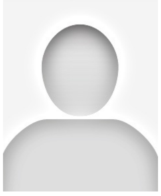
HealthManagement
Promoting Management and Leadership

Volume 7 - Issue 2, 2012 HIT - Cover Story

Data Ownership & Protection Issues

Luís Bastião Silva, CTO of BMD Software
******@***bmd-software.com



Carlos Costa, Director
******@***ua.pt

Professor - University of Aveiro

José Luís Oliveira, CEO
******@***ncl.pt

Associate Professor - Universidade de Aveiro

Technological advances have created great opportunities for society to develop new products and services, and to communicate and share data. A tremendous amount of ubiquitous computational power and online services are used every day as a normal commodity. These new facilities allow data storage and exchange of information anytime and anywhere, at high speed. In recent years, cloud computing is the new term that has emerged to define these services. The main idea is to merge computational power and storage in a dynamically scalable infrastructure, i.e. the system capability grows as needed, which allows decoupling of the business service from infrastructure. This new buzzword is changing the computing paradigm and has given rise to vendors dedicated to providing this new utility in a pay-as-yougo business model, offering customers huge computational power and storage. The offer is diversified, including virtual operating systems and basic services, for instance, storage, database and signaling.

It is evident that the computing-as-utility business model is becoming prevalent in the electronic world and numerous industries are adopting it. So this new paradigm ought be of interest to the healthcare industry in various ways and may likely be increasingly adopted in the coming years. The medical imaging sector will not be an exception, despite its special requirements. The main advantages of cloud computing are cost savings, wide availability and high scalability. However, this new technology also brings new challenges regarding data ownership, trust, privacy and interoperability with healthcare standards. In this article, we will stress the applicability of cloud computing solutions to support medical image repositories, addressing the existent problems and point out possible solutions to solve these issues.

Trust and Data Privacy

The outsourcing of data records can be a good solution, depending on the type of information transmitted to the cloud providers. The privacy of medical information is a vital requirement and a very sensitive issue, especially when medical digital images and patient information are stored in third parties and transmitted across public networks. Healthcare institutions often insist on safeguarding the privacy of involved actors to avoid data being tampered with by provider companies (i.e. cloud services suppliers).

Medical image repositories usually deal with outsized data volumes, regularly including an ever-growing list of files. Apart from medical exams, PACS also supports a database with textual information corresponding to those exams. Both are relevant and only authorised parties should access them. Thus, a challenge in outsourcing medical images over the cloud is how to protect the privacy of patients and physicians, including protection against misuse of data.

A possible way to minimise those risks is the use of a hybrid cloud solution, i.e. a combination of public computing utility with a local infrastructure retained by institutions. The idea is to keep critical mechanisms inside institutions and outsource the heavy computational resources. The hybrid cloud approach allows outsourcing of medical records without losing control, which means that only authorised entities can access the data. The third party entity, located within the institution’s control, provides the core element of privacy. This huge amount of medical information is stored across public cloud providers, granting patient privacy through data encryption. Possible unauthorised access to the cloud repository does not jeopardise data privacy, since access to the repositories requires the right key to get medical imaging records. Moreover, an additional strategy of splitting ciphered chunks of the same image across different storage providers could be used to provide an even higher level of privacy.

Data Ownership and Protection

Data protection in the outsourcing of medical images is required because these records are important assets for data holders. Medical institutions need to be aware of legal aspects when storing data in outsourced repositories. The first concern should be the SLAs (Service Level Agreements), giving special attention to the problem of data locking. Another topic to be considered is the permanence of patient data. Data protection laws in several countries, require knowledge of where data is stored. For this reason, storage of patient data in the cloud will be very difficult to use in countries like Spain, France or Italy. However, several cloud providers allow obligatory data storage in a specific geographic location. Thus, the problem addressed can be minimised and even countries with higher restriction laws might accept the solution.

Economic Aspects

Healthcare institutions need to reap certain benefits in terms of service quality and financial impact to be motivated to outsource their medical repositories. To analyse if cloud computing is economically viable in the imaging context, the following cost variables of the current solution are crucial:

- Server hardware;
- Network equipment;
- Licenses;
- Energy;
- Air conditioning;
- Maintenance; and
- Technological obsolescence.

A medical image repository based on the cloud does not require high initial investment compared to traditional archive solutions, which require purchase and maintenance of a data centre. It is well suited to a small centre because it does not require initial investment. However, for medium-to-large image centres there is a point of operation where it is economically more rational to have data centre storage in co-location. It is very difficult to define this tipping point because it is dependent on department workload and processes, and the cloud services market is rapidly changing, providing more resources at lower cost.

Furthermore, the cloud solution can facilitate multicentre collaborative environments, including the sharing of medical records across medical institutions. So it will reduce duplication of medical exams, on one hand reducing the costs of patient care, and on the other, reducing the dose of exposure to radiation.

Interoperability with Healthcare Standards

There are many standards in the medical community (DICOM, XDS-I, IHE, HL7, etc.) that need to be interoperable with current cloud providers' interfaces. Historically, healthcare communications standards were thought to operate inside an institution's intranet. However, new standards are starting to follow a service-oriented architecture (SOA), which allows inter-institutional communication. Nevertheless, the compatibility with cloud services' interface is not directly supported due to data privacy and confidentiality.

For instance, in medical imaging, communication between medical devices follows the DICOM standard. However, the cloud data store and database interfaces are not DICOM compliant. Most public cloud providers supply access to their services through a proprietary web service interface. Thus, we need a middleware component to provide interoperability between DICOM equipment and cloud repositories solutions compatible both with medical practice and pre-existing medical information systems (Bastião et al., 2011). To access cloud medical image repositories we need a cloud broker (see fig. 1), which will carry out the communication with healthcare standards (for instance, DICOM), as well as cloud services.

Data Availability

The availability rate of cloud services is very high, which means that services are always ready and reachable. However, availability in the medical imaging scenario is linked to the performance of access to the repository. Due to latency associated with service access and communication with public cloud providers, the retrieval process can be slower. This process is extremely important for the overall quality of the solution because there is real-time interaction with end-users, i.e. the professional is at the computer waiting for images. In order to reduce latency in data transmission, a caching mechanism can be placed on the cloud broker inside the medical institution. This mechanism is a local storage area that temporarily stores studies that are very likely to be requested in future operations. Moreover, the usage of pre-fetching mechanisms associated with the cache is fundamental to the solution's viability.

Conclusion and Future Perspectives

The use of a cloud computing utility has increased significantly in recent years and it appears to be a natural evolution of the data centre to execute computing and storage in a more scalable way. With such a significant increase, the market is growing quickly and more companies are providing new services with better features, including isolated services. We strongly believe that in the near future, cloud computing will be widely used in the healthcare sector. Several companies are already adopting this kind of solution, offering PACS and RIS services in private clouds.

Medical images are very important records, and so the storage repository needs redundancy to be a reliable system. Cloud providers offer this data security and backup system without any worries or additional charges for customers. Medical institutions can reduce the costs of local storage maintenance with PACS archive outsourcing. Moreover, outsourcing is an opportunity for small image centres that purchase modality equipment, despite not having the financial resources to buy software and hardware to keep up a PACS repository as it grants a redundancy/backup system.

Published on : Mon, 27 Aug 2012