



# Cloud Computing - Overview of Information Assurance Concerns and Opportunities

NSA's Systems and Network Analysis Center,  
Version 1.02 18 December 2009

## Cloud Technology Introduction

Cloud computing is an emerging trend which has progressed to the point of serious adoption in both public and private sector organizations, yet it remains a relatively immature paradigm, one which dictates a revision to the traditional characterization of risk in information technology environments. As a means of an introduction to those changes, this paper offers an overview of the information assurance aspects of cloud computing with a focus on potential security advantages and pitfalls. While many of the security concerns associated with cloud computing are shared with traditional computing models, this paper will focus on those issues unique to cloud computing or that are exacerbated by it. The intended audience is anyone who is considering the adoption of cloud computing and who needs to understand the security risks and potential opportunities cloud computing provides as part of a risk management process.

Cloud computing is an evolving concept and various definitions have been offered, some with widely varying scope. However, boiled down to the basic concepts and simply stated, cloud computing can be described as a style of computing in which dynamically scalable and often virtualized resources are provided as a service over the network.<sup>1</sup> Examples of cloud computing delivery models vary from *infrastructure as a service* (IaaS) where one can lease capabilities such as storage or computing resources (e.g., Amazon Simple Storage Service and Elastic Compute Cloud), *platform as a service* (PaaS) where one can lease an application development environment (e.g., The Microsoft Azure Services Platform) and *software as a service* (SaaS) which offers network based applications (e.g., Facebook, Google docs). The figure at the right illustrates how these various classes of cloud computing offerings build upon one another and offers additional examples from the commercial space.

