Volume 13 - Issue 2, 2013 - IT Intelligence

Cloud Computing for Health Information Management

Authors

Mu-Hsing KUO

Andre KUSHNIRUK

Elizabeth BORYCKI

School of Health Information Science

University of Victoria,Canada

akuo@uvic.ca

andrek@uvic.ca

emb@uvic.ca

Cloud computing refers to an on-demand self-service network infrastructure that enables the user to access computing resources at anytime from anywhere. Many managers and experts believe that it could have great benefits for health information management. However, cloud computing should be rigorously evaluated before its widespread adoption. In this paper, we discuss the concept, its current state in healthcare, and evaluate cloud computing opportunities and challenges for health information management. Software as a Service (SaaS)

Introduction

Healthcare is the most data intensive industry in the world. Modern health information systems (e.g. Electronic Health Records (EHR), Computerized Physician Order Entry (CPOE), Picture Archiving and Communications System (PACS)) used in healthcare settings (clinics, hospitals and labs) can generate an unimaginably vast amount of digital health data (so called Big Data). For example, in the 1970s, an X-ray computed tomography (CT) scan of a patient's body generated 100 tomographic images (slices) with a data volume of 50MB (5122 pixels/slice). Now, a CT scan can generate 24,000 slices (20GB) for one patient. It is predicted that the future CT can generate 1TB of slices for a patient which if printed equals to 800,000 phone books. G. Hughes estimates the growth in global healthcare data of between 1.2 and 2.4 Exabytes (1018 bytes) per year. This number represents roughly 10 times the data contained in every US academic research library combined. This data is also largely disparate and unstructured making health information management and extracting useful information all the more problematic.

In 2007, talk of a new on-demand selfservice network infrastructure (i.e. cloud computing) became prominent. Many managers and experts believe that it can improve health information management and EHR adoption. However, a healthcare organisation should carefully evaluate the benefits and risks before moving its services into the cloud. The objective of this paper is to discuss the concept of cloud computing, its current state in healthcare, and evaluate the opportunities and challenges of adopting this model for health information management.

What is Cloud Computing?

The U.S. National Institute of Standards and Technology (NIST) defined Cloud computing as follows: Cloud Computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or serviceprovider interaction.

Cloud computing is a new model of delivering computing resources, not a new technology. Similar, more limited, applications are not new to many of us because we have been using this kind of service, such as Microsoft Hotmail

or Google Docs, for years. However, when compared with conventional computing, this model provides three new advantages: massive computing resources available on demand, elimination of an up-front commitment by users and payment for use on a shortterm basis as needed.

According to the NIST, cloud computing includes three fundamental service models (see Figure 1):

(1) Software as a Service (SaaS)

© For personal and private use only. Reproduction must be permitted by the copyright holder. Email to copyright@mindbyte.eu.

The applications (e.g. EHR) are hosted by a cloud service provider and made available to users over the Internet. The user does not control either the underlying infrastructure or platform. Examples of this service are Yahoo Mail, Microsoft Exchange Online, Google Docs and Oracle CRM On-Demand.

(2) Platform as a Service (PaaS)

The application development resources (hardware, operation system, programming languages, toolkits) are hosted in the Cloud. The PaaS user can use the services to develop higher level applications and host them on the platform to serve its end-users. For example, Google AppEngine, Salesforce.com and Facebook provide user PaaS services.

(3) Infrastructure as a Service (IaaS)

The capability provided to the IaaS user is storage, networks, and other fundamental computing resources where the user can run and execute an operation system (OS), applications, or any software that they choose. However, the user is not able to manage or control the cloud infrastructure but has control over OS, applications, storage, and selected networking components (e.g. firewalls). Users typically pay on a per-use basis. Now, Amazon AWS (EC2, S3, SQS), Microsoft Azure and Rackspace Cloud offer such kind of services.

To deploy cloud computing, there are four commonly adopted infrastructures (see Figure 2):

(1) Public Cloud

A cloud service provider makes computing resources, such as applications (e.g. EHRs) and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model. For example, Amazon Elastic Compute Cloud (EC2), Google AppEngine, Windows Azure Services Platform, Salesforce Chatter and BM's Blue Cloud provide cloud services to the customers who registered to their Clouds.

(2) Private Cloud

The cloud infrastructure is dedicated to a particular organisation and not shared with other organisations. In other words, the proprietary network or the data centre supplies hosted services to a certain group of people. For example, Microsoft Azure enables customers to build the foundation for a private cloud infrastructure using Windows Server and System Center family of products with the Dynamic Data Center Toolkit.

(3) Community Cloud

The cloud infrastructure is shared by two or more organisations with common concerns, such as mission, security requirements, policy, and compliance considerations. The infrastructure management might be done by themselves or a third party.

(4) Hybrid Cloud

The cloud infrastructure is usually composed of several sub-infrastructures (private, public, or community clouds). In this infrastructure, an organisation provides and manages some computing resources within its own data centre and has others provided externally.

The Cloud Opportunities

The main advantage of cloud computing is its low cost. All kinds of IT measures, such as in hardware, software, human resources, and management, are cheaper when implemented on a large scale. Cloud users, such as smaller hospitals and medical practices, can easily get a cost-effective and on-premise IT solution through cloud computing without the need to purchase or evaluate hardware or software, or to hire internal IT staff to maintain and service inhouse infrastructure for mission-critical applications such as EHRs. The result is that the user can focus on critical tasks without having to incur additional costs with regard to IT staffing and training.

