Cloud 101

Cloud computing is the latest of the sexy buzzwords and has been understood as everything from data hosting services, IT “outsourcing”, to Apple’s iCloud or even Facebook. In many ways it is all of the above, but the national Institute of Standards and Technology (NIST) has defined it as:

“A model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.”

All this means is that instead of having all of your hardware and software sitting on the desk in front of you or within your company's network, it is provided to you as a service by another company accessed via the internet and you have the ability to add or remove workstations or servers on this network.

If you’re reading this article, you’re probably using the cloud already! Cloud-based services such as Gmail and Hotmail have been in widespread use for a decade. Social-media sites including Facebook and MySpace are also Cloud-based services that tens of millions of people have adopted and even use on a daily basis.
FLAVORS OF THE CLOUD

Cloud computing encompasses a broad cross-section of offerings and levels of security while maintaining five essential: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. To best understand the risks one must drill down into the concepts that fuel this industry buzz. Generally speaking, the broad understanding of the Cloud is “anything as a service” or XaaS, but there are three primary offerings that are of most interest to corporations today: Cloud software as a service (SaaS), Cloud platform as a service (PaaS), and Cloud infrastructure as a service (IaaS).

Fig. 2 Offerings within the Cloud

INFRASTRUCTURE AS A SERVICE (IAAS): HOSTING
This offering is a pay-as-you go method of accessing a third party’s raw computer hardware via the net. An example would be Amazon’s EC3 servers and storage utilized by Wikileaks, Northrop and countless other fortune 1,000 companies. In the truest sense of the word, this is what Greunberger and Mccarthy envisioned as utility computing. Another example of IaaS is the simple act of web-hosting where your company pays a per/GB to have a third party hosting company serve up your website’s files from their servers.

PLATFORM AS A SERVICE (PAAS): BUILDING
For this Cloud offering, a company uses a third party’s infrastructure and web-based tools to run systems and software/hardware necessary to develop applications. A simple example of PaaS in use is using a third party to run the shopping cart, checkout, and payment mechanism for a company’s ecommerce site. Force.com (from salesforce.com) and the Google App Engine are also examples of PaaS.
SOFTWARE AS A SERVICE (SAAS): DOING
The most inclusive offering in the Cloud space is Saas, here a company uses a complete application running on a third party’s system. G-Mail, Salesforce.com and Google Documents are perhaps the best-known examples but the options in the SaaS universe are extremely diverse. Additionally, companies are outsourcing their email, VoIP, messaging, and document management systems to SaaS providers. See fig 2.

CLOUD DEPLOYMENT OPTIONS

The primary service models highlighted above, SaaS, PaaS, and IaaS, offer different types of service management operations and utilize different entry points into the Cloud, which in turn creates differing areas of vulnerability for the data housed within the Cloud. As such, it is important to consider the impact of Cloud service models on security design and implementation. A common statement among professionals that work in the Cyber Security space is that data security is inversely proportional to accessibility, and this is especially true in the Cloud. One way to address this concern is to carefully select which deployment method best matches your company’s risk profile and infrastructure resources. Private Cloud, Community Cloud, Public Cloud, and Hybrid Cloud each offer different amounts of proprietary control over data and the greater the control the greater the cost for a company to implement.

PRIVATE CLOUD
A Private Cloud is dedicated to one consumer organization using exclusively company owned and managed systems for all operation or a combination of private and third party provided. Workload isolation is less of a security concern in a private cloud than in a public one because there are no other companies sharing these resources. This deployment method removes the need for each individual employee to be hardwired into company hardware and reduces overall expense to a degree without any compromise of data security, but the drawback is a significant cost to build and maintain the infrastructure. An example of this is a company’s web-accessible intranet.

Fig. 3 Private Cloud Example
COMMUNITY CLOUD
In this deployment model, several organizations from a specific community with common concerns (security, compliance, jurisdiction, etc.), share infrastructure that is either internally housed or provided by a third party or housed in a shared data center. The involved companies are able to garner many of the benefits of a Private Cloud without having to fully bear the cost of implementing the technology and human capital necessary to run a Private Cloud. An example of this might be universities linking together to share resources and research.

