

What are some of the security issues with respect to cloud computing?

by Gregg Zepp

When we examine computing from the perspective of the cloud computing paradigm, almost every technological facet of it becomes a security issue, the infrastructure, the software, and the platform as a whole. Clouds typically have a single security architecture but have many customers with different demands. [1] Scaling security to meet the demands of a large network of interwoven networked resources causes us to rethink traditional security methods.

First, one needs to consider which part of a cloud computing services is going to be used? [2]

- **Infrastructure as a Service (IaaS)** - Cloud infrastructure services can deliver computer infrastructure, typically a platform virtualization environment as a service. Rather than purchasing servers, software, data center space or network equipment, clients instead buy those resources as a fully outsourced service. The service is typically billed on a utility computing basis and amount of resources consumed (and therefore the cost) will typically reflect the level of activity. It is an evolution of virtual private server offerings.
- **Platform as a Service (PaaS)** - Cloud platform services can deliver a computing platform and/or solution stack as a service, often consuming cloud infrastructure and sustaining cloud applications. It facilitates deployment of applications without the cost and complexity of buying and managing the underlying hardware and software layers.
- **Software as a service (SaaS)** - Cloud application services can deliver software as a service over the Internet, eliminating the need to install and run the application on the customer's own computers and simplifying maintenance and support.

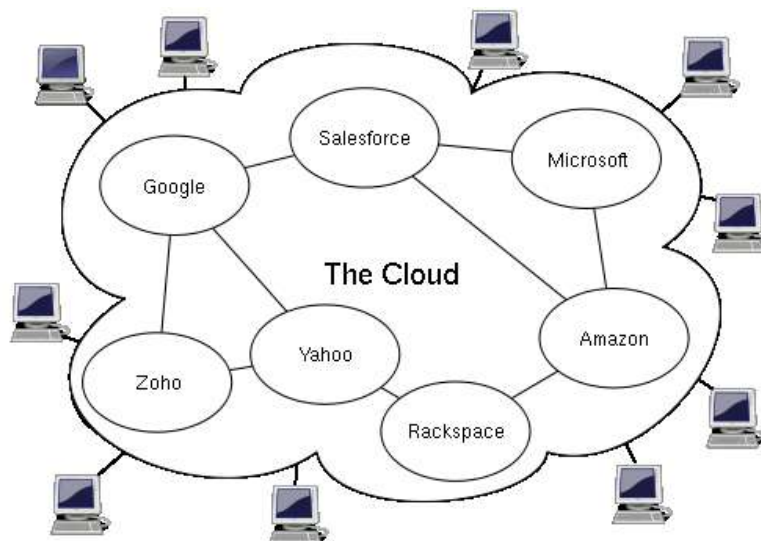


Figure 1 : Cloud Computing [3]

Incident Response Some concerns to consider are: 1) How to scale the incident response program to warn of incidents for the parts of the cloud your organization is responsible for? Or, should just one organization/person be in charge of incident responses for the entire cloud? When something happens, who get's called? An organization will need to understand the incident response strategy for the cloud provider they have chosen. [4]

Application Security The very nature of clouds, their flexibility, public availability, and openness will challenge many in locking their applications when on a cloud. The following is a list of Application Security considerations for cloud programs.

Applications in cloud environments will both impact and be impacted by the following major aspects [5]:

- **Application Security Architecture** –With Cloud Computing, application dependencies can be highly dynamic, even to the point where each dependency represents a discrete third party service provider. Cloud characteristics make configuration management and ongoing provisioning significantly more complex than with traditional application deployment. The environment drives the need for architectural modifications to assure application security.
- **Software Development Life Cycle (SDLC)** – Cloud computing affects all aspects of SDLC, spanning application architecture, design, development, quality assurance, documentation, deployment, management, maintenance, and decommissioning.
- **Compliance** – Compliance clearly affects data, but it also influences applications (for example, regulating how a program implements a particular cryptographic function), platforms (perhaps by prescribing operating system controls and settings) and processes (such as reporting requirements for security incidents).
- **Tools and Services** – Cloud computing introduces a number of new challenges around the tools and services required to build and maintain running applications. These include development and test tools, application management utilities, the coupling to external services, and dependencies on libraries and operating system services, which may originate from cloud providers. Understanding the ramifications of who provides, owns, operates, and assumes responsibility for each of these is fundamental.
- **Vulnerabilities** – These include not only the well-documented—and continuously evolving—vulnerabilities associated with web apps, but also vulnerabilities associated with machine-to-machine Service-Oriented Architecture (SOA) applications, which are increasingly being deployed into the cloud.

As Software as a Service (SaaS) continues to grow, we need to consider how this impacts perimeter security. For example, the more services we stream through traditional firewalls, the more we should consider Application Level Gateways to inspect web services packets for malicious content. One type of this device is called an XML Gateway.

Identity and Access Management User management presents so many challenges. How do we define the trust boundaries? How do we centralize authentication and authorization? Should we? New

security technologies such as the Security Assertion Markup Language (SAML) and the Service Provisioning Markup Language (SPML) and projects interoperability with them are already challenges being faced by many of today's development teams. These challenges will continue to be worked through as the number of projects on clouds grows. [6] Related to this is profile management and encryption of data in rest and in transit.

Data Security and Storage If an organization is using IaaS, then protection of data at rest can be easier. However, PaaS and SaaS presents a challenge as compensating control is not always feasible. Data-at-Rest used by a cloud-based application can be difficult to encrypt because it would prevent indexing or searching of the data.

Privacy Access to data, Compliance, Storage, Retention, Auditing, and Destruction are just a few challenges facing cloud computing vendors. [7] And, much of these depend on laws where the resources physically reside.

Local Law/Jurisdiction Possibly even more pressing an issue than standards in this new frontier is the emerging question of jurisdiction. Data that might be secure in one country may not be secure in another. In many cases though, users of cloud services don't know where their information is held. Currently in the process of trying to harmonize the data laws of its member states, the EU favours very strict protection of privacy, while in America laws such as the US Patriot Act invest government and other agencies with virtually limitless powers to access information including that belonging to companies. [8]

Service Level Agreements One theme continually pointed to in one of our class texts: Cloud Security and Privacy, is the importance in understanding of what is being provided by one's cloud service vendor. Service Level Agreements are part of a service contract where the level of service is formally defined.

In closing, cloud computing presents many challenges in adopting and managing security at the host, network, application, and services level. Just as in other technologies, cloud computing impacts security in various ways. As the CEO, Tim O'Reilly has said, "Everything we think of as a computer today is really just a device that connects to the big computer that we are all collectively building." [9] The internet as a platform will change many parts of our lives, not just security.

-
1. NIST Presentation on Effectively and Securely Using the Cloud Computing Paradigm: <http://csrc.nist.gov/groups/SNS/cloud-computing/>
 2. Cloud Security Alliance: <http://www.cloudsecurityalliance.org/csaguide.pdf>
 3. Wikipedia (image): http://en.wikipedia.org/wiki/File:Cloud_computing.svg
 4. Cloud Security Alliance: <http://www.cloudsecurityalliance.org/csaguide.pdf>
 5. Mather, Tim; Subra Kumaraswamy; Shahed Latif. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Books. 2009.
 6. Mather, Tim; Subra Kumaraswamy; Shahed Latif. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Books. 2009.

7. Mather, Tim; Subra Kumaraswamy; Shahed Latif. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance. O'Reilly Books. 2009.
8. ComputerWeekly.com - Top Five Cloud Computing Security Issues:
<http://www.computerweekly.com/Articles/2010/01/12/235782/Top-five-cloud-computing-security-issues.htm>
9. NIST Presentation on Effectively and Securely Using the Cloud Computing Paradigm:
<http://csrc.nist.gov/groups/SNS/cloud-computing/>