Journal of Digital Imaging

Will the Next Generation of PACS Be Sitting on a Cloud?

James Philbin,[1] Fred Prior,[2] and Paul Nagy[3]

Cloud computing has gathered significant attention from information technology (IT) vendors in providing massively scalable applications as well as highly managed remote services. What is cloud computing and how will it impact the medical IT market? Will the next generation of picture archiving and communication systems be leveraging cloud technology?

KEY WORDS: distributed computing, enterprise PACS, grid computing, information storage and retrieval, cloud computing

OPENING STATEMENT

James Philbin, PhD We are at the dawn of cloud computing[1] for medical images. Several recent technological developments have converged to create an opportunity to deliver better, more secure, and less expensive medical imaging services through the use of cloud computing. Before discussing these technical advances, we need to define what we mean by Medical Imaging Cloud (MICloud). For the purposes of this article we will use the following definition: Medical Imaging Clouds provide on demand medical imaging information technology (IT) services from remote or remotely managed third-party platforms over a network. This definition allows MIClouds to include local edge nodes at the source imaging locations, but those nodes would be managed remotely and serviced by the cloud provider.

At first blush, this might seem very difficult since medical images, even when compressed, are large, i.e., 2–500 MB, and moving them from one location to another in a timely manner requires lots of bandwidth. In fact, as medical imaging studies grow larger because of higher slice count scanners and higher resolution images, it will take longer and longer to move the study from the picture archiving and communication systems (PACS) to the providers' workstations. The MICloud will provide a solution to this problem. There are several technologies that make MIClouds possible, including transport layer security encryption technology, which allows Health Insurance Portability and Accountability Act of 1996 (HIPAA) covered data to be transmitted securely through the Internet; high-speed data center networks, which allow data to be transmitted from server to server in a data center at 10–40 Gb/s, and web technologies, such as HTTP and Web Services, but the two most important are remote rendering[2] and virtual desktops,[3] especially with remote terminal PC-over-internet protocols (PCoIP).[4]

Remote Rendering Medical images can now be rendered in 2D, 3D, or 4D remotely from the desktop on which they are displayed. This technique, called remote rendering or server-side rendering, allows images to be processed (rendered) on a server in a data center that then streams only the bits necessary to represent the current 2D image on the user's display using techniques similar to those that allow a digital versatile disk movie to be streamed into your home. In general, a 4-Mb/s broadband connection provides enough bandwidth to handle real-time 3D manipulation. Remote rendering technology solves

[1]*From the Johns Hopkins Hospital, Baltimore, MD, USA.*
[2]*From the Mallinckrodt Institute of Radiology, St. Louis, MO, USA.*
[3]*From the University of Maryland School of Medicine, Baltimore, MD, USA.*
Correspondence to: Paul Nagy, University of Maryland School of Medicine, Baltimore, MD, USA; e-mail: pnagy@umm.edu

Online publication 24 August 2010
doi: 10.1007/s10278-010-9331-4

the problem of moving large datasets from the PACS archive to a diagnostic or clinical workstation for them to be rendered. In general, the bandwidth between the PACS and the Digital Imaging and Communications in Medicine workstation is 100 Mb/s or at most 1 Gb/s. In the data center, we can deploy 10 Gb/s (Ethernet) and 40 Gb/s (Infiniband) today, and in the next couple of years network bandwidth in the data center will exceed 100 Gb/s.

Remote rendering also has the benefit that once the medical images are stored in the data center, they remain there and only temporary views of the data go to the desktop. Another important aspect of remote rendering is that it can now be done on commodity central processing units as well as graphical processing units (GPU). This means that it is affordable to put a remote render engine in a small imaging center that may have only one computed tomography (CT) modality. Today's remote render engine vendors have viewers that can display images rendered from two or more locations. For example, the current study might be rendered in a small outpatient center and the priors rendered from a central archive. Remote rendering allows the diagnostic physician to read, even a continent away, from the location where the patient is scanned.

The second technology that enables MICloud is virtual desktops. We have been using virtual desktops which use a technology called PCoIP for transmission from the remote desktop to the thin client or portal hardware. The PCoIP compresses, encrypts, and encodes the entire computing experience at the data center and transmits only the changing pixels across a standard IP network to stateless PCoIP technology-enabled devices. PCoIP technology is delivered in both hardware and software implementations. In the limit, the client can be as "thin" as a monitor with an embedded chip (reference). In this case, the network plugs directly into the monitor and the monitor feels and acts as if it were connected to a local workstation; however, the "workstation" is a virtual machine running in a data center in the cloud. So when the user closes the session, say at work, and then goes home she can log into the same session with exactly the same state and continue working at home. Since the virtual desktop is hosted in the data center, it is available in the reading room, in the office, at home, or on the road. No more maintaining multiple desktops that are always out of sync. A server, depending on the configuration, we can run 50–100 virtual desktops, which can conservatively amount to saving at least US $500 per desktop.