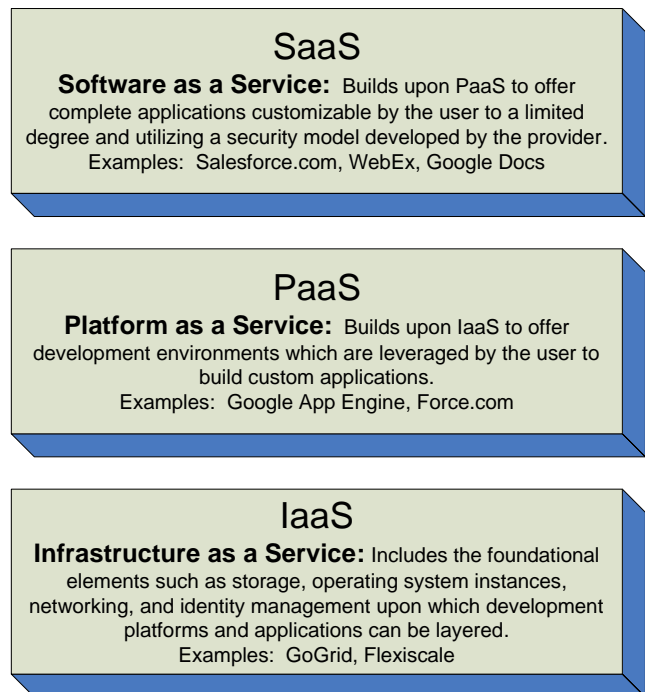


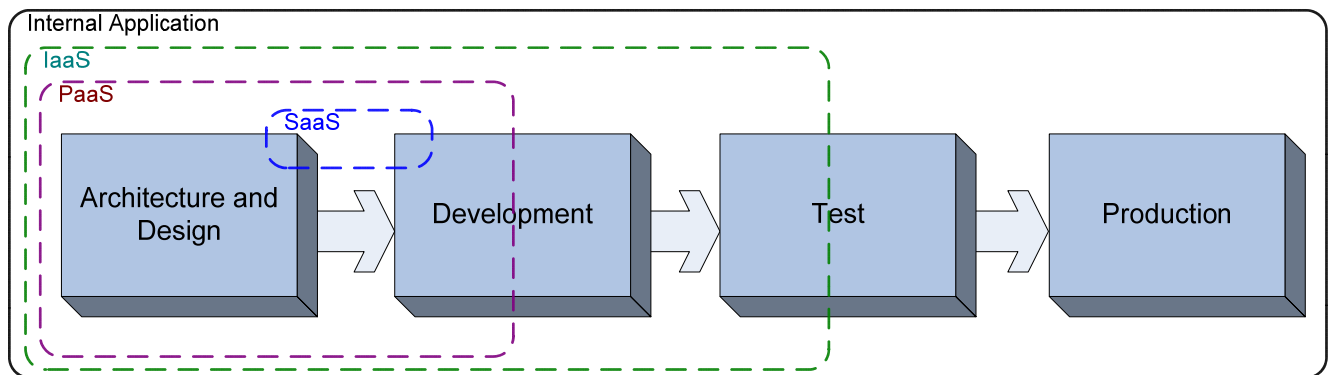
Figure 1: Cloud Service Delivery Models

<sup>1</sup> Derived from [http://en.wikipedia.org/wiki/Cloud\\_computing](http://en.wikipedia.org/wiki/Cloud_computing).

## IA Concerns

When considering the risk associated with cloud computing, the most fundamental element that must be considered is how the cloud environment affects the trust boundary. In thinking about this question, first consider a traditional computing model, one where applications reside on client machines or somewhere else on the infrastructure owned and controlled by the enterprise. In this environment it is possible to levy a host of countermeasures to mitigate the security risks that exist in the information technology world. Those countermeasures can include firewalls, data encryption, antivirus solutions, tight access permissions, separation of networks either virtually or physically, and more. Coupled with those technical countermeasures are the use of trusted administrators, trusted application developers, and internal processes which should reflect the value of the network and the data which resides on it. Now consider what happens when the application is moved to a cloud infrastructure provided by an outside provider, one whose business model is typically driven by the provision of a common service to a wide variety of customers. At this point the security of that data is largely a function of the skill, willingness, diligence, and fiscal ability of the provider to protect the data and provide reliable service.

The trust boundary will vary depending on the type of cloud service in question as shown in Figure 2, a presentation adopted from one offered by the Cloud Security Alliance [13]. This illustrates the software development process and notes that for traditional applications which are developed and deployed in-house, the architecture and design, development, testing, and deployment can be accomplished with trusted individuals using tools and processes integral to the enterprise. Certainly risks remain, even outside of the application development process, but the high degree of control and ownership allows a layering of process and technical countermeasures. At the other end of the spectrum, SaaS allows the user very limited control over the application, with customizations typically limited to a narrow set.



**Figure 2: Public Cloud Trust Boundaries**

Due to this issue of the movement of the trust boundary, public clouds (whereby cloud resources are dynamically provisioned over the Internet) represent the greatest challenge from a security perspective. While the specific concerns will vary somewhat depending upon the type of cloud service (IaaS, PaaS, or SaaS) there are some general issues incumbent in all three:

- *Trust Boundary:* Just how far does the trust boundary extend? This can be a lot further than is immediately obvious - for example, a separate provider might be utilized for aspects of the service, as is the case with Facebook applications which can utilize

Amazon Web Services [4, 7] for storage and other services. This notion of utilizing layers of providers is one that has many tentacles, each of which can ensnare a user in ways that are perhaps not immediately obvious. For example, how do the laws in those countries where the data is ultimately stored affect the security of data in the cloud? Do competitors or other adversaries now have easier access to that data by virtue of the country used for physical storage?