Fig. 4 Community Cloud Example

PUBLIC CLOUD
Public Cloud describes Cloud computing in the conventional sense; here resources are allocated to the general public on a fine-grained, self-serve basis via the web. This deployment method is the most cost efficient because it reduces infrastructure expense for a company the greatest by moving operational cost for all operations housed in the Cloud to the third party hosting them. As noted above, while this increases accessibility and reduces overall cost, the tradeoff comes in the form of overall security of the data migrated into the cloud. An example of this would be Amazon’s EC2 or Google App engine.

HYBRID
This format of the Cloud is a combination of the Public or Community Cloud with a portion of the Cloud housed on internal company managed infrastructure. This option offers a degree of the benefit in terms of cost containment that is offered by community/public systems without compromising to such a degree of data security and internal data control. An example of this would be Cisco’s Ironport SenderBase Security Network.
GENESIS OF CLOUD COMPUTING

The underlying concept of Cloud Computing in the on demand sense it is being applied today was first foreseen in the 1960s, when John McCarthy opined that "computation may someday be organized as a public utility." Fred Gruenberger also posited in a “Computing Utility” operating computation much like our present day electrical utility, which would allow users to draw computing resources as needed, while only paying for what they actually used. iii The modern-day characteristics of Cloud Computing (on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service) and the comparison to the electricity industry and the use of public, private, government, and community forms, were further analyzed in Douglas Parkhill's 1966 book, The Challenge of the Computer Utility.

So, while the technology may be updated, faster, cheaper and virtualized, at the end of the day, Cloud Computing is still operating like a mainframe core with nodes distributed as a utility, just in a sexier new dress.

IF CLOUD COMPUTING IS JUST LIPSTICK ON THE OLD MAINFRAME MODEL, WHY ARE WE SCARED?

Today we have what our predecessors did not, the internet and a digital universe of 1.2 zetabytes, or 1.2 trillion megabytes.iv The original mainframes were housed in secure, climate controlled rooms only accessible via "Dumb" terminals wired directly into the system with password and physical access requirements, data could only be preserved via printouts and viewed on the monitor. These technical limitations provided for an extremely secure communication network.

As we have progressed technologically and became interconnected via the internet, data could freely flow from machine to machine without regard to physical location. With this data freedom and the ability to virtualize, the scale and potential risk of operating in the Cloud has far outpaced the risks associated with their mainframe predecessors. It is unnerving just how much information is in the net either intentionally or unintentionally. Do a Google search for documents with the word "CONFIDENTIAL" in the title and you will be shocked at the amount of "secure" information is easily accessible. Add to this the fact that data centers are now owned by third parties the reason for some of the discomfort.

WHO’S AFRAID OF THE BIG BAD CLOUD?

Common obstacles to Cloud Computing adoption include security and availability of service as well as regulatory problems within the US and internationally. Consider this, when you click search on Google.com, the data may be accessed by a computer sitting in Hong Kong, London, Tokyo, or LA ; emails can be stored and processed through a server in any remote part of the world, easily accessible from a Web browser, wherever we happen to be. This is both astounding and problematic because a question that was once easily answered has lost clarity; where is your data? When analyzing international data privacy laws application to a set of data in the cloud or determining who has physical control over multiple company’s data for a government investigation, multiple physical locales and jurisdictions may be into play.
The EU Data Protection Directive and U.S. Safe Harbor program may be relevant depending on the interpretation of data locale. Customers in the European Union (EU) contracting with Cloud providers residing outside the EU/EEA have to adhere to the EU regulations on export of personal data. Data may also be exposed to foreign subpoenas and differing data retention requirements.

