Project title: HCLOUD – A Cloud Architecture for Healthcare

1. Project Scope and Objectives. Usability Features

Managing huge amount of clinical data and the massive capital required by EHRs for sourcing and maintaining IT infrastructure needed to store, transfer, modify or print data and reports transfer to a national level can be done efficiently and at minimum costs moving data into the Cloud.

Cloud computing paradigm is one of the popular healthcare IT infrastructures for facilitating clinical and administrative designated information systems (ERP, HER, PACS, etc.) data sharing and integration. Collaboration between medical, availability of a physician, a medical specialist, a product or a service at different times and in different cases can be checked at any time from everywhere within cloud computing healthcare infrastructure. Costs of the IT infrastructure is cheaper because the medical units will only rent the infrastructure to store medical data as it is needed and will no longer need the latest equipment for the applications used, managed or maintained (only computers and devices with access to Internet are needed).

Reports show 35% of healthcare organizations are either implementing or operating cloud computing in 2012 having as main concerns in implementing cloud healthcare: security of data/applications (51%), performance of cloud services (36%) and integrating cloud applications/ infrastructure with legacy systems (31%). Currently this cloud technologies are mostly limited to conferencing and collaboration (29%), compute power (26%), office and productivity suites (22%) [1].

Cloud computing technology is still new, but actually research results describe low price and minimum resources architectures and low waiting time values for data access [2].

The *scope of this project* is to propose and describe a solution to fully integrate healthcare clinical and administrative processes within cloud infrastructure based on service oriented architecture using existent information systems, focusing on radiology specialized units. The proposed platform is to be used by several units (hospitals) and entities (third parties) at large scale, geographically distributed over a large area.

It is considered that the deployment model is hybrid cloud for the healthcare environment, composed by several private clouds that are representing each specialized entity (Radiology Private Cloud, Emergency Private Cloud) and a public cloud used to integrate all entities. The purpose of the public cloud that is used for unit integration is to avoid the mesh networks within the private clouds connections.

As described in [2] the communications inside hybrid cloud (public cloud – private cloud) will be held through HL7 CDA messages after the link between the applications will be establish using an application defined in the public cloud. DICOM and HL7 are successfully used to integrate a large numbers of applications from various medical domains [3].

The radiology data will be stored in the radiology private cloud and all adjacent hospitals can access medical patient data when is needed, the connection being established by the public cloud application. From the perspective of a network of entities, defining multiple private clouds for data storage and a single public cloud as central point for external access and management of requests for data, a hybrid cloud architecture is proposed (Fig. 1).

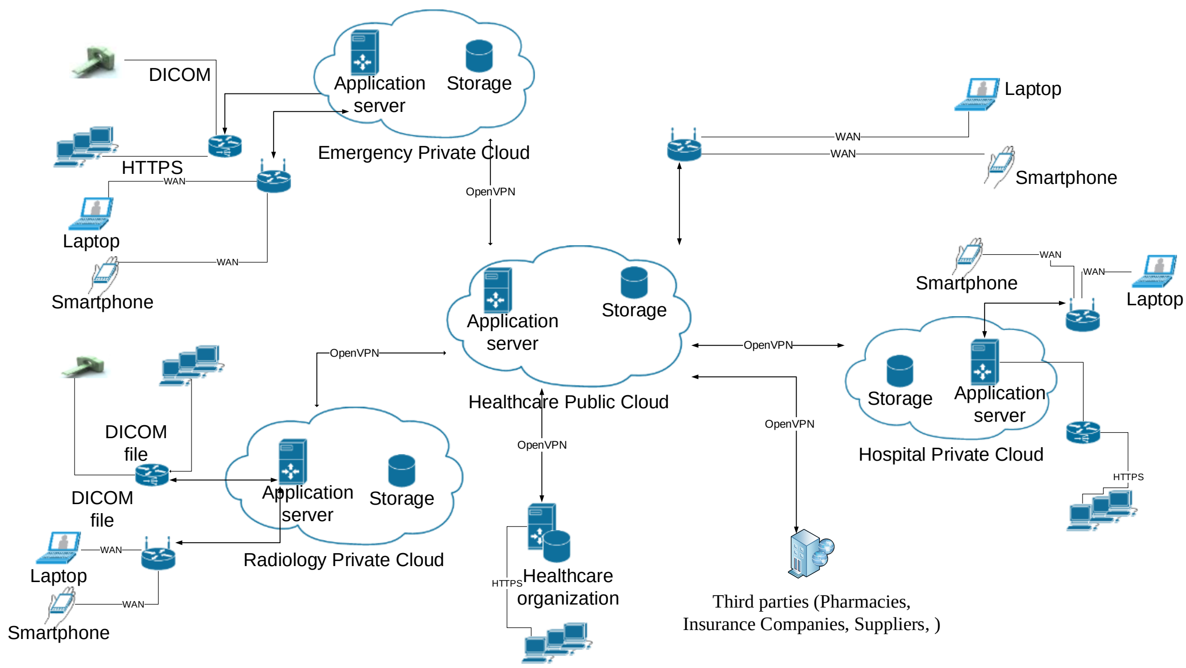

Fig. 1 Healthcare hybrid cloud architecture

The proposed integrated healthcare services using hybrid cloud is presented as IT deployment model that fully optimize healthcare service provisioning. Doctors, physicians, specialists use medical applications in their clinics to capture patient information and transfer them through Internet, using a web-based SaaS application hosted in the hybrid cloud managed by cloud service providers. They are able to access the records securely by exchanging secure electronic keys or third party security devices (tokens).

The integrated healthcare services infrastructure is able to support end-to-end chronic disease monitoring. Remote monitoring of a patient can be done by a physician/ specialized medical staff from the hospital or individual medical offices. The Hospital Private Cloud entity includes services for receiving and analyzing patient's medical data: asthma disease management, diabetes monitoring, hyper-tension disease management, ECG monitoring, etc. Physicians are able to retrieve and update patient health information providing a new prescription, comments with regards to recent examinations, require patient visit to hospital, etc. Patients access the public cloud entity and access updated information and according to physicians comments visit a pharmacy, diagnostic centre or hospital. Third party entities like (pharmacies, insurance companies, etc.) address public cloud according to outstanding orders and medical actions.

Advantages for deploying and maintaining server-side applications: high degree of flexibility implemented by hardware virtualization techniques which enable virtual machines to scale up and down computing and storage resources according to QoS level. Hybrid cloud helps healthcare providers to remove partially in-house server rooms.