- *Access Control:* How is access control within the cloud environment maintained and how are users' various cloud environments isolated from each other? What provision is made for remote administration? At the cloud provider's site, how is administrative access to the infrastructure policed? If the provider is acquired by another company or engages in an alliance that would change the dynamic of this access, would customers be notified and be allowed time to react, perhaps by switching providers?
- *Incident handling:* What are the provider's responsibilities when an intrusion, suspected intrusion, or security vulnerability is noted? How does the move to a cloud infrastructure impact any forensic procedures associated with incident recovery? As an example of the latter, in the event an employee is suspected of violating a company policy or law, or in response to a suspect intrusion, it may be standard practice to immediately create an image of the user's client machine. If that platform exists in the cloud, will that option still be available?
- *The "ilities":* Can the cloud provider offer adequate reliability, availability, and quality of service? The cloud can complicate questions such as availability in ways perhaps wholly unexpected by those accustomed to traditional computing paradigms. Take the case of the FBI's execution of a warrant against a data center, targeting individuals suspected of fraud and confiscating computers related to the suspects, but also housing the digital presence of a dozen other businesses, at least one of which was unable to execute their business [16].
- *Data backup:* Are backups of data and other perishables such as source code and configuration files the responsibility of the provider or the consumer? If the responsibility of the provider, how quickly can one expect data to be recovered? Can the entire image be restored as well as individual files?
- *Data purging:* Do you need a means of ensuring that deleted data is truly deleted and does not remain in an archive? For example, in a cloud application, is there an ability to truly delete an account or is it simply deactivated [6]?
- *Security Management:* Who is responsible for security management issues such as auditing and patch management? This is particularly topical when dealing with situations where security management may be a shared responsibility such as in the case of PaaS where the final installation may be a blend of network elements, operating systems, and tools offered by the cloud provider with a smattering of customer applications riding on top.
- *Provider's Pedigree:* What is the history of the provider with regards to security, incidence response, and availability? While past performance is no guarantee of future behavior, it can be an indicator. Also consider the security related certifications obtained

by the provider - while the value of such certifications can be debated, if their limits are understood they can offer value.

- *Data Rights:* What rights are relinquished to data stored in the cloud? Some user access agreements have given the cloud provider unlimited rights, in perpetuity [14].
- *Accreditation:* What impact does using the cloud have upon the user's ability to obtain necessary accreditations or certifications for their applications? One simple example is storage - in some environments there may be a requirement that certain data types cannot be transmitted or stored overseas.
- *Business Continuity:* What happens if the cloud provider goes out of business or simply decides to exit the business? Will users be given an opportunity to migrate applications and retrieve data before the provider's site goes down? Are users now locked into proprietary formats that hinder that movement to another provider? Do users own any domain names that are used to access data or applications?

Rest assured this is more than a case of paranoia. As more and more data moves to the cloud, the attackers are following, with high profile attacks against several cloud computing sites already in the proverbial history books of the web. References to several real-world examples have been provided at the end of this document [5, 8, 15, 17]. Other proverbial "war stories" include lost photographs when a vendor exited the on-line image storage business, the organization who thought "it was *their* responsibility to do backups", and a site where access control mechanisms have been thwarted repeatedly. In fact, nearly all - if not all - of the issues identified above have real-world examples associated with them.

Unfortunately, in the predator-prey relationship that so aptly characterizes security, the story of the attacker's reaction to cloud computing doesn't end with attacks against the cloud services, but extends to using those services as launching pads for compromising client computers. Their techniques include enticing users to download malicious code, posting links to malicious web sites that have the capability of achieving drive-by downloading attacks, cross-site scripting, and more.

## Countermeasures

So, how does one counter the uncertainty and risk of using public cloud resources? There are a range of options:

- *Limit Use:* Don't use the public cloud for sensitive data. For example, one might limit the data placed on a social networking site to data that one truly intends to be publicly available and not rely on any privacy or data confidentiality features the provider might offer. User training is a key element here.
- *Encryption:* Encrypt data before uploading it to the cloud. This could be a good solution for folks who are looking at the cloud as a means of data storage.
- *Characterize the Vendor:* Attempt to gain confidence in the provider and obtain answers to the security concerns posed by this document and others that may be unique to a situation. The question of enforcement of the expectations one obtains through such

insight is paramount and, while service level agreements and contract mechanisms can play a role, such legal distinctions are well beyond the scope of this document. Note there may be a practical limit to the insight and control one can gain through such means when dealing with providers who are in the business of providing a common service to the masses.

