CS 6393: Cyber Security Models and Systems

Views of Cloud Computing

Ravi Sandhu

L7-1
The Cloud is the Computer
- IEEE Spectrum, 2008

Datacenter as a Computer
- Barroso and Hölzle, 2009

The Network is the Computer
- Sun Microsystems, early 1990s

The Cloud
Cloudwashing

I need you to cloudwash our software.

Move some of its functions onto the Internet, but call the Internet a cloud.

No one will take us seriously unless we’re doing something in the cloud.

Will people take us seriously if we make technology decisions based on jargon?

We don’t care what smart people think. There aren’t that many of them.

We only need to convince our dumb customers.

Dumb people believe anything.

Do you believe I moved our software to the cloud yesterday?

You did?

I’m going to say yes.
The Cloud: Perspectives and Forces

Science

Business

Engineering

World-Leading Research with Real-World Impact!
NIST Cloud Computing 3-4-5 Definition

5 Essential Characteristics

2009-2011
16 versions

3 Service Models

4 Deployment Models
NIST Cloud Computing 3-4-5 Definition

5 Essential Characteristics

2009-2011
16 versions

3 Service Models
Software as a Service (SaaS)
Platform as a Service (PaaS)
Infrastructure as a Service (IaaS)

4 Deployment Models
NIST Cloud Computing 3-4-5 Definition

5 Essential Characteristics

2009-2011
16 versions

3 Service Models
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

4 Deployment Models
- Public
- Private
- Community
- Hybrid
5 Essential Characteristics

- On-demand self service
- Broad network access
- Resource pooling (multi-tenant)
- Rapid elasticity
- Measured service

3 Service Models

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

4 Deployment Models

- Public
- Private
- Community
- Hybrid

© Ravi Sandhu

World-Leading Research with Real-World Impact!
NIST Cloud Computing 3-4-5 Definition

5 Essential Characteristics
- On-demand self service
- Broad network access
- Resource pooling (multi-tenant)
- Rapid elasticity
- Measured service

2009-2011
16 versions

Other Common Characteristics
- Geographic distribution
- Homogeneity
- Resilience
- Massive scale
- Virtualization
- Security

3 Service Models
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

4 Deployment Models
- Public
- Private
- Community
- Hybrid
“We argue that Cloud Computing not only overlaps with Grid Computing, it is indeed evolved out of Grid Computing and relies on Grid Computing as its backbone and infrastructure support.”

I don’t think so
1. Coordinates resources that are not subject to centralized control
   - Virtual Organization (VO)
2. Uses standard, open, general-purpose protocols and interfaces
   - Globus toolkit
3. Delivers non-trivial qualities of service
Grid versus Cloud

Grid

1. Coordinates resources that are not subject to centralized control
   - Virtual Organization (VO)
2. Uses standard, open, general-purpose protocols and interfaces
   - Globus toolkit
3. Delivers non-trivial qualities of service
   - Yes

Cloud

- On-demand self service
- Broad network access
- Resource pooling (multi-tenant)
- Rapid elasticity
- Measured service

- Geographic distribution
- Homogeneity
- Resilience
- Massive scale
- Virtualization
- Security

No but VOs may be enabled on demand
No but standard opensource software and APIs may emerge (OpenStack is the current contender)
### Grid versus Cloud Drivers

<table>
<thead>
<tr>
<th>Cloud</th>
<th>Grid</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commercially developed</td>
<td>DoD funded, no commercial traction</td>
</tr>
<tr>
<td>Little or no academic input</td>
<td>Mainly academic driven</td>
</tr>
<tr>
<td>Pay-per-use</td>
<td>Pay-per-seat (one-time payment)</td>
</tr>
<tr>
<td>Payment driven</td>
<td>Project oriented, proposal driven</td>
</tr>
<tr>
<td>Centrally owned hardware</td>
<td>Multiply owned hardware</td>
</tr>
<tr>
<td>Centrally scheduled</td>
<td>Distributed scheduling</td>
</tr>
<tr>
<td>Single point of trust</td>
<td>Multiple trust points</td>
</tr>
<tr>
<td>Simple security</td>
<td>Complex PKI based security</td>
</tr>
<tr>
<td>Interactive</td>
<td>Batch</td>
</tr>
<tr>
<td>Commodity computing</td>
<td>High performance computing</td>
</tr>
<tr>
<td>Small and medium businesses</td>
<td>High end organizations</td>
</tr>
<tr>
<td>Virtualization essential</td>
<td>Virtualization often not used</td>
</tr>
<tr>
<td>Not so predictable performance</td>
<td>Predictable performance</td>
</tr>
</tbody>
</table>
The triangle model of next-generation Internet Computing
Figure 1. Users and providers of cloud computing. We focus on cloud computing’s effects on cloud providers and SaaS providers/cloud users. The top level can be recursive, in that SaaS providers can also be a SaaS users via mashups.
Not IaaS or PaaS but classes of utility computing
### Table 1. Comparing public clouds and private data centers.

<table>
<thead>
<tr>
<th>Advantage</th>
<th>Public Cloud</th>
<th>Conventional Data Center</th>
</tr>
</thead>
<tbody>
<tr>
<td>Appearance of infinite computing resources on demand</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Elimination of an up-front commitment by Cloud users</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Ability to pay for use of computing resources on a short-term basis as needed</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Economies of scale due to very large data centers</td>
<td>Yes</td>
<td>Usually not</td>
</tr>
<tr>
<td>Higher utilization by multiplexing of workloads from different organizations</td>
<td>Yes</td>
<td>Depends on company size</td>
</tr>
<tr>
<td>Simplify operation and increase utilization via resource virtualization</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
## Table 2. Top 10 obstacles to and opportunities for growth of cloud computing.

<table>
<thead>
<tr>
<th>Obstacle</th>
<th>Opportunity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability/Business Continuity</td>
<td>Use Multiple Cloud Providers</td>
</tr>
<tr>
<td>Data Lock-In</td>
<td>Standardize APIs; Compatible SW to enable Surge or Hybrid Cloud Computing</td>
</tr>
<tr>
<td>Data Confidentiality and Auditability</td>
<td>Deploy Encryption, VLANs, Firewalls</td>
</tr>
<tr>
<td>Data Transfer Bottlenecks</td>
<td>FedExing Disks; Higher BW Switches</td>
</tr>
<tr>
<td>Performance Unpredictability</td>
<td>Improved VM Support; Flash Memory; Gang Schedule VMs</td>
</tr>
<tr>
<td>Scalable Storage</td>
<td>Invent Scalable Store</td>
</tr>
<tr>
<td>Bugs in Large Distributed Systems</td>
<td>Invent Debugger that relies on Distributed VMs</td>
</tr>
<tr>
<td>Scaling Quickly</td>
<td>Invent Auto-Scaler that relies on ML; Snapshots for Conservation</td>
</tr>
<tr>
<td>Reputation Fate Sharing</td>
<td>Offer reputation-guarding services like those for email</td>
</tr>
<tr>
<td>Software Licensing</td>
<td>Pay-for-use licenses</td>
</tr>
</tbody>
</table>
Cyber Security: What is Different in the Cloud?

Risk = \( f \) (Threats, Vulnerabilities, Impact)

Threats

Vulnerabilities

Impact
Cyber Security: What is Different in the Cloud?

- Multi-Tenancy
- Security and Privacy
- Compliance and Forensics
- Cloud Service Provider