From the usability perspective, the key benefits of the healthcare hybrid cloud expressed from the perspective of industry stakeholders are expressed as:

- Physicians – have access to the most recent data that could be updated by the patients from anywhere, at any time, including data uploaded from health devices being able to make informed decisions;
- Patients – have access to updated medical record
- Pharmacies – patients are able to manage their prescriptions and administration information (quantity, frequency, sequence, etc.)
- Hospitals –in-house or offsite SaaS applications deployed on cloud benefit of healthcare processes like admission, patient care, discharge processes simplified due to patient history and information that are available in cloud.

2. Defining the HCLOUD architecture. Description of proposed solution

2.1. Hybrid Healthcare model

According to IHE requirements, the following concepts are defined for a hybrid cloud system model:

- *Domain* is defined as a distinct business area administrated by a healthcare organization such as: hospitals/clinics, pharmacies, insurance companies, research institutions.
- *User* is defined as a entity (person or a service) that acts as consumer for healthcare application and it is registered as a member of at least one domain in order to be able to resolve his identity in a specific role.
- *Object* is defined as the entity that is managed by a healthcare system (patient, medical device, etc.) registered in the system with an uniqueue identifier assigned by the corresponding domain.
- Attribute defines an object as unit of information. For example a patient is defined by a set of attributes like: name, allergies, blood preasure, heart rate, age, etc.
- *Service* is defined as a software entity, under SOA concept, designed to support integration of healthcare services for data gathering, storage, process and exchange. A service is represented by a singe instance that interacts with other applications based on messages.
- *Hosting infrastructure* is represented by cloud computing environment, defined as a hybrid cloud model composed by private cloud for data storage ans public cloud for hosting service instances. Hybrid cloud service provisioning is split into all three cloud available service models: IaaS and PaaS for private cloud entity and SaaS for public cloud.

The hybrid cloud scenario process and information flows are described in Fig. 2. Information systems (ERP, EMR, EHR, RIS, PACS) are migrated to cloud services or integrated with cloud applications. Online patient access to hospital/clinic services to order a medical procedure or to presenting to the hospital where the reception officer will book the medical procedureare feasible . Medical staff (clinician, radiologist, tehnician, reception officer, etc.) access private cloud in order to register/update patient information, register the medical procedure, store examination results and retreive patient data. Medical devices are connected to private cloud in order to retrieve and store procedure details via PACS server.

Clinician receives patient list from ERP (Report) service, examines the patient and if it’s the case, places the medical imaging examination request back to ERP (Order). Radiology orders are placed by ERP service through work list. After technologist performs procedure steps that are described in work list medical imaging are available on medical workstations. Radiologist interprets the studies, adds comments and sends the report (picture + radiology comments – radiological diagnostic) to PACS server hosted in private cloud. PACS server stores the radiology file in private cloud data centre from where it's accessible by all cloud services. Clinician accesses the radiologist comments and is able to provide final diagnostic to the patient.

Private cloud store reports containing general patient data and information about detail patient information, having a bidirectional integration, essential for update patient data. Insurance companies, IT providers, pharmacies, patients and hospital connect to public cloud in order to address required data.

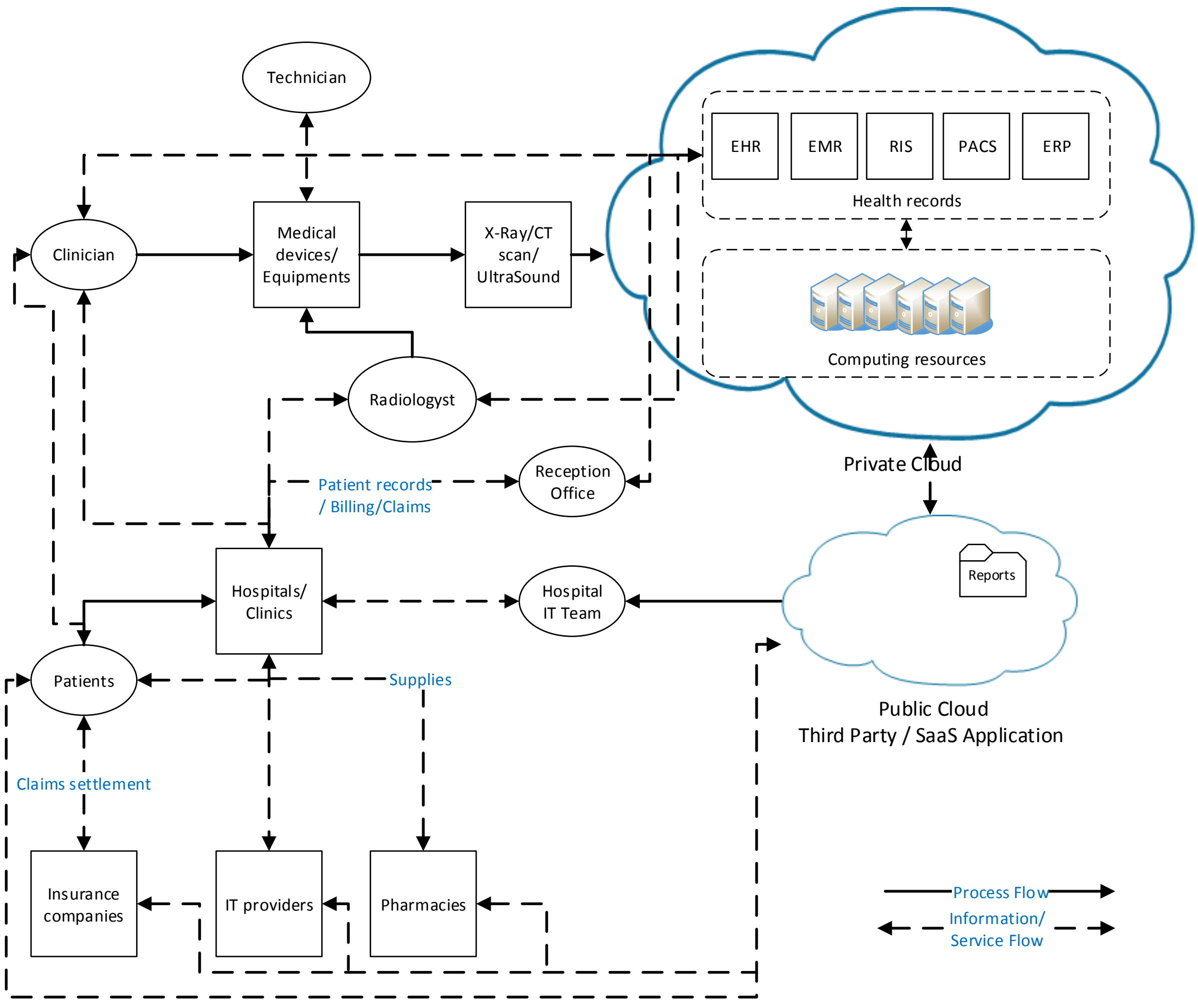

Fig. 2 Hybrid Cloud Integration - elements

An example of cloud scenario for hybrid cloud is given by a patient that has a requirement for a medical investigation placed in the system using healthcare portal or call centre containing only general information. An ERP planning and execution service selects the appropriate physician, lab, hospital and/or pharmacy for the exact requirement. Planning and execution ERP cloud service acts as single point of contact for patient in this case performing the following workflow/operations:

