INTERNET-ORIENTATED MEDICAL INFORMATION SYSTEM FOR DICOM-DATA TRANFER, VISUALIZATION AND REVISION[1]

Sergey Khludov, Lutz Vorwerk, Christoph Meinel
email:hludov@ti.fhg.de, vorwerk@ti.fhg.de, meinel@ti.fhg.de
Institute of Telematics, Bahnhofstrasse 30-321, D-54292 Trier, Germany

Abstract

Modern high-quality medicine is inconceivable without computer and communication technology since the late 80 `s. The physician can manage this enormous stream of data (espiacially images) only by using computerized information systems. That's why telemedicine applications are widely accepted in radiology. The high Standard for patients health care can not be maintained without the introduction of modern RIS and PACs.

The Institut für Telematik / Trier introduces by this paper a new, intranet / internet orientated radiological information system for transmission, visualization and processing of medical images, which can be used in hospitals and in settled doctor's offices.

1. Introduction

Internet-/Intranet-based applications open a wide range of opportunities for communication and data visualization. Many exemplary applications in the WWW have shown that user-friendly and efficient communication systems can be built easily and without a greater expenditure [1-3].

In this context this paper introduces a JAVA-based, Internet-orientated system for DICOM data transfer, visualization and revision. By means of the System a physician, provided that authentication of the user was successful, can get all important data (inclusive all the radiological images) of a patient from the hospitals DICOM-modalities or the archive via internet, no matter where the hospital is placed. Another possibility to employ the system is to establish real-time consultations with physicians of different hospitals for evaluating the patient status using the transferred results of radiological examinations.

2. The DICOM Standard

DICOM is the abbreviation for digital imgaging and comunication in medicine and defines protocols and mechanisms to manage and transfer medical data. The combination of patient Data and Image data which conform to the DICOM standard is called a DICOM image. There ore other elements of the DICOM standard like worklists or reports not mentioned here because these elements are not relevant for this paper, yet. The DICOM protocol is intendet to negotiate the features of the DICOM standard supported by two DICOM applications which want to communicate. The subset of DICOM features supported by both applications if there is one - a default set is defined, but often ignoreddecides if a communication is possible.

[1] Internet-Orientated Medical Information System for DICOM-Data Transfer,
Visualization and Revision , Proc. *CBMS 2000,* Houston (Texas, USA), 2000, 293-296.

3. Representation of the system

The system was developed at the institute of telematics and was constructed in using standard network protocols and the DICOM-protocol. The components of the system were written in the platform independent programming language Java. The software (i.e. the web server) consisting of this components is installed an one computer. Because the system bases an existing, open standards, there are these advantages, which define the system

easy to operate:	ensures fast lerning an how to operate the program
simplified strukture:	ensures low costs for Installation and maintenance
high speed transmission:	ensures fast transmission of large images
high security:	protects data from unauthorized access or manipulation
high stability:	ensures stable running of the system

The Image viewer of the system offers every function neccessary for viewing and processing in the viewer in doctors every day work (contrasting, enlarge, invert, write comment a.s.o.).
New procedures for lossless compression, developed at the Institut für Telematik, ensures fast transmissions even for large, high resolution graphics without risking to reduce the image's quality. This new developed adaptive algorithm of compression suits these needs especially well, because the compression algorithm bases an standardized procedures implemented in internet browsers.

System consists of.three components: imaging DICOM modalities, the web server installed an computer 1 and an internet browser installed an computer 2.

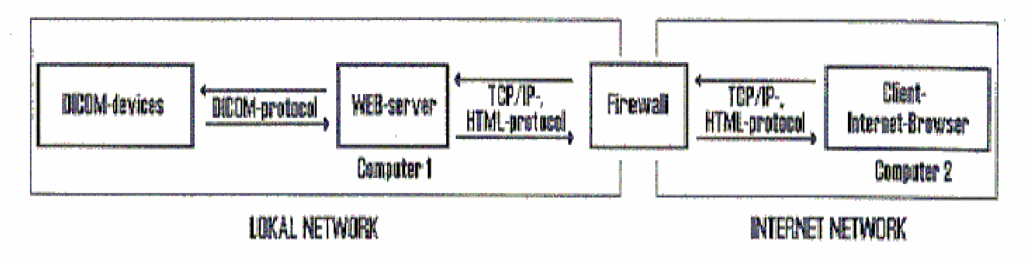

Figure 1: The structure of system

The DICOM data is located an the **computer of the DICOM modality** and is managed by the DICOM Server. On computer 1 a web server, a user database and the servlet-, applet classes and HTML-pages are installed. On client (computer 2) an internet browser is installed. The viewer software will be operated by the server side, so the doctor's client computer just needs an internet browser to be fully operational.

