

Cloud Computing Paradigm

Peter Mell, Tim Grance

NIST, Information Technology Laboratory

9-17-2009



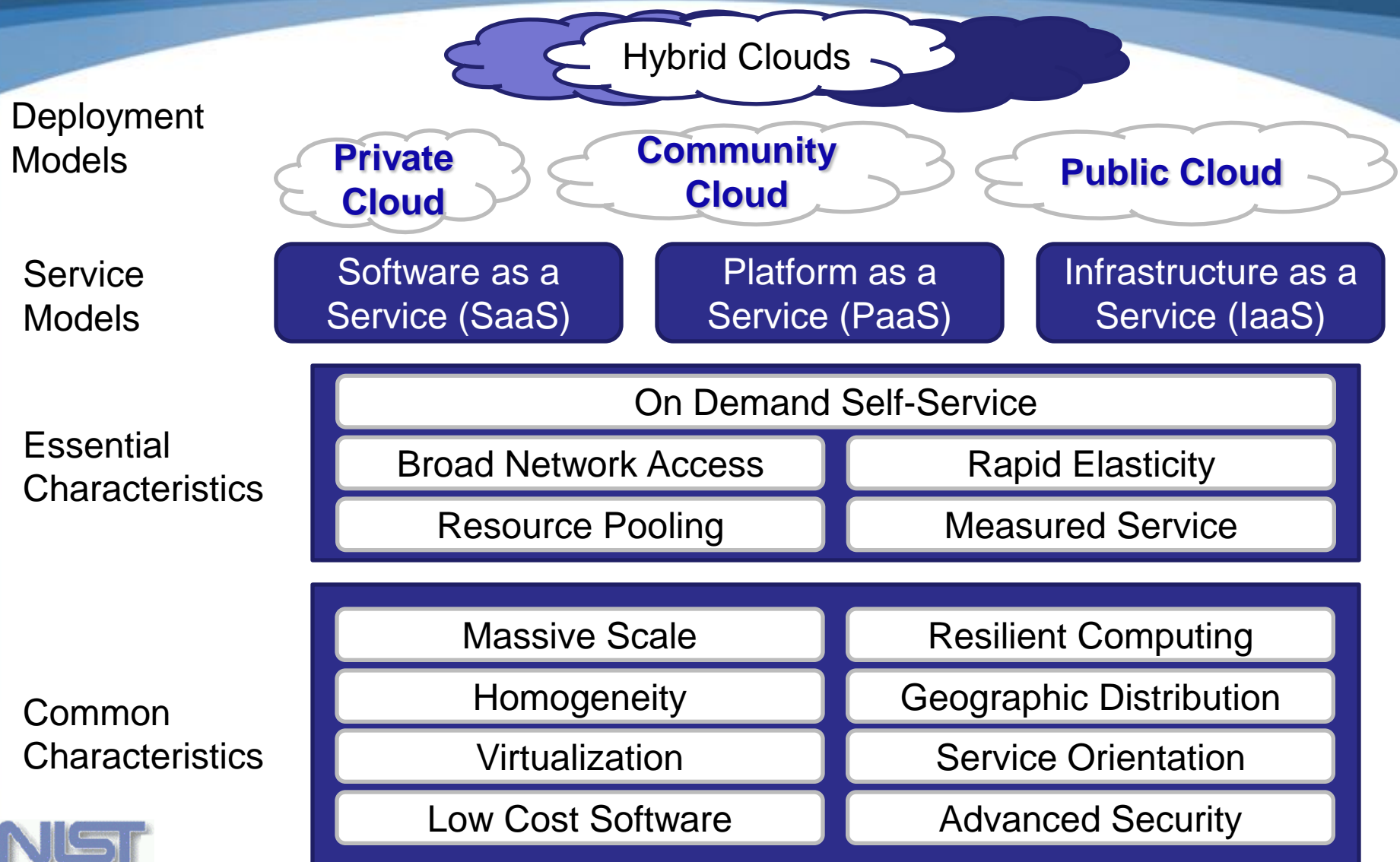
Caveats and Disclaimers

- This presentation provides education on cloud technology and its benefits to set up a discussion of cloud security
- Looking for feedback on NIST role and ideas presented
- 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

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**.