- Patient is registered through Web based portal or by reception office (call centre officer);
- Patient requests for services like appointment to doctor’s visit, health checkup to hospital or diagnostic lab, online order/delivery of prescription and medicine. Based on requested information a service ticket is created (by call centre officer or based on patient action on portal) and placed in the system.
- Service tickets are resolved by selecting appropriate doctors, hospitals, lab, pharmacy based on criterion like same locality, patient's scheduled date. The central planning and execution results are generated and patient is process parties involved are informed.
- Appointments are automatically placed in the system based for the registered doctors, radiologist, hospitals, pharmacy or diagnostic lab for each service tickets. The status of service tickets already allocated can be tracked by agent, patients.
- Medical staff, the doctors, labs, pharmacies and hospitals update the necessary information in Electronic Medical Records (EMR/EHR). Based on provided logon data patient is able to check his/her own EMR from anywhere through internet.
- Doctor makes visit to patients and keeps diagnosis/prescription record in the system. Cloud services forward the diagnosis record to pathologist/radiologist using automatic rules to send these to them without their intervention. This helps pathologist/radiologist to finish the lab test and upload report through healthcare system so that doctor and patient can see that from anywhere.
- Similarly, system sends the prescription to different registered pharmacies so that medicines can be delivered to patient’s house, if it’s the case.
- Emergency cloud services help immediate provision of emergency request for ambulance, blood, hospital emergency admission etc.
- Cloud services implement automatic syncs arranging for patient hospital claims management with provider/payers.

- Hard copy of all patient reports can be generated from cloud and sent to patient if is requested.

In the proposed hybrid cloud, public cloud is used for hosting service instances and act as an index for patient data that is stored in private clouds offering restricted access for patients, medical staff and third party personnel. Private cloud entities integrate legacy systems and offer specialized cloud services dependent on activity domain for example:

- Radiology private cloud: integration with legacy PACS systems, DICOM C-Store service for archive medical images, DICOM C-Find store for queries in cloud archive, DICOM C-Move for image exchange, DICOM anonymize and de-anonymize encryption services, etc.
- Emergency private cloud: special encryption and retrieval of medical data from hybrid cloud, emergency patient admission, etc.
- Hospital private cloud: patient access, diagnostic and treatments, billing, resource planning, supplier relationship management, etc.

Further, an *internal user* is considered a user that has a certain authorization to process (create, query, store) data and is represented mainly by hospital employees. *External users* groups patients, patient's family, third parties employees and all other actors that wants to access healthcare services providing a certain degree of authorization access.

The hybrid cloud access model is presented in Fig. 3 from the perspective of user access at two levels: public and private. An external user is able to connect to cloud services using any device that has internet connection (smartphone, tablet, laptop, etc.) via cloud portal, cloud application for mobile devices. An internal user can connect to cloud infrastructure from internal workstations or any device connected to the internet based on his account.

- Private cloud entities (radiology, emergency, hospital, etc.) provide full access to all internal users according to user group definition.
- Public cloud entities provide restricted access to both internal and external users.
- Private to public cloud communication is regulated based on emergency or non-emergency situations.

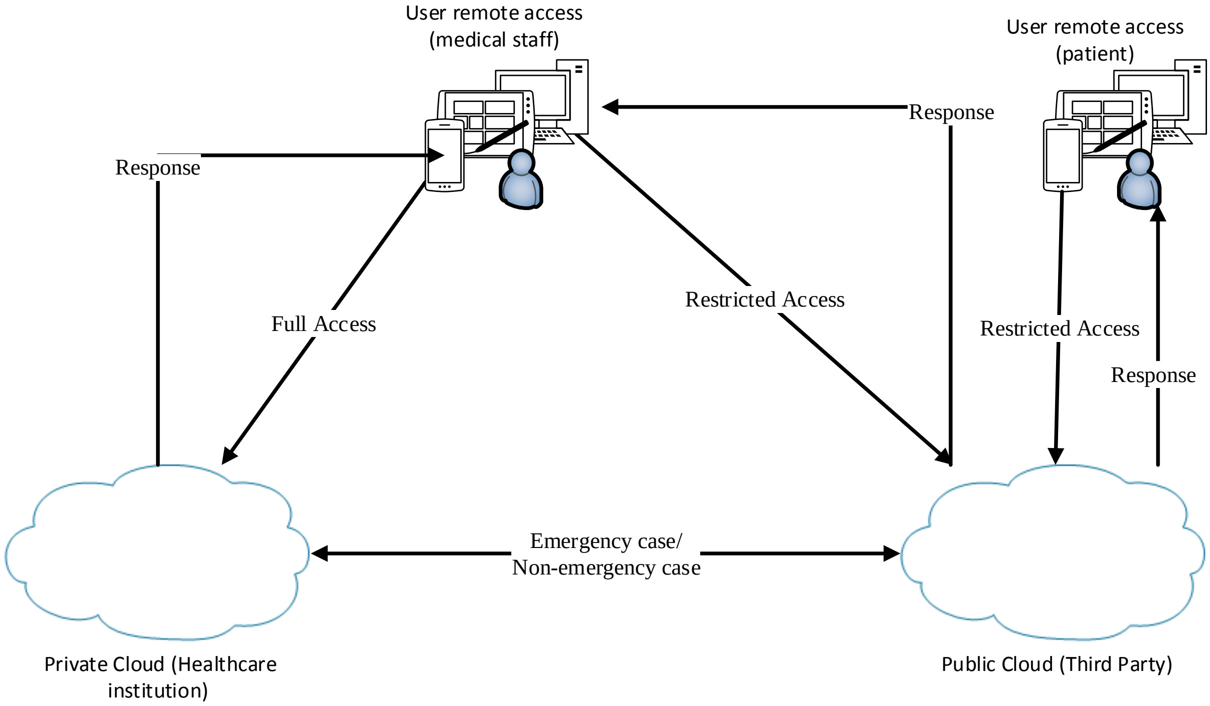

Fig. 3 Data access in hybrid cloud

Due to security and performance reasons, radiology images are accessible in high quality DICOM format from private cloud only to authorized persons using a special infrastructure based on DICOM devices. Third parties involved in medical process (insurance companies, pharmacies, etc.) and patients are able to access images in other formats (for example JPEG) from public cloud.