Most cloud providers replicate user data in multiple locations (data centres). This increases data redundancy and independence from system failure and provides a level of disaster recovery. In addition, a cloud provider always has the ability to dynamically reallocate security resources for filtering, traffic shaping, or encryption in order to increase support for defensive measures (e.g. against distributed denial-of-service attacks). The ability to dynamically scale defensive resources on demand has obvious advantages for resilience. Furthermore, cloud computing has advantages for socalled green computing - the more efficient use of computer resources to help the environment and promote energy saving. Usage of ready-made computing resources tailored to an organisation's needs certainly helps it to reduce electricity expenses to cool off computers and other components. This reduces the emission of dangerous materials into the environment.

Many previous studies reported the successful application of cloud computing in healthcare service and research. Among them, Koufi et al. reported a cloud-based prototype Emergency Medical Systems (EMS) that enabled physicians easy and fast access to patient data from anywhere and anytime. Hsieh and Hsu developed a cloud based 12-lead Electrocardiography (ECG) telemedicine service that enables healthcare collaboration between onsite clinicians and off-site senior cardiologists. The service provided patients convenient, efficient and inexpensive ECG telemedicine, especially for patients in rural areas. Kudtarkar et al used Amazon's EC2 to compute orthologous relationships for 245,323 genome-to-genome comparisons. The computation took just over 200 hours and cost US $8,000, approximately 40% less than expected. The Laboratory for Personalized Medicine of the Center for Biomedical Informatics at Harvard Medical School used high throughput sequencing and cloud computing to develop genetic testing models to develop innovative whole genome analysis testing models in record time.

The use of cloud computing for heath information management is reported worldwide. For example, the American Occupational Network and HyGen Pharmaceuticals are improving patient care by digitizing health records and updating its clinical processes using cloud-based software. Using the service, billing to individuals and insurance companies is faster and more accurate and has reduced medical transcription costs by 80%. Mount Sinai Hospital in Toronto and the Canadian government are working together to build a community cloud that will give 14 area

© For personal and private use only. Reproduction must be permitted by the copyright holder. Email to copyright@mindbyte.eu.

hospitals shared access to a fetal ultrasound application and data storage for patient information. In Europe, a consortium launched an advanced project called Trustworthy Clouds (TClouds) expected to be able to deliver a new level of secure, private and resilient computing and storage that is cost-efficient, simple and scalable. To demonstrate TClouds, scientists prototyped a patient-centered home healthcare service to remotely monitor, diagnose, and assist patients outside of a hospital setting. The complete lifecycle, from prescription to delivery to intake to reimbursement, will be stored in the cloud and will be accessible to patients, doctors, and pharmacy staff. In Australia, Telstra and the Royal Australian College of General Practitioners announced the signing of an agreement to work together to build an e-Health cloud for more than 17,000 GPs using a single sign-on to access healthcare applications, diagnostic tools and other clinical and administrative software. In Asia, the Department of Health, Taiwan is preparing to build a platform by storing citizen's personal health information and medical records in a cloud.

The Cloud Challenges

Despite the many benefits associated with using cloud computing, there are also a number of issues that will need to be addressed before its widespread adoption. According to Kuo (2011), there are many potential issues that may arise for a cloud project (see Table 1, pg.38). Some critical issues are as follows:

Security and Privacy Issues

It is believed that data security and privacy are the major concerns to the adoption of cloud computing in health IT. Cloud computing is a shared resource and multi tenancy environment for capacity, storage, and network. The security

and privacy risks of this type of environment include network breaks, separation failure, public management interface, poor encryption key management, and privilege abuse. Also, the centralised storage and shared tenancy of physical space means that users' sensitive data may be vulnerable to other malicious cloud users.

Data Jurisdiction Issues

In a cloud, physical storages could be widely distributed across multiple jurisdictions. Different jurisdictions may have

different laws regarding data security, privacy, usage, and intellectual property. For example, the US Health Insurance Portability and Accountability Act (HIPAA) restricts organisations from disclosing patient's health data to non-affiliated third parties. The Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) limits the powers of organisations to collect, use, or disclose personal (health) information. The European Union Data Protection Directive regulates the processing of personal data within the Union. Those regulations could make a great impact on a cloud project. Furthermore, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act gives the US government the right to demand data if it declares conditions as being an emergency or necessary to homeland security. The problem is that many main cloud providers such as Amazon, Microsoft and Google are US based.

Data Interoperability Issues

Cloud interoperability refers to the ability of two or more Clouds to share the same data, applications, services and platforms. There are many issues associated with interoperable data such as functional, data instance and metadata issues. Unfortunately, most cloud providers provide very little capability on data, application and service interoperability. This could be an issue for a cloud user migrating from one provider to another, or moving back to an in-house IT environment (i.e. data lock in).

Loss of Data Governance Issues

In some cases, a service level agreement (SLA) may not offer a commitment to allow a user to audit in-cloud data. The loss of data governance is the main concern when the user's confidential data and missioncritical applications move to a cloud computing paradigm where providers cannot guarantee the effectiveness of their security.

Conclusion

Healthcare managers and professionals are looking for strategies to increase health information management efficiency, flexibility and cost-effectiveness. Cloud computing is a new model of computing that promises to provide

more flexible, less expensive and more efficient IT services to the users. It is believed that this model can be a great opportunity for healthcare settings to improve information management. Nevertheless, when an organisation considers moving its service into the cloud, it needs to examine and address the new model's challenges, assess its capabilities to achieve the goal and identify strategies designed to implement it. We recommend that a potential user uses a SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis to evaluate the feasibility of the cloudbased approach. If the answer is yes then it can apply a strategic planning model to determine its direction, strategy and resource allocation to implement a cloud project.

Published on : Thu, 19 Sep 2013

© For personal and private use only. Reproduction must be permitted by the copyright holder. Email to copyright@mindbyte.eu.