Virtual desktops have many advantages; personal health information, in fact all data, are more secure as they reside in the data center. They are more cost effective, more reliable, easier to configure, backup, and maintain; user management is simplified, and the same computing environment is available from work, home, or on the road.

In summary, the medical imaging cloud will provide an improved viewing experience for medical providers, both diagnostic and referring from anywhere on the Internet with a 4-Mb/s connection or better. The combination of remote rendering and virtual desktops enable the medical imaging cloud by lowering the bandwidth requirements for clinical and diagnostic viewing.

OPENING STATEMENT

Fred Prior, PhD Cloud computing has garnered considerable attention and marketing ink as vendors both large and small attempt to position themselves in a new market niche. As it frequently happens in such cases, the concept of cloud computing has become somewhat fuzzy,[5] so before addressing the question of "PACS on a cloud", it is appropriate to identify a few key characteristics of cloud computing as this concept might apply in the medical imaging context.

Cloud computing refers to a provisioning model for virtualized processing and storage capacity.[6] The physical processors and storage systems are housed in large data centers (usually widely distributed) and managed by professional IT organizations. All functionality is provided by web services (grid services if you prefer) accessed via the Internet. Computing capacity, infrastructure, and applications are dynamically provisioned and scheduled with the end user essentially renting capacity on demand.[5] Frequently, this suite of characteristics are summarized by three acronyms: IaaS (Infrastructure as a Service), PaaS (Processing as a Service), and SaaS (Software as a Service).[7] Cloud computing may also be described in terms of privacy and exclusivity along a continuum from widely shared public clouds to restricted access and more secure private clouds with everything in between referred to as some type of hybrid.[8]

From this brief characterization of cloud computing, several critical challenges immediately come to mind when one contemplates migrating a clinical PACS to this type of service-based model. Since the inception of the PACS concept, performance, particularly in terms of image visualization and analysis by a radiologist, has been a key technology driver. PACS, as a cloud service, would demand sufficiently high network bandwidth between the radiologist's client workstation and the relevant cloud service such that two or more screens of full-resolution images are presented in less than 2 s and manipulated in real time. Similarly, the annual image-related data volume produced by an academic medical center is on the order of 10 TB and growing. This means a lot of data will need to be moved to and be retrieved back from cloud storage services over the network. While this level of performance and data handling is routinely managed on a hospital local area network, many institutions lack sufficiently high bandwidth connections to the internet or external service providers to achieve appropriate levels of performance. Taking my own institution as an example, while we have a multi-gigabit internal network backbone, all Internet traffic for the entire university travels over two 1-gigabit connections.

Privacy and security of medical records became a major issue for PACS with the passage of HIPAA and shows every sign of becoming an even more significant issue under the HITECH Act.[9] The covered entity is responsible for ensuring patient privacy and taking appropriate security measures. This responsibility would logically be shared with the cloud service provider under a business associate agreement or similar arrangement. A cloud service provider who supports multiple covered entities would be faced, therefore, with a substantial financial risk. Since privacy and security policies necessary to comply with HIPAA are defined by the covered entity, a cloud service provider might also be faced with multiple and perhaps conflicting security requirements.[10] Certainly, the network bandwidth issues mentioned above would be exacerbated by the additional complexity of ensuring secure data communication between the covered entity and the cloud provider as well as appropriate user authentication and credential management.

Although a patient's medical records are in theory that patient's property, many medical institutions also consider patient records to be business assets. The desire to maintain strict control of these assets may make cloud-based storage difficult for some institutions to accept or, at the very least, add an additional dimension to data privacy and security. When an institution that chose to use a cloud-based storage service eventually made an alternative decision, there would be a strong desire to retrieve all stored data (a substantial undertaking in its own right) and insure that no data is retained by the service provider.

While it may be argued that the technical challenges listed here are surmountable, for a price, it is questionable if the business risks are outweighed by the business gains that, in theory, might be derived from the Cloud Computing model. For many reasons, healthcare IT is a conservative business that traditionally lags the general IT market. A completely outsourced, service-based PACS on a cloud would seem an unlikely near term prospect.

REBUTTAL

James Philbin, PhD I agree that "performance, particularly in terms of image visualization and analysis by a radiologist, has been a key technology driver." As imaging studies continue to increase in size, the most economic way to improve performance is to render the images in a data center, where they can be moved from storage to the render engines over a high bandwidth network and to deliver a low bandwidth "difference stream" to the radiologist viewer. This type of rendering system allows the radiologist to use a broadband connection to view the 2D, 3D, and 4D imaging studies remotely. We believe that a medical imaging cloud, where the edge of the cloud would include some IT equipment near the modalities, will be best suited to provide this type of service.