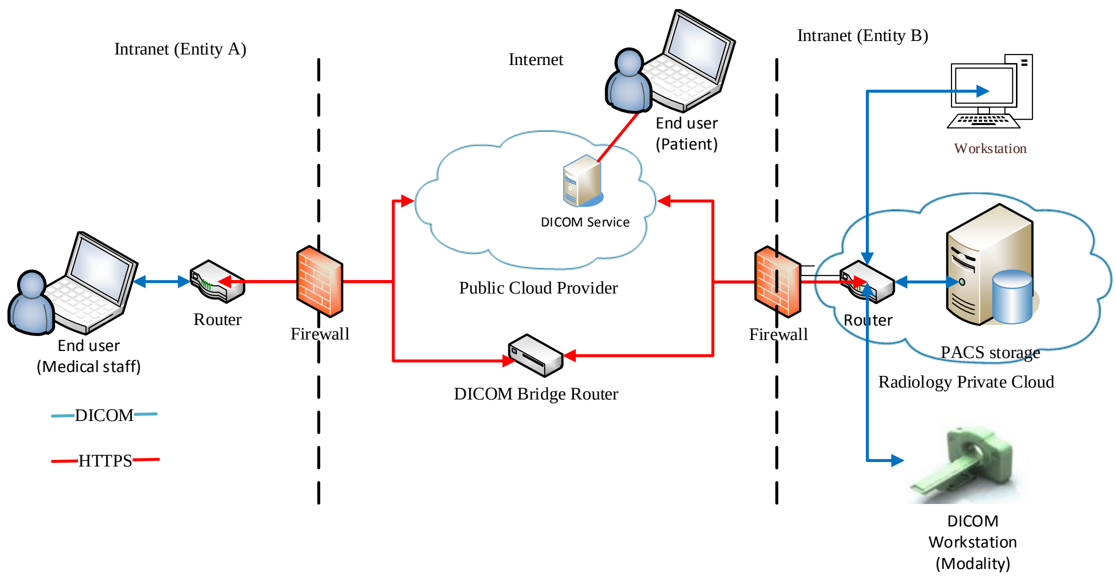

Fig.4 Radiology data access in hybrid cloud

As example, in a radiology private cloud DICOM objects are available for all users dependent on their profile and point of access in two quality formats: DICOM (high quality) and JPEG (low quality). DICOM objects are available, for both internal and external users, in JPEG format (DICOM objects are converted to JPEG format by DICOM Service available at private cloud level) and DICOM objects format (Fig. 4).

2.2. Private Cloud Platform

Private cloud platform provides hardware and software components (PaaS) addressing all identified IHE healthcare requirements. Main functionalities implemented at this level are:

- Authentication via cryptographic protocols that allow users to access private cloud resources after successful identity verification.
- Authorization process allows individuals or user group access to private cloud resource based roles.
- Data persistence function assures healthcare data storage for a long-term.
- Data integrity ensures data is complete and consistent during any exchange operation.
- Data confidentiality consists in mechanism hat store and transmits data accessible only for user that are entitled.

Private cloud generic workflow presents a scenario in which a user consumes a healthcare cloud service provided by Healthcare Hybrid Cloud platform in order to support healthcare data capture, storage and consumptions in five main steps:

- Authentication process considers internal or external user logs on using a user name and a password using a device connected to the Internet to a healthcare service.
- Service request is send from the user's client software using the security credentials achieved in the authentication step.
- Instantiate the service is done after the user's identity is resolved in a role and matches the service request to existing security policies.
- Authorization occurs after the service corresponds to security policies and is instantiated. User logon data, role, reference to the service endpoint and validity period enable the user's client software to establish a secure SOAP session. In case service request is not permitted by security policies, a message is returned to tell the reason for rejection.

- Service consumption performs after the user's client software initiates a secure session.

Access workflow of the hybrid cloud is presented from the perspective of private and public cloud communication scenario. Conceptual structure of cloud services access at private cloud platform is presented in Fig. 5.

