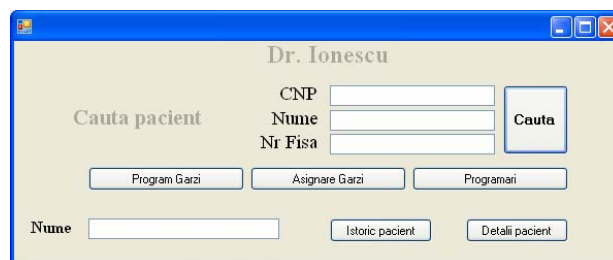


Fig.2 Client GUI main menu

One of the most important aspects of the application is the search engine, designed to index the database in order to quickly gain access to the patient charts. The

search mechanism allows users to retrieve data based on different criteria. We chose the patients' ID, name and chart number as the possible search options. All of these can be used together or individually. The advantage of this technique is that if the doctor is familiar with the patient, he can retrieve exactly the data that s/he is looking for. Another option of the search engine is the possibility to control which time period of the patients' medical history is displayed. Each record in the database has a corresponding date allowing the system to retrieve only part of the entire medical history. The user has the option to choose between the past six months, the last year, past 5 years and the entire life. This offers a high granularity in regards to data manipulation on the user part.

The search result is displayed in the form of the patient name, the user being able to choose between viewing the patient's details or medical history. The patient details window, as seen in figure 3, corresponds to information found on the first page of the standardized medical chart. This information includes demographic data about the patient such as name, address and citizenship. General medical history records are also displayed: blood type, RH, allergies, and, for newborns or young children, the weight at birth and Apgar score. This allows medical staff to quickly identify each patient.

The form contains the following fields:

ID Intern	Grupa sanguina
CNP	RH
Prenume	Alergii
Nume	Greutate la nastere
Sex	Apgar
Data nasterii	Cetatenie
Adresa	Pasaport
Strada	Certificat de nastere
Numar	Data adaugarii
Apartament	Ultima editare
Oras	Ultima internare
Judet	Nr telefon
Tara	Nr Telefon mobil
Urban/Rural	E-mail

Close

Fig. 3 Patient details window

The core of the application is the patient history form (figure 4). It is divided in two panels. The first one displays all the medical visits in the previously selected time frame. In order to differentiate between visits, each one has an ID and the year when it was created. Each visit corresponds to one of the patient's charts. All the information is displayed in the secondary panel. In order

to organize the information, we have structured it in a tabbed manner. By clicking the desired button on the top of the panel, the user is able to control what information is displayed. Each of these buttons corresponds to a portion of the patient's standardized chart. One of our goals in the implementation of the software is to maintain a familiar view of the information, thus easing the transition to the digitized system, for the medical staff. Most of them have been using paper charts with a standardized format for many years. Using a different data organization format would make it very difficult for the digitized system to be largely accepted. For example, the information from the first pages of the standardized chart is presented in figure 4, representing the "Visit Details" tab.

The form is titled 'pacient\_history' and has a tabbed interface. The 'Vizite' tab is active, showing a list of visits on the left and a detailed form on the right. The list of visits includes columns for ID, Year, and a description. The detailed form on the right includes fields for:

- Stare internare, Tipuri internare, Examinari, Asigurare
- Transferuri, Foarte Diagnostic si Tratament, Foarte Evolutie si Tratament, Tip Externare
- Stare Externare, Diagnostic, Interventi Chirurgicale, Info Deces, Detalii Vizita
- Data internarii, Medic Sef Sectie
- Data externarii, Medic Curant
- Nr zile concediu medical dat, Trimis de
- Data adaugarii vizitei, ID Stare externare
- Intocmit de, ID Tip Externare
- Medic de garda, Cod morfologic
- Motivale Internarii
- Antecedente heredo-colaterale
- Antecedente personale patologice
- Conditii de viata si munca
- Comportament

Fig. 4 Patient history window

As depicted, at the top of the form, the user can view administrative information such as the date of admission, the staff attending the patient and identifiers like the discharge status code. Following the administrative information, the first fields present the motive of the admission, family history and complete medical history. The last field is inherited from the standardized health system chart. This field complements the transition to digital format, which means that during the early stages of this system's use, 90% will already have had a certain medical history that is yet to be digitized. In the next two fields, one can view life and work conditions, and behavior of the patient. The last two fields are the most important, containing the administered medication and the history of the present illness.

The client can also insert data into the system. The database will update its contents almost instantaneously, thus enabling the possibility to access this information quickly by other users. For example, other experts from different hospitals could assist a doctor treating a rare condition as soon as s/he uploads the patient's information.

Based on the user permissions issued by the Domain Controller (Active Directory), the user can edit the current chart of the patient in treatment. In order to have full control over the permissions, the system must be aware of the shifts and the on-call doctors. To ensure the system's flexibility, the administrative personnel have the possibility to input the entire schedule of the hospital in a separate database. In conjunction with this database, the Domain Controller assigns the necessary permissions to each member of the hospital staff. This is done in order to increase security in the system and to maximize the efficiency of human resources' administration.

One of the most important features is the users' ability to collaborate on the same patient's chart. In the vast majority of cases the treatment process requires multiple examinations from different medical specialties. In order to ensure this possibility, every department has the right to edit only the fields regarding its specialty. This is done by direct interaction with the Domain Controller. Active Directory has the possibility to group users in Organizational Units (OU). By assigning all the users to their respective OUs and in conjunction with the hospital schedule, the system guarantees parallel input from all the staff attending the patient, without the possibility of overwriting each others' data. For example, the surgery department can input only information regarding the surgical procedure performed on the patient, while the laboratory staff can only insert test results, with the possibility of all of these being done simultaneously.

