

# Perspectives on Cloud Computing and Standards

Peter Mell, Tim Grance

NIST, Information Technology  
Laboratory



# Standardization and Cloud Computing



- Cloud computing is a convergence of many technologies
  - Some have their own standards
- This convergence combined with massively scaled deployments represents “**leap-ahead**” capabilities
- We have a choice
  - proprietary stovepipe clouds
  - standards based clouds
- Standards will be vital to achieve success
- Can't standardize what you can't define

# A NIST Definition of Cloud Computing

- A computing capability where the architecture surrounding massive clusters of computers is abstracted from the applications using it and a software and server framework (usually based on virtualization) provides clients scalable utility computing capabilities to elastically provide many servers for a single software-as-a-service style application or to host many such applications on a few servers.



# Foundational Elements of Cloud Computing

## Business Models

- Web 2.0
- Software as a Service (SaaS)
- Utility Computing
- Service Level Agreements
- Open standards, Data Portability, and Accessibility

## Architecture

- Autonomic System Computing
- Grid Computing
- Platform Virtualization
- Web Services
- Service Oriented Architectures
- Web application frameworks
- Open source software

# Need for Cloud Computing Standards

- Standards for the cloud architecture
  - Emerging
  - Cloud interfaces are the key
  - Leverage autonomic computing, grids, and virtualization?
- Standards for cloud applications
  - Mature technologies but various approaches exist
  - Software as a service / Utility computing
  - Service Oriented Architecture
  - Web Services standards
  - Web Application frameworks

# Enterprise Cloud Infrastructures



- The Need
  - Security and privacy concerns in using 3<sup>rd</sup> party clouds with sensitive data
  - Problem of security boundaries and security compliance (e.g., HIPAA, FISMA, SOX)
- How should large enterprises create their own clouds?
  - Which standards should be adopted?
  - What is the role of open source and proprietary software?
  - How should one leverage existing data centers (cloud interconnections)?
  - Can one acquire isolated instances of 3<sup>rd</sup> party clouds?
    - Government owned, contractor operated (GOCO)
  - What is the minimum size needed to make it cost effective to build a cloud?

# The Federal Cloud Infrastructure



- An idea: The Federal government identifies minimal **standards** and an **architecture** to enable agencies to create or purchase interoperable cloud capabilities
  - Agencies would own cloud instances or ‘nodes’
  - Nodes would provide the same software framework for running cloud applications
  - Nodes would participate in the Federal cloud infrastructure
  - Federal infrastructure would promote and adopt cloud architecture standards (non-proprietary)
  - ‘Minimal standards’ refers to the need to ensure node interoperability and application portability without inhibiting innovation and adoption thus limiting the scale of cloud deployments

# The Federal Cloud Infrastructure



- Benefits
  - Federal applications could run on any cloud node
  - Federal applications could migrate between cloud nodes
    - Contingency planning/disaster recovery
    - Scalability/elasticity
  - Centralized and standardized security enforcement and monitoring (intrusions, secure configurations, vulnerabilities, malware)
  - Interagency billing of resources used will self-optimize growth of cloud nodes
- Limits to agencies independently building their own clouds
  - Lack of the massive scale needed to leverage cloud benefits
  - Non-interoperable architectures (e.g., no disaster recovery capabilities)

# Possible Approaches Moving Forward



- Should the U.S. government:
  - solely use 3<sup>rd</sup> party clouds (probably just for non-sensitive data)
  - procure a single USG cloud
  - procure multiple independent non-interoperable USG clouds
  - work towards a Federal cloud infrastructure (standards and architecture)

# Upcoming Draft NIST Cloud Computing Security Publication



- NIST Special Publication to be created in FY09
  - Overview of cloud computing
  - Cloud computing security issues
  - Securing cloud architectures
  - Securing cloud applications
  - Enabling and performing forensics in the cloud
  - Centralizing security monitoring in a cloud architecture
  - Obtaining security from 3<sup>rd</sup> party cloud architectures through service level agreements
  - Security compliance frameworks and cloud computing (e.g., HIPAA, FISMA, SOX)

# Questions?



- Peter Mell
- Senior Computer Scientist
- NIST, Information Technology Laboratory
- 301-975-5572
- [mell@nist.gov](mailto:mell@nist.gov)
  
- Tim Grance
- Program Manager, Cyber and Network Security Program
- NIST, Information Technology Laboratory
- 301-975-4242
- [grance@nist.gov](mailto:grance@nist.gov)