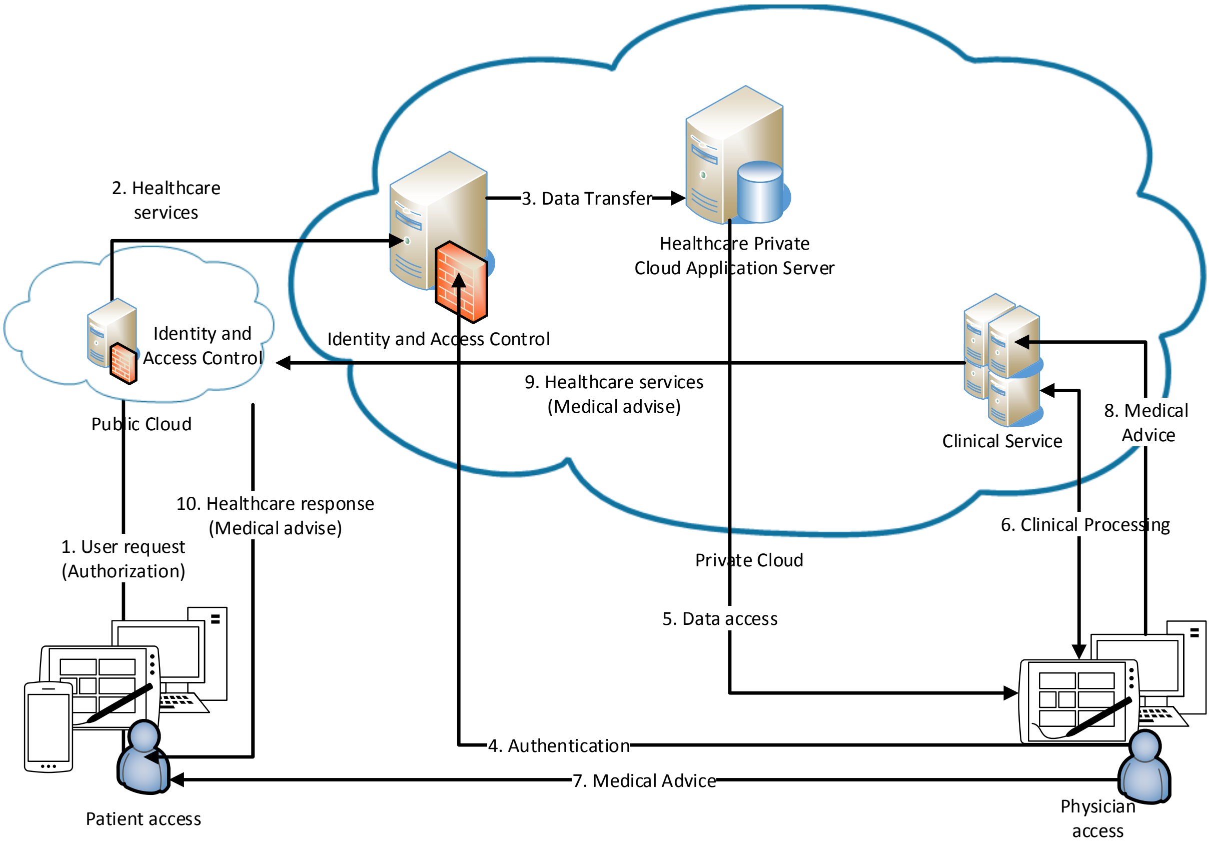

Fig. 5 Private cloud scenario

A patient is considered as external user; therefore he accesses the hybrid cloud authentication services, deployed on public cloud identity and access control using a user name and a password and place a request for authorization (1). Based on the request type (storage, access, process of health data) it is processed at public cloud level or is forwarded to identity and access control service from private cloud (2). In case request is accepted by private cloud server, it is forwarded to healthcare private cloud application server (3) otherwise a message is returned specifying rejection reason.

The physician is considered as internal user and logs on to the private cloud services and sends an authorization request containing user and password to identity and access control (4), access data using healthcare private cloud application server (5), process data (research studies, additional specialist comments, etc.) accessing clinical cloud services defined (6) and provide medical advice directly to the patient or updating the information in the system (8). Patient is informed for the latest medical data condition using notification services defined in hybrid healthcare cloud (9)-(10).

2.2.1. Image virtualization

Private cloud for radiology needs to offer support for high quality image viewing for end user, for a large amount of image studies that needs to be transferred to diagnostic workstations. Concept of remote virtualization, describing the split between desktop environment and associated application software on one side and physical client device on the other side, is applied for cloud data center servers that are responsible for providing the images and send them to the end-point device or remote client.

Three technologies can be successfully used for end-point devices (mobile devices, medical workstation, etc.) to exchange images over the internet in a radiology private cloud [91]. Radiology private cloud focus mainly on Rich Internet Applications and browser zero-footprint web application:

- Rich Internet Applications (RIA) web applications developed especially for clinical viewer devices, provided over the Internet using standard browser. Applications relay on client environment (Adobe Flash, Microsoft Silverlight) with options to be automatically loaded and upgraded by the browser.
- Browser based zero-footprint web applications become recently available for clinical viewers for displaying images and restricted applications for diagnostic-quality viewers with the advance of HTML5. Viewing applications are available for all devices that support HTML5 browser (Chrome, Firefox, Internet Explorer and Safari) and can be deployed on any device that runs a supported browser.
- Desktop virtualization procedure converts traditional thick clients into cloud friendly applications providing remote access to an operation system running on a remote virtual machine.
- Thin client applications are implemented as desktop applications that use image provision service from remote cloud server. Hybrid cloud recommendation is to adopt this technique only for end devices that do not support RIA or zero footprint applications due to the following disadvantages: operating system incompatibilities - applications depend on the operating system that runs on initially deployed end-point

device; installation costs - applications need to be installed in each end-point device; maintenance costs – each installed instance needs to be maintained involving additional costs.

2.2.2. Workflow engine

The traditional PACS workflow engine should be migrated to private cloud servers in order to achieve full integration processes with enterprise resource planning services. Work list for all medical resources (medical equipment, physicians, radiologists, nurses, etc) are unified in a single general list that is to be planned for all radiology centers that are registered to the private cloud. New cases are sent to the most available specialist avoiding healthcare organizations overflow based on a list of parameters: patient history, patient – hospital/clinic distance, waiting time, etc.

2.2.3. Image archive

Image archive is aggregated in the radiology private cloud storage including existing legacy PACS storages that are migrated. All healthcare organizations from different geographical locations have access to radiology data base providing the following overall advantages:

- All previous studies from different locations are available for study in order to provide a documented diagnostic/ medical advice.

- In case of emergency situations unnecessary imaging are prevented due to the availability of patient history in the centralized archive.

- Usage of physical memory devices (CD/DVD) is significantly reduced since data is available to all involved parties at the required quality

2.3. Public Cloud Platform

The conceptual structure of public cloud platform described in Fig. 6 presents a generic access to public cloud services of healthcare hybrid cloud platform.

Public cloud services are addressed only by external: patients, third parties employees (insurance companies, pharmacies, research healthcare companies, drugs manufactures, etc.) The external user logs on using account data (user and password) addressing public identity and access control cloud services place a request for authorization (1). If access is provided user request is forwarded to public cloud application server (2). Application server request data retrieve/store from private cloud services through clinical cloud services (3). Public clinical cloud services request authentication from private cloud identity and access control in order to gain data access (4). Once authentication succeed private cloud services process the request and provide required response to service application services from public cloud (5).

In case physician access is required notification is send and as response she/he logs on to the private cloud through identity and access control, access data and provides comments, update healthcare data. Public cloud services provide feedback to the external user as response to his/her request (6).

