Cloud Computing: Opportunities, Challenges, and Solutions

Jungwoo Ryoo, Ph.D., CISSP, CISA
The Pennsylvania State University
What is ‘cloud computing’?

• What are some of the keywords?

• How many of you cannot think of anything?
Essential Characteristics

• Rapid provisioning

• Minimal
  o Management effort
  o Service provider interaction

• Scalability but
  o Multi-tenancy
Essential Characteristics II

- On-demand self-service
- Rapid elasticity
- Broad network access
- Measured service
  - Metering
- Resource pooling
What is ‘cloud computing?’

- A Model for enabling
  - Ubiquitous
  - Convenient
  - On-demand **network** access to
    - A shared pool of **configurable** computing resources

Source: SP 800-145 by National Institute of Standards and Technology (NIST), 2011
Types of Clouds According to Uses

- **Software as a Service**
  - SaaS

- **Platform as a Service**
  - PaaS

- **Infrastructure as a Service**
  - IaaS
Types of Clouds

• Public cloud
• Private cloud
• Community cloud
The Bad News

- Many of the characteristics that make cloud computing **great** also

  - Make it **less secure**

  - Present extra **security challenges**
The Bad News II

• Problems

  o Countermeasures
    ▪ Traditional security controls are ineffective

  o Evaluation of the security of cloud services
    ▪ Conventional security auditing approaches are insufficient
Goals

• Security challenges specific to cloud computing

• What is available for cloud security
  o Standards
  o Technologies

• Guidance for Cloud Service Users (CSUs)
  o What to look out for
Cloud Security

Challenges
Root Causes

• **Scale**
  - The sheer number of VMs

• **Scope**
  - New types of technologies
    - Security of hypervisors
  - Intangible and logical
    - Virtual switches
    - Virtual routers
Root Causes

• Complexity → more time and resources to properly manage security
  o Scale + scope
  o Third-party involvement
  o Colocation via multi-tenancy
  o Cross-border concerns → the importance of physical location of data
    ▪ Compliance requirements for varying laws and regulations
Financial Industry-Specific Causes

• More end user traffic
  o Online banking

• Diversity of devices
  o PC, mobile, tablet, etc.

• Various network types
  o Public Wi-Fi, 4G, etc.
More Stringent Requirements

• Availability
  o 24/7

• Accessibility
  o End user-driven access control

• Confidentiality
  o Encryption
Bottom Line

- Knowing what to look for is critical!
  - In addition to the traditional IT security checklist
Transparency

• Quality of Service (QoS) information
  o Availability?

• Incidents
• Certifications
• Policies
• Controls
Transparency II

• Subcontractors

• Location of data

• Privacy
  o Government surveillance

• Legal and liability issues
  o For example, service outages
Transparency III

• Does the contract or Service-Level Agreement (SLA) include a transparency clause?

• Proper propagation of risk knowledge is the key!
Encryption

• Who encrypts the data?
  o CSU
  o CSP
    ▪ By default (e.g., Amazon S3)
  o Third party encryption service

• Who keeps the key?

• How much to encrypt?
Encryption II

- Tradeoffs
  - Security vs. cost
    - Fully homomorphic encryption
  - Security vs. usability
  - Security vs. performance
  - Security vs. complications associated with external auditing efforts
Colocation

- Sharing → cost savings but ...
- Sharing → more security vulnerabilities
  - Access to the physical hardware
    - Especially, in the context of IaaS
  - Hypervisor vulnerabilities
    - Xen, VMWare, virtual server, Kernel-based Virtual Machines (KVM), PowerVM, etc.
Colocation II

• Countermeasures
  
  o Proper cloud segmentation environments
    
    ▪ Separate physical servers
    
    ▪ Dedicated virtual servers
    
    ▪ Logical partitions and separate database servers on the same VM without sharing a disk storage
Cloud Security

Solutions
The Good News

• Newly emerging **standards and guidelines** to **evaluate** CSPs
  o How well they are dealing with
    ▪ Cloud-specific security challenges
# Cloud Security Standards

<table>
<thead>
<tr>
<th>Standards</th>
<th>Type</th>
<th>Strength</th>
<th>Sponsoring Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOC</td>
<td>Audit for outsourced services</td>
<td>Technology-neutral</td>
<td>AICPA</td>
</tr>
<tr>
<td>ISO/IEC 27017</td>
<td>Cloud-specific</td>
<td>Technology-neutral</td>
<td>ISO</td>
</tr>
<tr>
<td>NIST 800-144</td>
<td>Cloud-specific</td>
<td>Technology-neutral</td>
<td>NIST</td>
</tr>
<tr>
<td>Cloud Security Alliance</td>
<td>Cloud-specific</td>
<td>Dedicated to cloud security auditing</td>
<td>CSA</td>
</tr>
<tr>
<td>PCI-DSS</td>
<td>PCI-qualified security assessor cloud supplement</td>
<td>Technology-neutral but still providing guidance</td>
<td>PCI-DSS</td>
</tr>
</tbody>
</table>
Additional Reading

Any Questions?

- **Contact information**
  - jryoo@psu.edu