Accessibility and multi-tenancy also raise significant concerns in the Cloud Computing space, first of all when relying on a third party possibly hosting data from multiple companies, how can you ensure that there is minimum downtime and that data is readily accessible in the event of a subpoena or government investigation. This gets further confused when in the multi-tenant arena when you have company A (in one country) and Company B (in another country) hosting their data in a third country’s data center. Secondly, when operating in the Cloud, the limitations and protections that are in place to prevent cyber snooping or outright hacking (AT&T, Sony) may not be sufficient. Your company must be vigilant about passwords and internal data controls to mitigate this risk, also having an understanding of which other companies are co-located with your vendor will help in the event of a breach.

OPTING OUT IS NOT AN OPTION, NOW WHAT?

In the CDW 2011 Cloud Computing Tracking Poll, 84% of the 1200 IT professionals stated that their company has one or more applications currently housed in the Cloud with a fairly large percentage confirming that a more inclusive Cloud migration was in the future. Even the US Government has made a move to begin migrating data from their 10,000+ data centers into the Cloud. Each Agency CIO will be required to identify three “must move” services and at least one fully migrate to a Cloud solution within 12 months and the remaining two within 18 months.

Since the train has already figuratively left the station, and operating in the Cloud is a reality, what can a company or individual do to best safeguard their data while benefitting from the cost reduction that migrating away from fully internalized infrastructure and human capital? The first step is to understand what offerings best match the needs of your organization, not all applications, platforms and services should be put into the cloud and in some case it can cost more money, reduce availability, and utility service you are trying to provide.

Who you choose to rely on as a third party (vendor) can make a large impact because not all Cloud Computing providers are created equally. As with the Cloud itself, the vendors offering these solutions also come in many flavors; there are security specific providers, specialized niche providers, low cost solutions, large and small scale providers— and everyone says they can do it all. The Cloud Security Alliance put together an Assessment Initiative Questionnaire to help guide in vetting prospective providers and is a good stating point for your

---

2 12/9/2010, Vivek Kundra , U.S. Chief Information Officer
3 [https://cloudsecurityalliance.org/research/initiatives/consensus-assessments-initiative/](https://cloudsecurityalliance.org/research/initiatives/consensus-assessments-initiative/)
company/firm to develop a specific questionnaire tailored to your company’s needs. Also always ask for references and call those references no matter how big the provider you select.

A company should only look at an expansive migration when they have an understanding of what it wants to get out of migration and a firm understanding of which vendors can best provide those services with minimal risks. Cloud Computing, although based on old concepts has been fundamentally changed by the scale it has grown to via virtualization and the internet. Be sure to do your due diligence and take the proverbial look before you leap onto the Cloud migration train.

CAT CASEY
ACCOUNT EXECUTIVE | HUDSON LEGAL

About the Author
Catherine (Cat) Casey consults with law firms and corporations on the processes and procedures involved with Attorney Document Review. Cat has extensive experience with the full cycle of the EDRM including: E-Discovery processing, early case assessment, litigation preparedness, review staffing and sophisticated project management. Her current focus is on providing cost saving options via solutions that include onshore and major metropolitan area review options and application of a variety of review management strategies and tools. She also offers full cycle case management options and experience based consultation, this includes ensuring compliance with the amended Federal Rules of Civil Procedure and ensuring defensibility. She provides law firms and corporations with cost saving strategies and hands on insight from her many years facilitating and running the attorney review aspects of large scale E-Discovery and hard copy reviews as well as her recent experience spearheading DC based E-Discovery document processing, analyzing and culling with national ESI consulting firms.

Cat has extensive experience working with large multinational corporations and law firms on intensive government investigations, HSR second requests and complex litigations from data collection through final production.

Prior to joining Hudson Legal, Cat served as the Regional Business Development Director for Kelly Law Registry. In this capacity, she consulted with NLJ top 50 firms and fortune 100 Corporations on the most efficient operation, management and implementation of large scale electronic discovery reviews. During her tenure at Kelly Law Registry, she managed and consulted on nearly 100 separate matters including one of the single largest on-going litigation reviews to date.

Cat graduated cum laude from Harvard University with a B.A. in Government and Philosophy and attended Pepperdine School of Law.

3 Fred Gruenberger, Computers and Communications: towards a computer utility
4 IDC