In order to enhance its functionality, the client offers the user the possibility to view his on-call schedule and his patients' appointments. This additionally improves user experience, by taking advantage of an all-in-one platform, which offers users all information regarding their work.

### 2.3 Securing the connection

Through the use of the Domain Controller, we ensured data security among the system's users. But in order to implement a completely secure solution, the connection between the client and the server must also have strict enforcement rules and policies.

As our system architecture suggests, the infrastructure has two gateways, which apply packet-filtering techniques on data sending or receiving from

the client side to the server-farm side and vice-versa, as well as the logical path between sites. In most cases, the connection between the different sites is created through a public network, such as the Internet. There is also the possibility of deploying a private communication backbone, exponentially raising the costs of the system, but offering full control of the data flow. The architecture was designed to use inter-site communication over the Internet.

The central component of this solution is the use of encrypted tunnels. This is done by implementing Virtual Private Networks (VPNs) between gateways. By communication through VPNs, we can ensure that data passes in an encrypted way through the public data network. VPN technology deploys its own Certificate Authority on the VPN server. This server is located on the same site as the Domain Controller and databases, which is the server farm. By using digital certificates issued by this authority, we can ensure which gateways can participate in the VPN community. This method completely eliminates the risk of man-in-the-middle attacks. These attacks consist of a rogue gateway trying to gain access to the VPN community, thus intercepting data traffic between the logical sites. By using strong traffic encryption, we can ensure that even if the data is intercepted, it cannot be deciphered.

Besides creating the VPN tunnels, the gateways filter the traffic, protecting sites from external attacks. The filtering policies are based on each institution's needs, being highly adaptable, thus providing security for any other applications used in hospitals.

For the infrastructure we implemented two solutions, one being proprietary, and the other open-source. The proprietary solution involves the use of Checkpoint software and equipment. It has the advantage of being the best enforcement option available for enterprise environments. This infrastructure has a three tier architecture consisting of the enforcement part using Checkpoint VPN-1, the firewall management server using SmartCenter, and the administration tier using the SmartConsole software suite. The main advantages are the centralized management system, via SmartCenter, and a highly optimized enforcement engine, while the main disadvantage is cost-related.

Similar results can be obtained using the open-source solution, deploying Linux machines running openVPN for the encrypted tunnels and IP tables for the filtering decisions. The main advantage of using this solution is the low cost hardware and free software. Using the open-source solution has the disadvantages of reduced performance compared to a Checkpoint system and limited central management mechanisms.

Any of the two solutions are widely used, according to each environment's needs, achieving traffic encryption and secure data transfers.

### 3 Conclusions

Throughout the development of the architecture several factors have been taken into consideration, such as scalability, the possibility of integration with other existing networks, remote and secure resource access and user friendliness.

Scalability is necessary in order for the system to adapt to any health institutions, ranging from county hospitals to private practices. As the system begins to be widely adopted, the growing amount of data has to remain available without any downtime on the server site. This is achieved through load balancing and clustering techniques that enable redundancy.

Because of the convergence between data networks it is highly important that any new architecture can be integrated in existing structures. Given the fact that the architecture is modular, integration is possible without modifying the implemented communication mechanisms.

Another fulfilled objective is complete data security. This was achieved using two main approaches. The first one was concerned with internal security, being implemented through user permissions and token based authentication. The second approach was concerned with attacks originated outside the network. In order to prevent system penetrations or data interception VPN tunnels and traffic filters were configured at the edge of each structural component.

Probably the most important element of our architecture was the client application. This is the interface between the medical staff and the database servers. The application design has taken into consideration the fact that the target audience has no technical background, making user friendliness a key factor in the wide acceptance of the solution. The foundation of the graphical user interface was the standardized patient charts, widely used throughout the health system. This offers a high degree of familiarity to the medical staff that is already trained to use them. As the core of the application, we implemented a structured perspective of a large amount of patient charts, creating the possibility to store the entire medical history of a patient and to access it according to each user's needs. By adding the adjacent functionalities we migrated the application to an all-in-one platform that tends to the administrative needs in the form of generating, distributing and viewing the hospital's schedule. Also

deriving from the lack of a technical background of the end users, all the implemented security mechanisms must be as transparent as possible. Therefore we replaced the usual username and password based authentication method with eToken smartcard based system. These devices hold the users' credentials and provide a more natural login system. This is the only interaction that the user has with the underlying security mechanisms of the system, as the encryption and traffic filtering are done transparently.

Another essential advantage of the usage of a system like the one we propose comes from the ease with which statistical analysis might be conducted. Conducting effective statistical research can lead to improved performance of medical institutions, and by comparing different treatments administered to the same illness can lead to overall better patient care.

In conclusion, we can state that this architecture is a suitable replacement for the current health system's data acquisition, storage and manipulation. Its implementation could represent the cornerstone towards a better healthcare environment.

#### References:

- [1] Cordos, A., Studii și cercetări privind managementul, prelucrarea și transmisia, informațiilor cu aplicații în domeniul medical, *Doctoral thesis, Technical University of Cluj-Napoca*, 2008
- [2] Rankl, W., Effing, W., Smart Card Handbook, *Third Edition, Wiley*, 2003
- [3] Tan, J., Wen, H., Gyires, T., M-commerce security: The impact of wireless application protocol (WAP) security services on e-business and e-health solutions, *International Journal of M-Commerce*, 1(4), 2003
- [4] Xudong, L., Huilong D., Haomin L., Chenhui Z., Jiye, A., The Architecture of Enterprise Hospital Information System, *Engineering in Medicine and Biology Society*, 2005, pp. 6957-6960
- [5] <http://www.aladdin.com/etoken/devices/pro-usb.aspx>
- [6] <http://www.cisco.com/en/US/solutions>, white paper: Cisco Unified Communications and Service-Oriented Network Architecture