

# What is Special about Cloud Security?

Peter Mell, National Institute of Standards and Technology

## Problem Statement and Background

While cloud security concerns have consistently ranked as one of the top challenges to cloud adoption<sup>1</sup>, it is not clear what security issues are special with respect to cloud computing. To approach this question, we attempt to derive cloud security issues from various cloud definitions and a reference architecture.

The European Network and Information Security Agency (ENISA) defines cloud computing<sup>2</sup> as “an on-demand service model for IT provision, often based on virtualization and distributed computing technologies.” They say that cloud computing architectures have: highly abstracted resources, near instant scalability and flexibility, near instantaneous provisioning, shared resources, service on demand, and programmatic management.

The U.S. National Institute of Standards and Technology’s (NIST) has also published a cloud definition that has been submitted as the U.S. contribution for an International standard<sup>3</sup>. According to the NIST definition, “cloud computing is a model for enabling ubiquitous, 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.”

The NIST definition lists five essential characteristics of cloud computing: on-demand self-service, broad network access, resource pooling, rapid elasticity or expansion, and measured service. It also lists three “service models” (software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS)) and four “deployment models” (private, community, public and hybrid) that together categorize ways to deliver cloud services.

NIST has also published a cloud computing reference architecture<sup>4</sup>. As shown in figure 1, this architecture outlines the five major roles of cloud consumer, produce, broker, auditor, and carrier.

---

<sup>1</sup> An IDC Enterprise Panel survey in August of 2008 to “rate the challenges/issues ascribed to the ‘cloud’/on-demand model” showed that 74.6% of respondents rated security as the top concern.

<sup>2</sup> [www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at\\_download/fullReport](http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport)

<sup>3</sup> <http://www.nist.gov/itl/csd/cloud-102511.cfm>

<sup>4</sup> [http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST\\_SP\\_500-292 - 090611.pdf](http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_SP_500-292_-_090611.pdf)

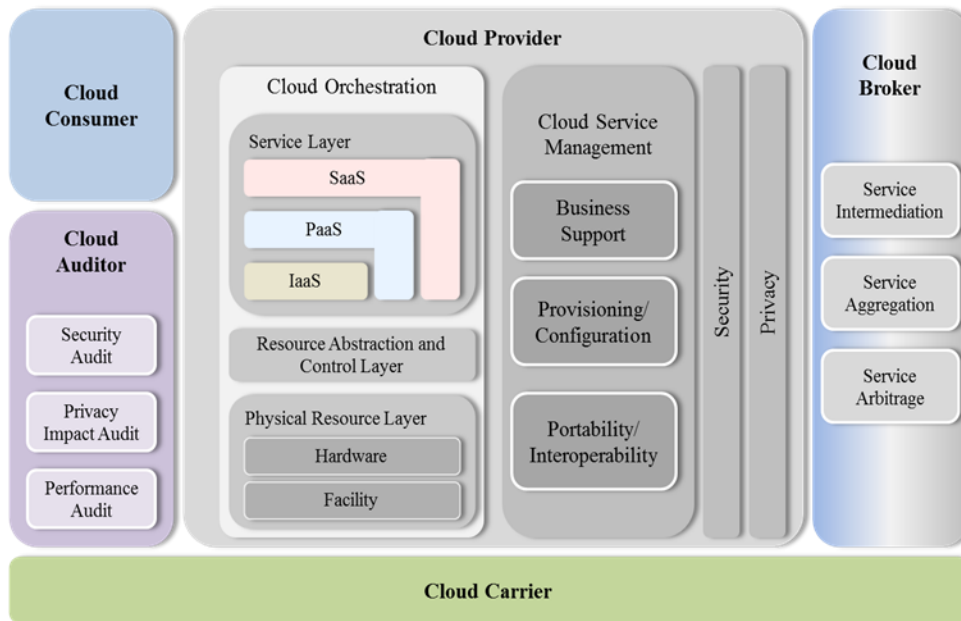


Figure 1. NIST Cloud Computing Reference Architecture

These definitions and reference architecture provide a foundation from which one can begin to analyze cloud security issues. For this article, we want to identify which security issues are special with respect to the cloud computing paradigm.