In figure 2 the process of data exchange between the components of the system is shown. The user gets the Internet address (URL) of the system installed in a medical institution by clicking an it. This action causes the transfer of a first HTML-page, which contains applet 1. The user is instructed to identify himself or herself as an authorized user in typing a password and the keys which are used to encrypt DICOM data. Applet 1 encrypt the password and send it to the web browser (computer 1). Servlet 1 (computer 1) decrypts and verifies the password. In the case of authentication failure a new applet (applet 2) is started which manages the encryption of data by which the user is identified.

After verifying of this data a password and the keys for encryption of patient data will be chosen by the user. The password, the keys and the data necessary to identify the user will be stored by servlet 2 in a user-database (computer 1).

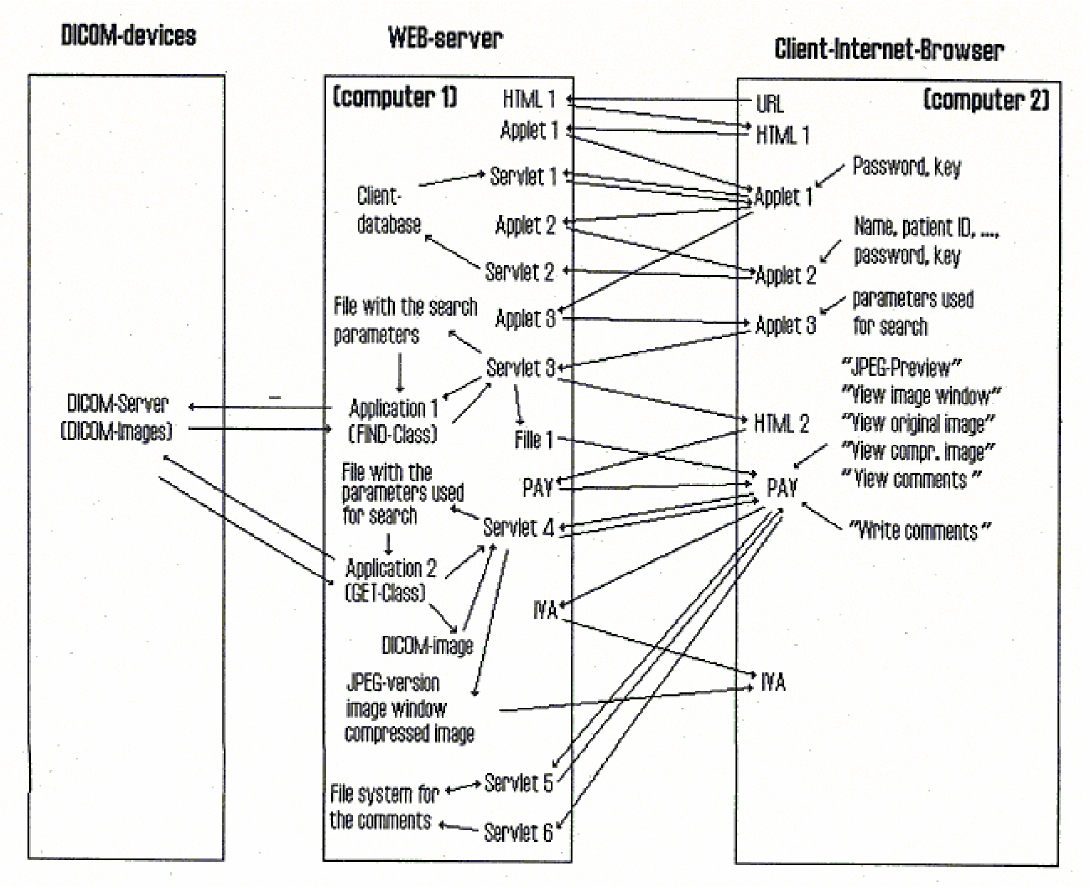

Figure 2: Process of data exchange between components of system

After successful authentication applet 3 is called by applet 1 in order to deternvne and afterwards encrypt the parameters of a search for particular DICOM-images. Servlet 3 is started by applet 3. Afterwards applet 3 sends the encrypted parameters to servlet 3. Servlet 3 decrypts the parameters, creates the file with search parameters and starts the client represented as a Java-application, that implements the DICOM-FIND-Service class. Application 1 transfers the file with search parameters to a DICOM-modality and receives the file that contains the result. Afterwards servlet 3 encrypts the file 1, stores the decrypted data in file 1 and creates a HTML-page. This page enables to start the patientlist-viewer-applet (PAV). The PAV reads file 1, decrypts the stored data and displays it by using the internet browser of the client (computer 2).

In every kind of representation of the images (i.e. ordering an original image, parts of an image, or an iconified image) in the system, the parameters used for the search are encrypted by the PAV and transferred to the web server. Afterwards the servlet will be started. Servlet 4 decrypts the parameters used for search and starts the client application 2 written in Java, that implements the DICOM-GET-Service class. Application 2 transfers the file which contains the parameters for search to the DICOM-modality by using the DICOM-protocol and receives the DICOM-image found. Afterwards, a scaled and compressed version of the DICOM-Image or a part of it is created by servlet 4. Finally, the Image-viewer-application (IVA) is started by the PAV by using servlet 4. The IVAapplet reads the original image (or a part of an image or a compressed image [4]), loads and shows it by using the Internet browser of the user (computer 2). For a selected image the user can read comments made for an image. To do this, the user starts servlet 5, that reads an computer 1 the file containing the comments for the chosen image. The comments will be encrypted and transferred to the PAV an computer z. The comments will be decrypted by the PAV and will be displayed in a window used for conunents. The PAV poses a digital form in which the user can write assignments for the cömrnents.