The NIST Cloud Definition Framework



Cloud Standards Vision

- Provide advice to industry and government for the creation and management of relevant cloud computing standards allowing all parties to gain the maximum value from cloud computing

NIST and Standards



- Promote cloud standards:
 - Propose roadmaps
 - Act as a catalyst
 - Promote adoption of cloud standards

Cloud Standards Ideas

- Fungible clouds
 - (mutual substitution of services)
 - Data and customer application portability
 - Common interfaces, semantics, programming models
 - Federated security services
 - Vendors compete on effective implementations
- Enable and foster value add on services
 - Advanced technology
 - Vendors compete on innovative capabilities

A proposal: Standards Roadmap



- We need to define minimal standards
 - Enable secure cloud integration, application portability, and data portability
 - Avoid over specification that will inhibit innovation
 - Separately addresses different cloud models

Towards the Creation of a Roadmap (I)

- Thoughts on standards:
 - Usually more service lock-in as you move up the SPI stack (IaaS->PaaS->SaaS)
 - IaaS is a natural transition point from traditional enterprise datacenters
 - Base service is typically computation, storage, and networking
 - The virtual machine is the best focal point for fungibility
 - Security and data privacy concerns are the two critical barriers to adopting cloud computing

Towards the Creation of a Roadmap (II)

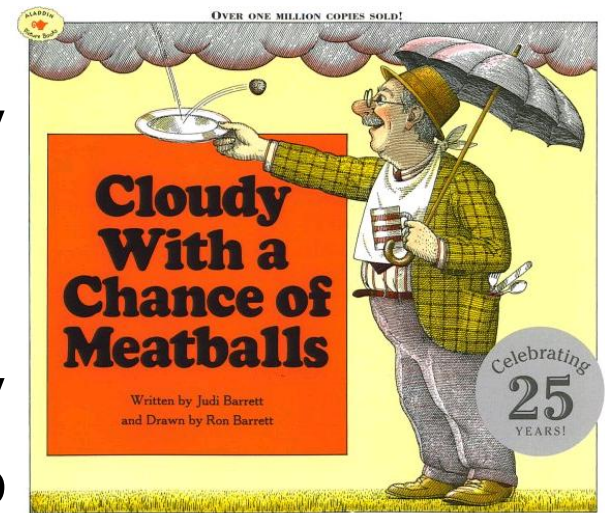
- Result:
 - Focus on an overall IaaS standards roadmap as a first major deliverable
 - Research PaaS and SaaS roadmaps as we move forward
 - Provide visibility, encourage collaboration in addressing these standards as soon as possible
 - Identify common needs for security and data privacy standards across IaaS, PaaS, SaaS

A Roadmap for IaaS

- Needed standards
 - VM image distribution (e.g., DMTF OVF)
 - VM provisioning and control (e.g., EC2 API)
 - Inter-cloud VM exchange (e.g., ??)
 - Persistent storage (e.g., Azure Storage, S3, EBS, GFS, Atmos)
 - VM SLAs (e.g., ??) – machine readable
 - uptime, resource guarantees, storage redundancy
 - Secure VM configuration (e.g., SCAP)

A Roadmap for PaaS and SaaS

- More difficult due to proprietary nature
- A future focus for NIST
- Standards for PaaS could specify
 - Supported programming languages
 - APIs for cloud services
- Standards for SaaS could specify
 - SaaS-specific authentication / autho
 - Formats for data import and export (e.g., XML schemas)
 - Separate standards may be needed for each application space



Security and Data Privacy Across IaaS, PaaS, SaaS

- Many existing standards
- Identity and Access Management (IAM)
 - IdM federation (SAML, WS-Federation, Liberty ID-FF)
 - Strong authentication standards (HOTP, OCRA, TOTP)
 - Entitlement management (XACML)
- Data Encryption (at-rest, in-flight), Key Management
 - PKI, PKCS, KEYPROV (CT-KIP, DSKPP), EKMI
- Records and Information Management (ISO 15489)
- E-discovery (EDRM)

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

Questions?

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

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