

Effectively and Securely Using the Cloud Computing Paradigm

Peter Mell,

NIST, Information Technology Laboratory

4-28-2009



NIST Cloud Research Team



Peter Mell
Project Lead

Lee Badger

Erika McCallister

Tim Grance
Program Manager

Karen Scarfone

**Contact information is available from:
http://www.nist.gov/public_affairs/contact.htm**

Caveats and Disclaimers

- This presentation provides education on cloud technology and its benefits to set up a discussion of cloud security
- It is NOT intended to provide official NIST guidance and NIST does not make policy
- Any mention of a vendor or product is NOT an endorsement or recommendation

Citation Note: All sources for the material in this presentation are included within the Powerpoint “notes” field on each slide

A Working Definition of Cloud Computing

- Cloud computing is a pay-per-use model for enabling available, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.
- This cloud model promotes availability and is comprised of five **key characteristics**, three **delivery models**, and four **deployment models**.

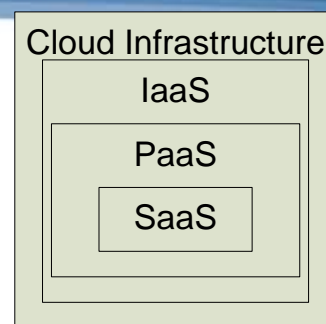
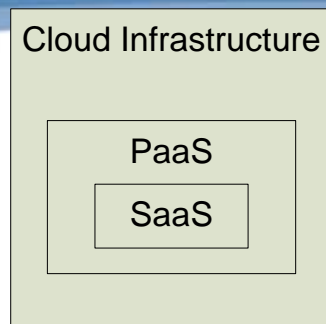
5 Key Cloud Characteristics

- On-demand self-service
- Ubiquitous network access
- Location independent resource pooling
- Rapid elasticity
- Pay per use

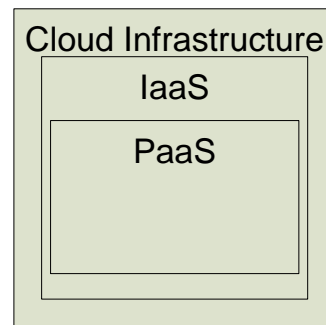
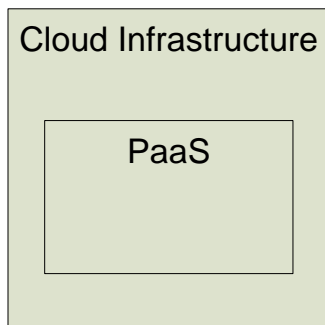
3 Cloud Delivery Models

- Cloud Software as a Service (SaaS)
 - Use provider's applications over a network
- Cloud Platform as a Service (PaaS)
 - Deploy customer-created applications to a cloud
- Cloud Infrastructure as a Service (IaaS)
 - Rent processing, storage, network capacity, and other fundamental computing resources
- To be considered “cloud” they must be deployed on top of cloud infrastructure that has the key characteristics

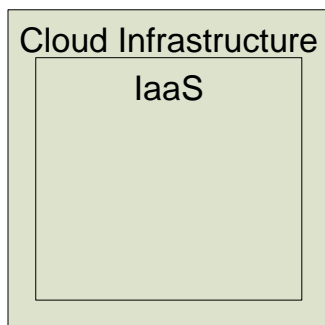
Delivery Model Architectures



Software as a Service
(SaaS)
Architectures



Platform as a Service (PaaS)
Architectures



Infrastructure as a Service (IaaS)
Architectures

4 Cloud Deployment Models

- Private cloud
 - enterprise owned or leased
- Community cloud
 - shared infrastructure for specific community
- Public cloud
 - Sold to the public, mega-scale infrastructure
- Hybrid cloud
 - composition of two or more clouds
- Two types: internal and external

Common Cloud Characteristics

- Cloud computing often leverages:
 - Massive scale
 - Virtualization
 - Free software
 - Autonomic computing
 - Multi-tenancy
 - Geographically distributed systems
 - Advanced security technologies
 - Service oriented software

Planned NIST Cloud Computing Publication



- NIST is planning a series of publications on cloud computing
- NIST Special Publication to be created in FY09
 - What problems does cloud computing solve?
 - What are the technical characteristics of cloud computing?
 - How can we best leverage cloud computing and obtain security?