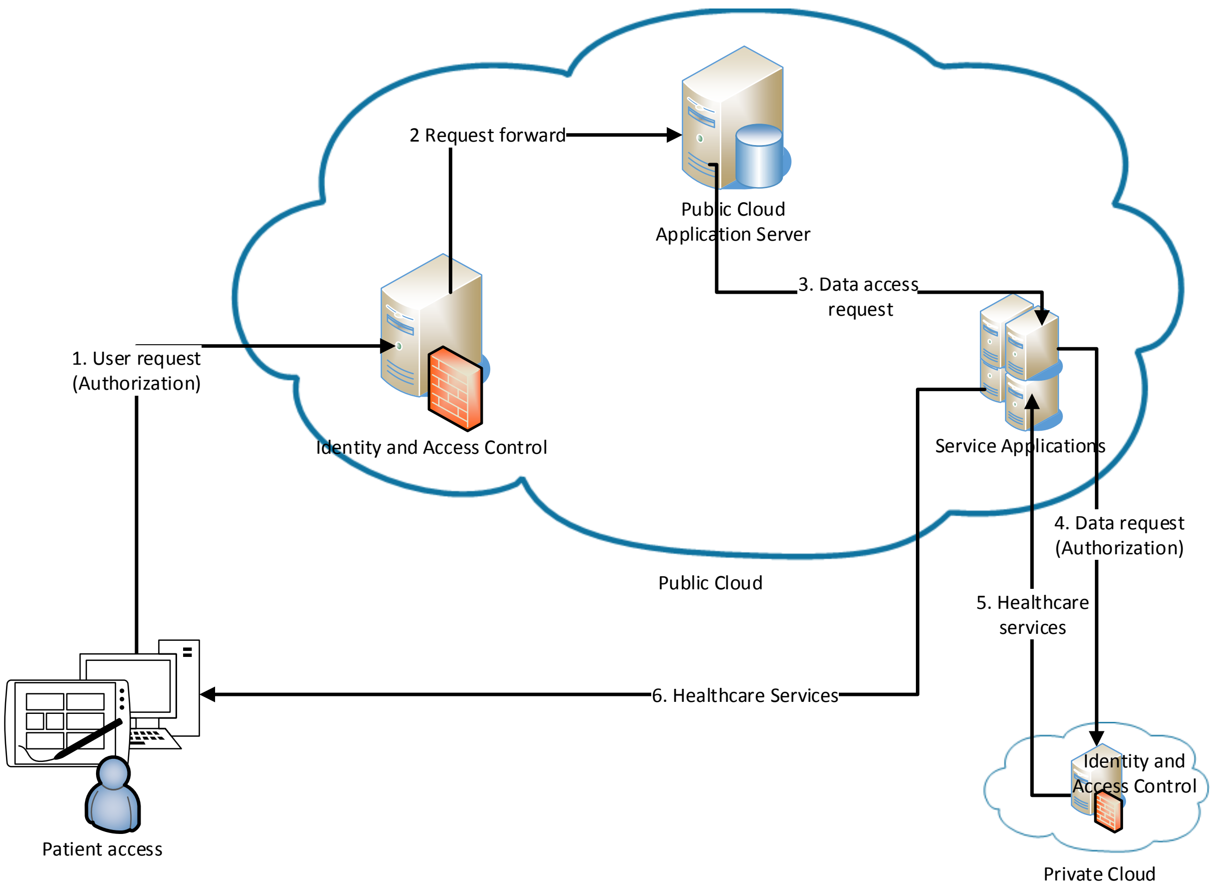

Fig.6. The Public cloud scenario

2.4. The mathematical model of the Hybrid Cloud architecture

Cloud computing systems offer the illusion of infinite computing resources available on demand allowing dynamic resource allocation for customers when they need it. Performance parameters need to be taken into consideration when scaling the system presented above that deploys a platform able to support computing needs of many hospitals with different clinical departments along with their clinicians and patients. Performance parameters are considered at public cloud level due to high number of requests that are received his point as system input.

As stated, the objective of this research project is to consider the healthcare organization as a business that fully integrates clinical processes. Cloud service and deployment model is determined based on the healthcare organization strategy expected to be accomplish. In order to validate the model proposed in section 2.1, several cloud services included in the model need to be considered. As a scope of this section model of accessing radiology data in an integrated healthcare cloud platform is built using queuing theory.

In order to achieve the highest value of quality in the service that is to be designed it is required a strong analysis of the service system from dedicated resources and demands placed on the system perspective. Ideally in a healthcare information system a patient should never wait for a medical service but in this case we face a limited number of resources (medical staff, modalities, waiting times etc.) and an uncontrollable number of patients. Based on analyses of 141 papers presented in [4] queuing theory use in analysis of healthcare processes is feasible and recommended for QoS analysis for both physical queues that are created for clinical service access or for healthcare information system modelling processes. Queuing theory is used to predict the QoS measured in a variety of ways, as a function of both the demands on the system and the service capacity that has been allocated to the system [5], [6].

2.4.1. Private cloud Controller

HTTP requests are received from private cloud users (local staff, administrators, etc.) and requests that are received from public cloud application server. Cloud controller dispatcher organize the input requests in a single waiting queue, following priority discipline (highest priority class requests first) allocated to private pool of resources. A schematic representation of private cloud model is given in Fig. 7.

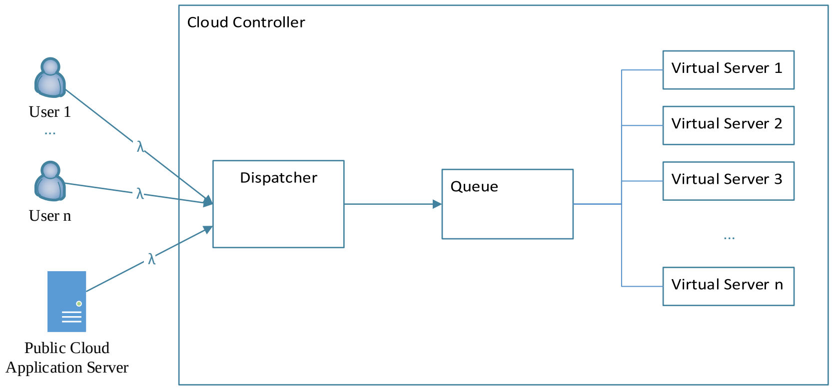

Fig. 7 Private cloud controller

Considering the above cloud platform queuing theory is applied in order to analyze the platform as a typical queuing model, described in Fig. 8 having a FCFS queue that follow priority queue discipline (highest priority classes are processed first) established as input by the cloud controller that is to be processed by a dispatcher that forwards the requests to the database.