Afterwards, the PAV encrypts the comment together with the Image and starts servlet 6 on the web-browser. Servlet 6 decrypts the encrypted assignments and stores them in a file that contains the selected image and the comments which belongs to it.

4. Security concept

The security concept is based an authentication of the user and an encryption of the patient's data. Authentication and encryption is based an certification mechanisms as well as an dynamic, adaptive and fully automatic Java-cryptography, which won't allow outsiders to access the personal password and key of the authorized user.

An asymmetric encryption algorithm (RSA) is implemented to encrypt the user's data. The public key will be generated by the server and sent separately from the applet to the user's browser after the user's request and the successfully vetting of the requesting user. The Internet-user chooses his own password for authentication as well as a personal key for encryption of the patient's data. He may change both of them, the key as well as the password, whenever and as often as he wants. Whenever the user changes one or both of these secrets, a new pair of keys (56 Bit key length) will be generated. Password and key, as well as the personal data of the user, will be stored in an user database an the web server. Administration employees have a read-only access to the personal information of the user only; password and key are accessible (and changeable) by the authorized user only. In the ideal case the check of the user's personal data should be made automatically, if the user uses certified software; a manually performed check is also possible.

References

[1] S. Hludov, C. Meinel, F. Warda, G. Noelle. PACS for Teleradiology. 12 th IEEE Symposium an ComputerBased Medical System. Stamford, Connecticut. June, 1999, S.641.

[2] L. Vorwerk, S. Khludov, C. Meinel. Concept for Increased Security for Internet/Intranet - Based Administration of Patient Data [R61]. 8-th International Conference an Computer Graphics, Visualization and lnteractive Digital Media'2000. Plzen, Czech Republic. February, 2000.

[3] L. Vorwerk, F. Losemann, T. Engel, C. Meinel. Constructing a secure HIPACS with structured reporting [3980-46]. Medical Imaging 2000. San Diego, California. February, 2000.

[4] S. Hludov, C. Meinel. DICOM-Image Compression. 12 th IEEE Symposium an Computer-Based Medical System. Stamford, Connecticut. June, 1999, S 282-287.