- *Utilize Safe Web Surfing Practices:* Since that attacker's motivation is not focused solely on compromising cloud services, but using those services as a platform for compromising client computers, following safe web surfing practices is paramount. NSA's *Mitigation Monday #2, Defense against Drive-By Downloads* [11] describes technical steps that can be taken to reduce such risks, and US-CERT offers guidelines which also extend into the behavioral aspects of safe web surfing [3].
- *Use Private Clouds:* Avoid, or limit, dependence on public cloud services by utilizing a private cloud. While in a public cloud, the service is open to possible exploitation by the internet community at large, moving to a private cloud has the effect of limiting the threat exposure by restricting access to a much greater degree through layers of protection mechanisms such as firewalls and routing restrictions. Practically speaking, for many organizations a mix of public and private clouds will prove optimal. In essence, organizations might use their risk management and return on investment analysis to choose the most cost effective architecture that meets their security needs.

## IA Opportunities

To security practitioners, this notion of using private clouds - cloud services implemented behind the firewall on the enterprise's networks - eliminate the most perplexing security issues of cloud computing by avoiding the extension of the security boundary that is at the heart of public cloud security issues. Hybrids, which include characteristics of both public and private clouds exist as well, but will not be explored here.

Private clouds are catching on. Security concerns are part of the reason they are chosen over public clouds, but cost is also a consideration as some organizations have concluded the fiscal benefits of using a public cloud disappear in the context of a long term, large scale project - they conclude it's cheaper to roll their own private cloud [2].

From a security perspective, what potential benefits can cloud computing provide, specifically in the context of a private cloud? If it's done right, there are several:

- Manageability may be improved by the consolidation incumbent in moving disparate applications to an enterprise cloud. Some organizations have realized significant simplification of their application space by consolidating their business apps into a much smaller number of cloud assets [2]. Others talk about how they have used the cloud to simplify the application of patches - clone the environment, patch, test, and deploy.

One of the most fundamental steps one needs to take toward securing a network is making certain it is manageable - understanding what is on your network and being able to perform security management. Consolidation and simplification aid manageability and are nice security enablers.

- Auditing and security monitoring may be simplified in this more consolidated environment.
- Scalability, and therefore availability, may be improved. Some of the key tool providers in the cloud computing space advertise a capability to easily add storage and processing capability to the pool of resources available to cloud applications.
- Some aspects of data protection can be simplified. It may be easier to protect data at rest if it exists in a limited number of locations vice being spread out across the enterprise on an untold number of desktop or laptop hard drives.
- It is possible to leverage particular aspects of cloud services to provide some unique security benefit. For example, the DISA RACE cloud infrastructure offers the ability to obtain an operating system image pre-configured to recommended security guidelines [12]. Utilizing such an image can assist developers in ensuring that applications are compatible with securely configured platforms and can help establish that systems used operationally begin in a sound configuration. One can also consider provisioning such images with the proper security tools as appropriate to the intended usage of the platform - that could include everything from code scanning tools for developers to antivirus solutions.

## In Closing

Thoughts on the information assurance impact of cloud computing are continuing to evolve as this technological model matures. The Cloud Security Alliance's *Security Guidelines for Critical Areas of Focus in Cloud Computing* [13] delves much more deeply into many of the issues raised here, representing the consensus thoughts of many experts in the cloud computing and information assurance arenas. It is highly recommended reading.

