

# Effectively and Securely Using the Cloud Computing Paradigm

Peter Mell, Tim Grance

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](http://www.nist.gov/public_affairs/contact.htm)**

# 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**.

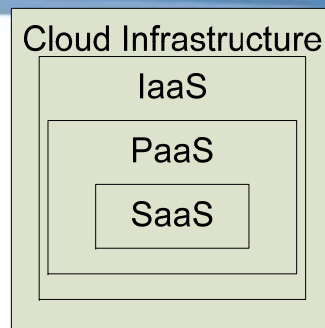
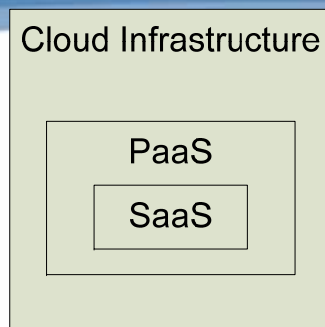
# 5 Key Cloud Characteristics

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

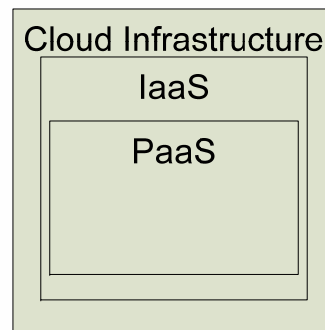
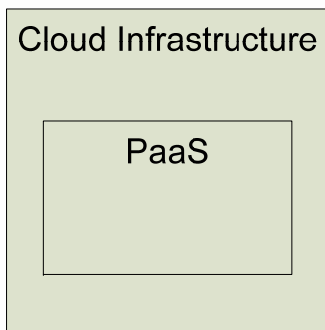
# 3 Cloud Delivery Models

- 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

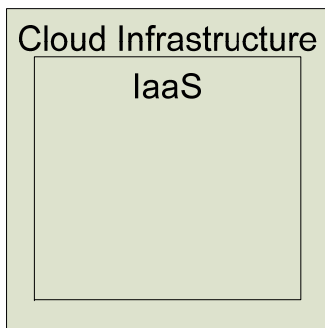
# Delivery Model Architectures



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

# Cloud Computing Publications



# 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?

# Cloud Computing 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

# Questions?

- Peter Mell
- NIST, Information Technology Laboratory
- Computer Security Division
  
- Tim Grance
- NIST, Information Technology Laboratory
- Computer Security Division

Contact information is available from:  
[http://www.nist.gov/public\\_affairs/contact.htm](http://www.nist.gov/public_affairs/contact.htm)