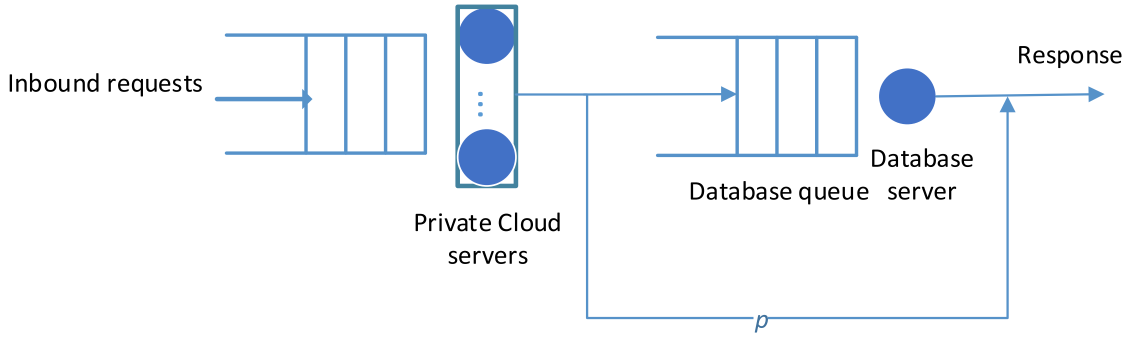

Fig. 8 Private cloud queue system

Using Kendall notation for queues we consider a model of a cloud system composed by two queues $M/M/s$ entry queue and $M/M/1$ database precede queue. Medical imaging devices generate extremely massive data requiring huge data storage therefore from simplification reasons second queue from cloud controller is considered a single server queue as buffer for database.

Considering the probability that a request from $M/M/s$ will enter in $M/M/1$ before database p (server is still busy with preceding request) or access directly the database $(1-p)$proposed mathematical model for the cloud system considers two serially connected queues with arrival rate λ for $M/M/s$ and λp for $M/M/1$ (Fig. 9.).

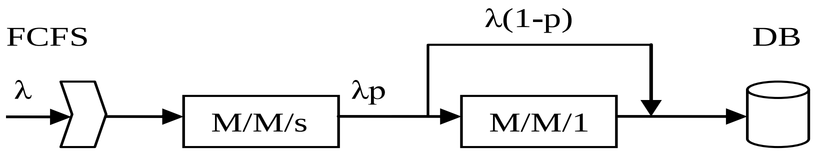

Fig. 9 Private cloud service mathematical model

2.4.2 Public cloud Controller

All HTTP requests from cloud users (patient, third parties users and external clinicians) are received by the public cloud controller. The Cloud controller dispatcher organizes the input requests in a number of input waiting queues that are allocated to pools of resources. A schematic representation of public cloud model has been depicted in Fig. 10.

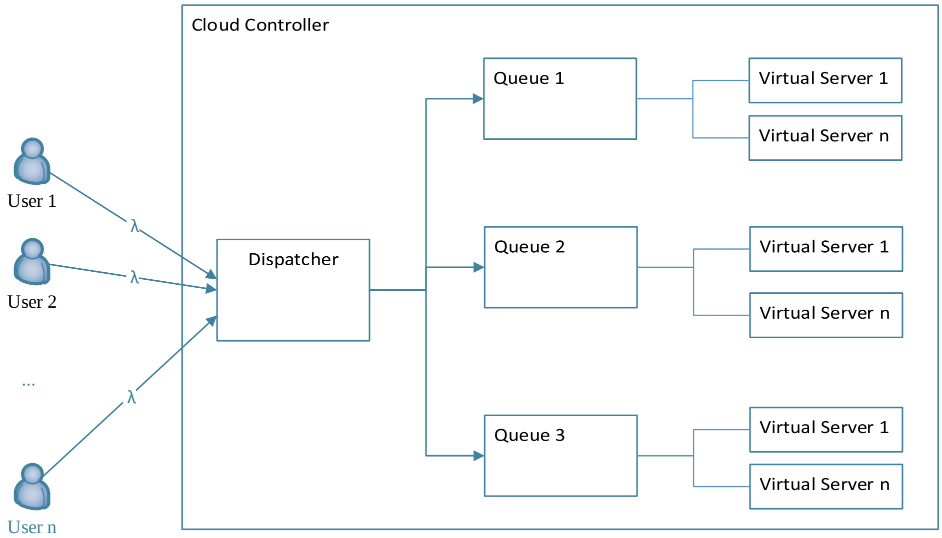

Fig. 10 Public cloud controller

Waiting queues for patient/resource scheduling and data access represents a challenge for healthcare IT research domain due to the need of understanding clinical and information processes from service modelling and management perspective. Cloud architecture proposed in Fig.1 considers a PACS database integrated in a private cloud and a management application integrated in public cloud in order to obtain full access to data for any point. Requests for medical images are coming in the presented hybrid cloud architecture from multiple points: mobile infrastructure (mobile phones, tablets, laptops, etc.), hospital management systems, radiology cliques, emergency units, insurance companies, etc.

Based on high demand requirement from healthcare application, advantages and disadvantages of cloud computing platform aim of this section is to discuss theoretical analysis for performance of the proposed model based on queue model. The mathematical analysis is done for measure system performance in terms of queue length, response time including average waiting time, mean queue size, delay and resource utilization in order to demonstrate effect of priority classes on overall system performance.

In order to understand the behaviour of the proposed healthcare cloud application all properties required by the process of requests for medical data are drawn as following:

- All user requests are gathered in a service centre as single point of access for all users (cloud controller). Arrival time between two client requests is independent of each other;

- Client requests will receive response after they are processed with a response time that must be lower than the agreed SLA response time;

- Service response time is defined as $T_{srt} = T_{sub} + T_W + T_S + T_E + T_R$ introducing the following notations: submission time T_{sub}, waiting time T_W, service time T_s, execution time T_e and return time T_r. T_{sub} and T_r are considered negligible.

- Client requests are to be processed by the service in a first come first serve (FCFS) order

- Application cache/buffer is limited therefore number of waiting requests is limited. Since lost request should be minim or even should not be the case queue length must be analyzed.

Considering the above cloud platform properties, the queuing theory is applied in order to analyze the platform as a typical queuing model, described in Fig. 11 having a FCFS queue established as input by the cloud controller that is to be processed by a dispatcher that forwards the requests to the scheduler.