### Evaluation of Cloud Security Controls

To answer this question, we first look at cloud security controls documented within the Cloud Security Alliance (CSA) security control framework that was informed by both the ENISA and NIST work. The CSA guidance, version 2.1, contains 98 different cloud security controls from 13 domains that are intended to “help evaluate initial cloud risks and inform security decisions<sup>5</sup>.” This body of work would seem to indicate that, based on published cloud definitions, one can identify 98 cloud-specific security controls. However, all 98 controls have been mapped to existing implementation independent security control frameworks<sup>6</sup>. This includes NIST Special Publication 800-53 and the International Organization for Standardization (ISO) 27001-2005. Thus, based on this evaluation, we cannot claim that these security controls are unique with respect to cloud computing since U.S. government and internationally standardized general purpose security controls cover all known CSA cloud security controls. The U.S. government’s Federal Risk and Authorization Management Program<sup>7</sup> (FedRAMP) for cloud computing also uses the NIST cloud definition<sup>8</sup>. Instead of creating new cloud security controls, FedRAMP published

<sup>5</sup> <https://cloudsecurityalliance.org/wp-content/uploads/2011/07/csaguide.v2.1.pdf>

<sup>6</sup> <https://cloudsecurityalliance.org/research/initiatives/ccm/>

<sup>7</sup> <http://www.fedramp.gov>

<sup>8</sup> <http://www.cio.gov/fedrampmemo.pdf> (see footnotes 5 and 6)

a selection of existing general purpose controls from the NIST Special Publication 800-53 security control catalog<sup>9</sup>. Thus, the FedRAMP controls are also generically applicable.

This lack of novel security controls for cloud may arise from the fact that cloud computing is the convergence of many different technology areas including broadband networks, virtualization, grid computing, service orientation, autonomic systems, and Web 2.0<sup>10</sup>. Each of these underlying technology areas have been independently addressed by existing general purpose security controls and so it is logical that the composition of these technology areas can also be addressed by these same general purpose security controls.

However, the cloud paradigm may still present us with security issues that require a novel application of the set of existing general purpose security controls. Evidence for this argument lies in the fact that each CSA cloud security control was mapped to multiple controls from the general purpose control frameworks.

### **Derivation of Cloud Security Issues**

To show the existence of these security issues, we list a sampling of them derived from our initial cloud definitions and reference architecture. Many of the essential cloud characteristics, definitional models, and architectural components suggest cloud security issues:

Cloud Broker: This reference architecture actor implies security composition challenges within composed clouds such as a software as a service built upon an infrastructure as a service.

On-demand: This cloud characteristic suggests security challenges associated with the business user being able to easily and instantly obtain new computing resources that must be pre-secured on delivery.

Resource pooling: This cloud characteristic guides customers towards a 'put all your eggs in one basket' approach that may allow one to concentrate security resources on a single basket but that also heightens the need for backup and resiliency solutions. From a cloud customer perspective, this characteristic reveals the possibility that attacks against one customer may inadvertently affect another customer using the same shared resources.

Service Models: The cloud definition service models reveal challenges with multi-tenancy in a resource pooled environment. All service models have data multi-tenancy while PaaS and IaaS additionally have processing multi-tenancy where user processes might attack each other and the cloud itself.

Infrastructure as a Service: This service model reveals challenges with using virtualization as a front line security defense perimeter to protect against malicious cloud users.

Broad network access: This cloud characteristic shifts the security model to account for possibly untrustworthy client devices that are fully reliant on the network for service.

---

<sup>9</sup> [http://www.gsa.gov/graphics/staffoffices/FedRAMP\\_Security\\_Controls\\_Final.zip](http://www.gsa.gov/graphics/staffoffices/FedRAMP_Security_Controls_Final.zip)

<sup>10</sup> <http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-computing-v26.ppt>, slide 61

Measured service: This cloud characteristic reveals the need to measure cloud usage to promote overall availability of the cloud.

## **Conclusion**

The cloud computing paradigm appears to present special security issues that will require research and careful consideration. At this point, however, these issues do not appear to require completely new security controls but instead the creative application of existing security techniques.

## **Disclaimers**

*Certain products or organizations are identified in this document, but such identification does not imply recommendation by the U.S. National Institute of Standards and Technology (NIST) or other agencies of the U.S. government, nor does it imply that the products or organizations identified are necessarily the best available for the purpose. This paper reflects the author's personal opinions, not the opinions of the Department of Commerce or NIST.*