Analyzing Cloud Security

- Some key issues:
 - trust, multi-tenancy, encryption, compliance
- Clouds are massively **complex systems** can be reduced to **simple primitives** that are replicated thousands of times and **common functional units**
- Cloud security is a tractable problem
 - There are both advantages and challenges

Former Intel CEO, Andy Grove: “only the paranoid survive”



General Security Advantages

- Shifting public data to a external cloud reduces the exposure of the internal sensitive data
- Cloud homogeneity makes security auditing/testing simpler
- Clouds enable automated security management
- Redundancy / Disaster Recovery



General Security Challenges

- Trusting vendor's security model
- Customer inability to respond to audit findings
- Obtaining support for investigations
- Indirect administrator accountability
- Proprietary implementations can't be examined
- Loss of physical control

Security Relevant Cloud Components

- Cloud Provisioning Services
- Cloud Data Storage Services
- Cloud Processing Infrastructure
- Cloud Support Services
- Cloud Network and Perimeter Security

- Elastic Elements: Storage, Processing, and Virtual Networks

Provisioning Service

- Advantages
 - Rapid reconstitution of services
 - Enables availability
 - Provision in multiple data centers / multiple instances
 - Advanced honey net capabilities
- Challenges
 - Impact of compromising the provisioning service

Data Storage Services

- Advantages
 - Data fragmentation and dispersal
 - Automated replication
 - Provision of data zones (e.g., by country)
 - Encryption at rest and in transit
 - Automated data retention
- Challenges
 - Isolation management / data multi-tenancy
 - Storage controller
 - Single point of failure / compromise?
 - Exposure of data to foreign governments

Cloud Processing Infrastructure

- Advantages
 - Ability to secure masters and push out secure images
- Challenges
 - Application multi-tenancy
 - Reliance on hypervisors
 - Process isolation / Application sandboxes

Cloud Support Services

- Advantages
 - On demand security controls (e.g., authentication, logging, firewalls...)
- Challenges
 - Additional risk when integrated with customer applications
 - Needs certification and accreditation as a separate application
 - Code updates

Cloud Network and Perimeter Security

- Advantages
 - Distributed denial of service protection
 - VLAN capabilities
 - Perimeter security (IDS, firewall, authentication)
- Challenges
 - Virtual zoning with application mobility

Cloud Security Advantages

Part 1



- Data Fragmentation and Dispersal
- Dedicated Security Team
- Greater Investment in Security Infrastructure
- Fault Tolerance and Reliability
- Greater Resiliency
- Hypervisor Protection Against Network Attacks
- Possible Reduction of C&A Activities (Access to Pre-Accredited Clouds)

Cloud Security Advantages

Part 2



- Simplification of Compliance Analysis
- Data Held by Unbiased Party (cloud vendor assertion)
- Low-Cost Disaster Recovery and Data Storage Solutions
- On-Demand Security Controls
- Real-Time Detection of System Tampering
- Rapid Re-Constitution of Services
- Advanced Honeynet Capabilities

Cloud Security Challenges

Part 1



- Data dispersal and international privacy laws
 - EU Data Protection Directive and U.S. Safe Harbor program
 - Exposure of data to foreign government and data subpoenas
 - Data retention issues
- Need for isolation management
- Multi-tenancy
- Logging challenges
- Data ownership issues
- Quality of service guarantees

Cloud Security Challenges

Part 2



- Dependence on secure hypervisors
- Attraction to hackers (high value target)
- Security of virtual OSs in the cloud
- Possibility for massive outages
- Encryption needs for cloud computing
 - Encrypting access to the cloud resource control interface
 - Encrypting administrative access to OS instances
 - Encrypting access to applications
 - Encrypting application data at rest
- Public cloud vs internal cloud security
- Lack of public SaaS version control



Additional Issues

- Issues with moving PII and sensitive data to the cloud
 - Privacy impact assessments
- Using SLAs to obtain cloud security
 - Suggested requirements for cloud SLAs
 - Issues with cloud forensics
- Contingency planning and disaster recovery for cloud implementations
- Handling compliance
 - FISMA
 - HIPAA
 - SOX
 - PCI
 - SAS 70 Audits

Migration Paths for Cloud Adoption

- Use public clouds
 - Option 1: as is with multi-tenancy
 - Option 2: no multi-tenancy of servers or storage + enhanced organization defined security
- Develop private clouds
 - Procure an external private cloud
 - Migrate data centers to be private clouds (fully virtualized)
- Use hybrid-cloud technology
 - Leverage a private and public cloud architectures
 - Workload portability between private and public clouds
- Build or procure community clouds

Possible Effects of Cloud Computing



- Small enterprises use public SaaS and public clouds and minimize growth of data centers
- Large enterprise data centers may evolve to act as internal clouds
- Large enterprises may use hybrid cloud infrastructure software to leverage both internal and public clouds
- Public clouds may adopt standards in order to run workloads from competing hybrid cloud infrastructures

A proposal: The Cloud Interoperability Profile

- We need to define minimal standards
 - Enable cloud integration, application portability, and data portability
 - Avoid over specification that will inhibit innovation
- Let's create a blueprint for cloud design
 - Specifies versions of standards
 - Separately addresses different cloud models
- Example: WS-I Basic Profile for SOA
- Let's call it the "Cloud Interoperability Profile (CIP)" (pronounced 'sip')

Strategies for Enabling Effective Migration

- Provide guidance on secure and effective use
- Research cloud standards
- Create a cloud interoperability profile

Service Level Agreements (SLAs)

- Contract between customers and service providers of the level of service to be provided
- Contains performance metrics (e.g., uptime, throughput, response time)
- Problem management details
- Documented security capabilities
- Contains penalties for non-performance