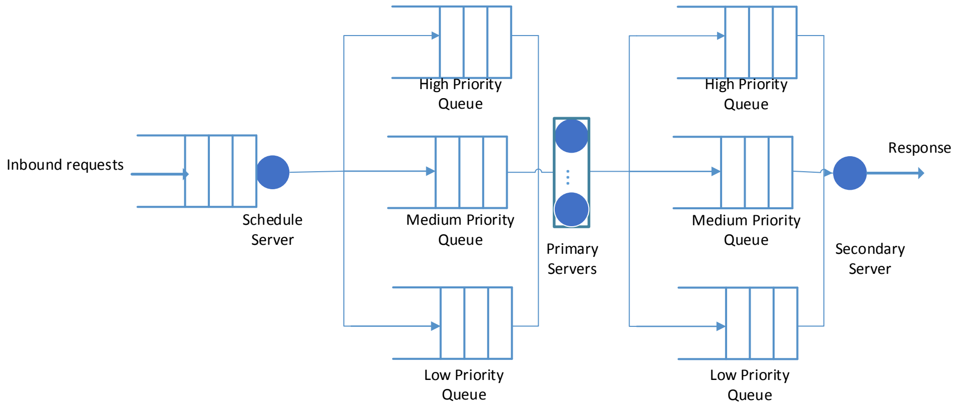

Fig. 11 Public cloud queue system

The Cloud system is defined as a pre-emptive priority service (low priority service is interrupted and high priority service is executed). The schedule queue system receive a FCFS queue and classify each requests as high, medium or low priority request building three input queues for primary system. The primary system is a queue system that receives multiple waiting queues that are processed by multiple servers. Primary servers will schedule the highest priority requests first and place the result in three priority queues as input for secondary servers. In secondary queue system results are sent to the requester, sending the highest priority requests first.

In order to collect all requests at public cloud level a special handling of requests is proposed based on queuing theory. Each request that is entering in the cloud is linked to an entity with a certain priority class assigned from 1 to r. Based on the priority class the application creates r queues after first come first served ($FCFS_r$) principle and offer as input to the primary queue system r FCFS queues in priority order: $FCFS_1$; $FCFS_2$; … ; $FCFS_r$. In order to simplify the simulation three main priority classes are considered: high, medium and low.

The algorithm is as follows:

Algorithm: Dispatcher priority queuing

Input:

  HTTP request queue

Output:

  Three FCFS priority queues

Algorithm:

repeat

while $FCFS_r \neq \Phi$ *do*

  case priority

    when 'High':

      add r to $FCFS_H$*;*

    when 'Medium'

      add r to $FCFS_M$*;*

    when 'Low':

      add r to $FCFS_L$*;*

  end case.

end while.

  Until $\exists r_i \in FCFS_r$

Using Kendall notation $A/S/c/K/N/D$ for queues, where A is the arrival process defined here as Poisson process M, S is service time distribution defined as exponential service time, c is the number of servers, K is capacity of queue, considered infinite in case it is not specified, N represents the size of population of jobs to be served, considered infinite in case is not specified and D defines the queue discipline defaulted as FIFO.

The proposed model considers a model of queuing system composed by three serially connected queues: M/M/1 schedule queue, M/M/k/N primary queue and M/M/1 secondary queue (Fig. 12).

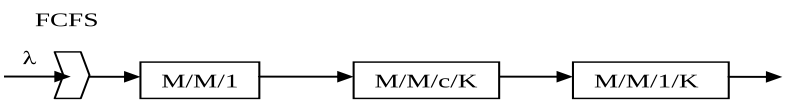

Fig. 12 Public cloud service mathematical model

Observation 4.1: Priority class defined for a request has the following values: high, medium, low and is characterized average request arrival rate λ, and service response τ in seconds.

Observation 4.2: Queue discipline is defined base on priority: requests with the highest priority have absolute priority over lowest priority requests.

3. Concluding Remarks

The proposed architecture is designed to support end-to-end healthcare provided services from clinical and administrative perspective sharing information between multiple internal entities with different health applicability domains and third parties (insurance companies, government institutions, etc.) over a large geographical area. The design criteria were presented from the perspective of radiology domain integration due to high amount of data that needs to be stored and complex DICOM objects to be shared between imaging centers.

The proposed cloud based architecture for the healthcare system specified considers that all the medical data are stored in a private cloud and all the departments of the healthcare provider can access medical patient data when is needed. In this case, the medical act is performed quickly without high waiting times driving to higher quality of the provided service.

Mainly due to security concerns and required applications architecture consists in a hybrid cloud-based architecture composed by several private clouds that are representing each specific department (Radiology Private Cloud, Emergency Private Cloud) and a public cloud used to integrate all healthcare entities and the third parties. Applications and data storage can be found within each private data centre of the healthcare provider (specialized department that requires a particularly handle of data, for example: radiology, emergency, etc.).

The purpose of the public cloud is to avoid the mesh network within the private clouds connections. Communications between two public clouds will be held through HL7 CDA messages after the link between the applications will be establish using an application defined in the public cloud. The radiology data will be stored in private centers that owe an imaging centre (radiology, emergency) and that have migrated from a PACS archive to the cloud centre. Data can be accessed by all entities from the infrastructure using a designated private cloud application

The Cloud architecture proposed considers a PACS database integrated in a private cloud and a public cloud management application in order to obtain full access to data for any point.

Having multiple points of access at private and public level, a mathematical model based on input requests priority classes has been provided and analyzed in terms of queues waiting time in order to demonstrate cloud platform performance. Arrival requests are classified in three priority classes: high, medium and low that needs to be handled by the system according to a predefined priority policy. Priority policy assumes that highest priority classes are processed first by the system.

Due to the high numbers of request that are expected to be received, a mathematical model should be used for numerical calculations and simulations in order to analyze the system's performance parameters:

- The public cloud is defined by an analytical model, which is built up as a three serial connected queues, first one to classify requests based on their priority (schedule queue), second one having a dynamic algorithm of resource allocation based on priority classes that concentrates most of the available resources (primary queue) and the third one that sends the requests received from the preceding queue to the requestor. Using the queuing theory system it can be defined as a three serial connected queues that can be analyzed individually: $M/M/1$, $M/M/c/K$ and $M/M/1/K$.

  The performance is handled by the determination of mean performance parameters for number of request in the system, time spent in the system and waiting time. From the perspective of request handling at public cloud level the following aspects are considered: level of QoS services that can be guaranteed by a given number of service resources and the number of service resources that are required for a given number of customers in order to ensure that customer services can be guaranteed in terms of percentile of response time.

- The private cloud focuses on accessing radiology data from database. Analytical model considers variance of requests waiting time in order to decide number of needed resources. Using the queuing theory, this system is defined as a two serial connected queues that can be analyzed individually: $M/M/s$and$M/M/1$.

  Performances are handled by the determination of waiting time as a variation of needed resources in the private cloud and the quality of database services. Quality of database services is simulated by introducing a probability p that requests will reach the second $M/M/1$ queue before database services are processing the request.

4. Project Partners

- University Politehnica of Bucharest
- University Transilvania of Brasov
- The Clinical Hospital Fundeni
- The Clinical Hospital for Children Marie Curie
- The company RMS, ICT systems developer