As far as privacy and security are concerned, a medical cloud using remote rendering and virtual desktops will provide much better security for the data since once the data resides in the data center it would never leave it. Virtual desktop portals have no disk storage, so if they are stolen there is no HIPAA-covered data on the portal. When using diagnostic workstations to view images the HIPAA-covered data resides on the workstation and is much less secure than in a data center with the appropriate security measures.

I also agree with my opponent that for a medical imaging cloud to be viable, it will be necessary to protect the business asset aspect of the medical record. We would expect any medical imaging cloud vendor to prevent any access to patient-identity information, except for the case where the patent is being treated at a healthcare institution. In that case, the patient identity would already be known to the institution requesting the imaging record. The imaging record would be delivered to the requesting institution using that institution's MRN. The cloud company would have to become a trusted partner of all participating institutions and would have to ensure a "level playing field" where all customers' business assets are protected equally, but where the patient's healthcare, in the form of a complete imaging record, comes first.

Finally, while it is true that traditional healthcare IT has been very conservative, that is also the reason that it is, in general, 5 to 10 years behind IT in other industries. If healthcare is to become more productive and less expensive, it will be necessary to adopt new IT technologies much more aggressively than has traditionally been the case. The medical imaging cloud is one of these advances in technology.

REBUTTAL

Fred Prior, PhD A medical imaging cloud based on "IT services from remote or remotely managed third party platforms…" must be cost effective and acceptable to the user community. From the dawn of digital imaging and soft copy reading, image latency has been a critical issue for the user community. User acceptance of image rendering and analysis applications is often driven by, primarily, performance criteria. The concept of remote rendering has gained acceptance for CT/MRI-based volumetric analyses, but it is not clear this technology has been adapted to the high spatial and contrast resolution requirements of digital radiography. It is also unclear that remote rendering will provide sufficiently low display latency for all medical imaging applications when the server must be accessed over the internet. Latency is controlled by the lowest bandwidth pathway in the communication chain. High bandwidth networking in a remote data center cannot overcome the limitations of relatively low bandwidth, shared communication links between an institution and a remote data center. As more image processing functions are ported into low-cost GPUs, will remote rendering remain an attractive option versus real-time local image processing?

Is cloud computing a cost effective model for medical image management? Walker et al.[11] have developed a financial decision model based on differential net present value to study the lease–buy decision for data storage capacity. Their analysis indicates that a cloud-based storage model is cost effective for institutions that store 10 TB per year and must retain this information for up to 9 years. These results suggest that the storage component of a cloud PACS makes financial sense for all but the largest healthcare systems; however, the authors point out that their model does not reflect the opportunity costs resulting from latency. In addition, the model is not specific to medical imaging and so does not reflect costs associated with the shared risk of managing protected health information outside of the covered entity that created that information. Both of these additional costs would tend to weigh the analysis against the cloud storage model.

The core technologies of the cloud computing model are clearly attractive for medical imaging but the fundamental issues are not purely technical in nature. Data latency, data ownership, cost effectiveness, data security issues all must be taken into account. These factors argue against remotely hosted clouds.

REFERENCES

1. http://en.wikipedia.org/wiki/Cloud_computing. Last accessed June 21, 2010

2. Combining local and remote visualization techniques for interactive volume rendering in medical applications. Proceedings of the conference on visualization, Salt Lake City, Utah, USA, pp 449–452, 2000

3. http://www.vmware.com/products/view/. Last accessed June 21, 2010

4. http://www.teradici.com/pcoip/pcoip-technology.php. Last accessed June 21, 2010

5. Qian L, Luo Z, Du Y, Guo L: Cloud computing: an overview. Spring Berlin, Heidelberg, 2009

6. Buyya R, Yeo CS, Venugopal S, Broberg J, Brandic I: Cloud computing and emerging IT platforms: vision, hype, and reality for delivering computing as the 5th utility. Future Generation Computer Systems 25:599–616, 2009

7. Zhu J, et al: IBM cloud computing powering a smarter planet. Springer Berlin, Heidelberg, 2009

8. Introduction to Cloud Computing architecture 1–35, 2009 http://www.scribd.com/doc/17274860/Introduction-to-Cloud-Computing-Architecture. Last accessed June 21, 2010

9. Prior F, Ingeholm ML, Levine BA, Tarbox L: Potential impact of HITECH security regulations on medical imaging. Proc. Engineering in Medicine and Biology Society, 2009 EMBC 2009 Annual International Conference of the IEEE: City

10. Rosenthal A, Mork P, Li MH, Stanford J, Koester D, Reynolds P: Cloud computing: a new business paradigm for biomedical information sharing. Journal of Biomedical Informatics 43:342–353, 2010

11. Walker E, Brisken W, Romney J: To lease or not to lease from storage clouds. Computer 43:44–50, 2010