## References:

1. *Amazon Web Services: Overview of Security Processes.*  
[http://s3.amazonaws.com/aws\\_blog/AWS\\_Security\\_Whitepaper\\_2008\\_09.pdf](http://s3.amazonaws.com/aws_blog/AWS_Security_Whitepaper_2008_09.pdf)
2. *Capturing the Private Cloud.* A description of the fiscal motivations driving some to choose private clouds over public. <http://gcn.com/Articles/2009/07/13/Private-cloud-computing-for-government.aspx>
3. *Cyber Security Tips.* A variety of technical and behavioral guidelines for safe usage of the Internet. <http://www.us-cert.gov/cas/tips/>
4. *Facebook and AWS.* A description of how developers can use Amazon Web Services to build Facebook applications. <http://aws.amazon.com/solutions/featured-partners/facebook/>
5. *Facebook Hit by Five Security Problems in One Week.*  
[http://www.pcworld.com/article/160545/facebook\\_hit\\_by\\_five\\_security\\_problems\\_in\\_one\\_week.html](http://www.pcworld.com/article/160545/facebook_hit_by_five_security_problems_in_one_week.html)
6. *Facebook Needs To Improve Privacy Practices, Investigation Finds.* A look at Facebook security as compared to Canadian privacy laws. [http://www.priv.gc.ca/media/nr-c/2009/nr-c\\_090716\\_e.cfm](http://www.priv.gc.ca/media/nr-c/2009/nr-c_090716_e.cfm)
7. *Hosting Facebook Applications on Amazon EC2.* A tutorial describing how to host a Facebook application utilizing cloud services from Amazon.  
<http://developer.amazonwebservices.com/connect/entry.jspa?entryID=1044>
8. *Imageshack Hacked By Anti-Full Disclosure Movement.* Describes an attack whereby users were redirected to a single image explaining why the site was hacked.  
<http://blogs.zdnet.com/security/?p=3725>
9. *Lawyers Shine Light On Real Cloud Concerns.* A summary of legal issues surrounding the use of cloud computing. [http://news.cnet.com/8301-19413\\_3-10286028-240.html?part=rss&subj=news&tag=2547-1\\_3-0-20](http://news.cnet.com/8301-19413_3-10286028-240.html?part=rss&subj=news&tag=2547-1_3-0-20)
10. *Microsoft's Azure Cloud Platform: A Guide For The Perplexed.* A terse overview of Azure. <http://blogs.zdnet.com/microsoft/?p=1671>
11. *Mitigation Monday #2, Defense against Drive-By Downloads.* A set of guidelines for safer web surfing.  
[http://www.nsa.gov/ia/guidance/security\\_configuration\\_guides/fact\\_sheets.shtml](http://www.nsa.gov/ia/guidance/security_configuration_guides/fact_sheets.shtml)
12. *Rapid Access Computing Environment.* DISA's portal for access to a DoD platform as a service cloud. <http://www.disa.mil/race>

13. *Security Guidelines for Critical Areas of Focus in Cloud Computing.* Cloud Security Alliance. Offers detailed discussions of the security considerations associated with Cloud Computing. <http://www.cloudsecurityalliance.org/guidance/csaguide.pdf>
14. *The Good, Bad, and the Ugly of SaaS Terms of Service, Licenses, and Contracts.* Includes specific excerpts from user agreements dealing with the rights users of software as a service platforms retain - or forfeit - as a condition of using the site. <http://peterlaird.blogspot.com/2008/06/good-bad-and-ugly-of-saas-terms-of.html>
15. *The Twitterhack Is Cloud Computing's Wake-Up Call: Time for Security That Works.* Describes an attack the cloud that resulted in the compromise of sensitive files belonging to Twitter employees. <http://mediamemo.allthingsd.com/20090715/the-twitterhack-is-cloud-computings-wakeup-call-time-for-security-that-works/>
16. *When the FBI Raids a Data Center: A Rare Danger.* A story of how the FBI's execution of a warrant had serious consequence for 3rd parties in a data center. <http://www.itworld.com/legal/67004/when-fbi-raids-data-center-rare-danger>
17. *Why Cloud Computing Needs Security.* Describes the challenges that consolidated cloud computing sites pose for security. <http://gigaom.com/2008/06/10/the-amazon-outage-fortresses-in-the-clouds/>