

Effectively and Securely Using the Cloud Computing Paradigm

Peter Mell, Tim Grance

NIST, Information Technology Laboratory

8-12-2009



A Working Definition of Cloud Computing

- Cloud computing is a model for enabling 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.
- This cloud model promotes availability and is composed of five essential **characteristics**, three **service models**, and four **deployment models**.

5 Essential Cloud Characteristics

- On-demand self-service
- Ubiquitous network access
- Resource pooling
 - Location independence
 - Homogeneity
- Rapid elasticity
- Measured service

3 Cloud Service 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

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

Common Cloud Characteristics

- Cloud computing often leverages:
 - Massive scale
 - Virtualization
 - Non-stop computing
 - Free software
 - Geographic distribution
 - Service oriented software
 - Autonomic computing
 - Advanced security technologies

Secure Migration Paths for Cloud Computing



The 'Why' and 'How' of Cloud Migration

- There are many benefits that explain **why** to migrate to clouds
 - Cost savings, power savings, green savings, increased agility in software deployment
- Cloud security issues may drive and define **how** we adopt and deploy cloud computing solutions

Balancing Threat Exposure and Cost Effectiveness

- Private clouds may have less **threat exposure** than community clouds which have less threat exposure than public clouds.
- Massive public clouds may be more **cost effective** than large community clouds which may be more cost effective than small private clouds.
- *Doesn't strong security controls mean that I can adopt the most cost effective approach?*

Cloud Migration and Cloud Security Architectures

- Clouds typically have a single security architecture but have many customers with different demands
 - Clouds should attempt to provide configurable security mechanisms
- Organizations have more control over the security architecture of private clouds followed by community and then public
 - This doesn't say anything about actual security
- Higher sensitivity data is likely to be processed on clouds where organizations have control over the security model

Putting it Together

- Most clouds will require very strong security controls
- All models of cloud may be used for differing tradeoffs between threat exposure and efficiency
- There is no one “cloud”. There are many models and architectures.
- How does one choose?

Migration Paths for Cloud Adoption

- Use public clouds
- Develop private clouds
 - Build a private cloud
 - Procure an outsourced private cloud
 - Migrate data centers to be private clouds (fully virtualized)
- Build or procure community clouds
 - Organization wide SaaS
 - PaaS and IaaS
 - Disaster recovery for private clouds
- Use hybrid-cloud technology
 - Workload portability between clouds

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