HealthManagement
Promoting Management and Leadership

Volume 14, Issue 5, 2012 - Information Technology Special

Applying Cloud Solutions in the EHR Environment

Over the last few years everybody involved in the IT world has been talking about the famous cloud.

Maybe you have heard about it, but what are they actually referring to?

Cloud computing essentially refers to a change of mentality in the way of developing the storage systems of either a company or a single user. This new paradigm allows the customers to hire IT services as if they were renting them. So, now a company that needs a storage platform doesn't need to deploy its own platform, they just have to contact a cloud services provider and get the whole system as a service. This whole process must be absolutely transparent for the end-user as if he had its own IT infrastructure.

What does this mean? Through cloud solutions customer companies are not responsible for the management and maintenance of the IT infrastructures. Moreover, with this kind of model customers just rent the services for a third-company provider and get the final service. More advantages like the flexibility, scalability, availability and on demand services will be explained later.

Focusing on the e-health environment, the cloud business model offers a lot of advantages like those quoted above. However, it is important to remember that there are several risks to overcome in the data migration process. Security and confidentiality of patient data must always be preserved.

Concepts of the Cloud

In this section the models of deployment and types of cloud computing are very briefly described so explain how the "cloud-world" works.

Models of Deployment

Depending on the services or infrastructures that are rented by the cloud customer there are mainly three models of cloud computing:

1. SaaS: Software as a Service
This model of cloud computing offers the whole service to the client. So the cloud provider is responsible for the whole infrastructure and the application itself. The end user is able to access the data or resources without having to install any kind of software. Normally applications are accessed through a traditional web browser or an application \ provided by the cloud company.This model is not really useful for EHR management systems, because it doesn't allow the personalisation of the application, which is essential. Even though there are several options of cloud providers that offer complete solutions for managing EHRs in which the software itself is included, on hiring SaaS solutions hospitals will have to overcome the problem of compatibility with the handling system.

2. PaaS: Platform as a Service
With this type of model the application is the responsibility of the health centre. The cloud provider offers the platform and databases under the application. This means that the EHRs management application can be personalised by the hospital IT personnel, increasing in that way the compatibility with the previous systems and adjusting the software to the health centre needs.

3. IaaS: Infrastructure as a Service
With IaaS the cloud provider is only responsible for the hardware infrastructure. This infrastructure includes network and storage devices responsible for providing the bandwidth and capacity to fulfill the client requirements. What does this mean? With this type of model the customer has total ability to personalise its own software application, including the database.

The three cloud deployment models are graphically explained in Figure 1.

Types of Clouds

Depending on several factors like security and performance, health organisations can choose to migrate their data to different kinds of cloud.

1. Public Cloud

In the public cloud, the infrastructure, storage and computing resources are shared by several clients. Thanks to the virtualisation concept that will be explained briefly later, the cloud provider is able to provide the different hired resources of each client through the same platform. Security and privacy mechanisms are integrated in this kind of cloud but the customer must be aware that sensitive data will be more exposed to security attacks in this kind of cloud.

2. Private Cloud

Health centres and hospitals handle patients' sensitive information. This can be problematic when it's time to move their data to the cloud. To solve privacy and security issues companies choose to store their resources in its own cloud. That is why it is called a private cloud. There are two types of private clouds:

- On Premises Private Cloud: The cloud infrastructure belongs to the enterprise that uses;
- Externally Hosted Private Cloud: The cloud provider deploys an infrastructure used exclusively by the customer; the customer rents the whole cloud. Deploying a private cloud is the best option in terms of privacy and security but, obviously, the cost of this type of cloud computing is higher.

3. Hybrid Cloud

The hybrid model represents a mixture of both models above. Sensitive data is stored in the private part of the infrastructure whereas the rest of the information in stored in the public infrastructure. By deploying a hybrid cloud the company ensures the security and privacy for their sensitive data with a lower cost than if a complete private cloud were deployed.

Why Cloud on a Hospital Environment? Virtualising the E-Health Environment

Before explaining the benefits and advantages of deploying a cloud model over a health cen-tre EHR management infrastructure it is interesting to explain the concept of virtualisation, which is the key to cloud computing.

Virtualisation: Key of Cloud Computing

Virtualisation can be defined as the ability of abstracting physical resources and making them appear as logical resources. What does this mean? Through virtualized environments it is not necessary to have the physical network or storage infrastructure. With cloud environments hospitals don't need to deploy their own IT infrastructure: "It's all on the Cloud".

Benefits

Table 1 explains the main advantages of a cloud environment for EHR management system.

Challenges to Overcome

Security and privacy of patient health information stored in the EHRs must be essential when migrating the data to the cloud. Hospitals must be aware that with the cloud model this sensitive data will be stored on the thirdparty servers.

Conclusions and Outlook for the Future

In the past few years digital information has experienced an amazing growth. Cloud-based solutions arise as a way of handling this huge amount of information. The e-heath environment can take advantage of this new technology; improving the availability of clinical information will help medical personnel improve their efficiency. Through cloud-based solutions the patients can also play an active part in this process, consulting their own EHR from any device with an Internet connection. Privacy and security issues must be the priority for both parties: health organisations and cloud service providers in order to guarantee the confidentiality of patient data.

Authors:

Gonzalo Fernández-Cardeñosa
Isabel de la Torre-Díez

Department of Signal Theory and Communications and Telematics Engineering University of Valladolid

gonzalo.fernandez.cardenosa@proact.es
isator@tel.uva.es

Published on : Fri, 22 Mar 2013