ITC 250/CPET 499 Web Systems

Special Lecture on

NIST Cloud Computing Definition, Standards & Roadmap, Security & Privacy Guidelines

Fall 2015

Paul I-Hai Lin, Professor

Dept. of Computer, Electrical and Information Technology

Purdue University Fort Wayne Campus

Topics of Discussion

- NIST Cloud Definition
- NIST Cloud Computing and Standards Roadmap
- NIST Cloud Computing Security & Privacy Guidelines

ANSI Cloud Definition

- NIST Definition of Cloud Computing, Special publication 800-145, by Peter Mell and Timothy Grance, Sept., 2011, U.S. Dept. of Commerce, http://www.nist.gov/itl/csd/cloud-102511.cfm
- NIST Cloud Computing Standards and Roadmap, Version 1.0, Specification 500-291, July 2011, http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909024
- NIST Government Cloud Computing Technology Roadmap Vol I, Special Pub. 500-293, Nov. 2011, http://www.nist.gov/itl/cloud/upload/SP_500_293_volumeI-2.pdf
- NIST Cloud Computing Reference Architecture, Sept. 2011, http://www.nist.gov/customcf/get_pdf.cfm?pub_id=909505
- Business Use Case, NIST Information Technology Laboratory, http://www.nist.gov/itl/cloud/bususecases.cfm

The NIST Definition of Cloud Computing

- Special publication 800-145, by Peter Mell and Timothy Grance, Sept. 2011

"Cloud computing is **a model** for enabling ubiquitous, 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** is composed of five essential characteristics, three service models, and four deployment models. "

The NIST Definition of Cloud Computing

- **Five Essential Characteristics**
  - On-demand self-service, Broad network access, Resource pooling, Rapid elasticity, Measured service
- **Three Service Models**
  - Software as a Service (SaaS)
  - Platform as a Service (Paas)
  - Infrastructure as a Service (IaaS)
- Four **Deployment Models**
  - Private cloud
  - Community cloud
  - Public cloud
  - Hybrid cloud

The NIST Definition of Cloud Computing

- Three Service Models
  - **Software as a Service (SaaS)**
    - The **capability provided** to the consumer is to use the provider's applications running on a cloud infrastructure.
    - The **applications are accessible** from various client devices through either a thin client interface, such as web browser (e.g., web-based email), or program interface.
    - The consumer **does not** manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited specific application configuration settings)
  - **Platform as a Service (Paas)**
  - **Infrastructure as a Service (IaaS)**

The NIST Definition of Cloud Computing

- Three Service Models
  - **Software as a Service (SaaS)**
  - **Platform as a Service (Paas)**
    - The **capability provided** to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired application created using programming languages, libraries, services, and tools **supported by the provider**.
    - The consumer **does not manage or control** the underlying cloud infrastructure
    - The consumer **has control over** the deployed applications and possibly configuration settings for the application-hosting environment
  - **Infrastructure as a Service (IaaS)**

The NIST Definition of Cloud Computing

- Three Service Models: **Software as a Service (SaaS), Platform as a Service (Paas)**, and
  - **Infrastructure as a Service (IaaS)**
    - The **capability provided** to the consumer is to provision processing, storage, networks, and fundamental computing resources where the consumer is able to deploy and run arbitrary software which can include operating systems and applications.
    - The consumer **does not** manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deploying applications; and possibly limited control of select networking components (e.g. host firewalls)

The NIST Definition of Cloud Computing

- Four Deployment Model
  - **Private Cloud**
    - **The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g. business units).**
    - **It may owned, managed, and operated by the organization, or some combination of them. And**
    - **It may exist on or off premises.**
  - Public Cloud
  - Community Cloud
  - Hybrid Cloud

The NIST Definition of Cloud Computing

- Four Deployment Model
  - Private Cloud
  - **Public Cloud**
    - **The cloud infrastructure is provisioned for open use by the general public.**
    - **It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them.**
    - **It exits on the premises of the cloud provider.**
  - Community Cloud
  - Hybrid Cloud

The NIST Definition of Cloud Computing

- Four Deployment Model
  - Private Cloud, Public Cloud
  - **Community Cloud**
    - **The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security, requirements, policy, and compliance considerations.)**
    - **It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and**
    - **It may exist on or off premises.**
  - Hybrid Cloud

The NIST Definition of Cloud Computing

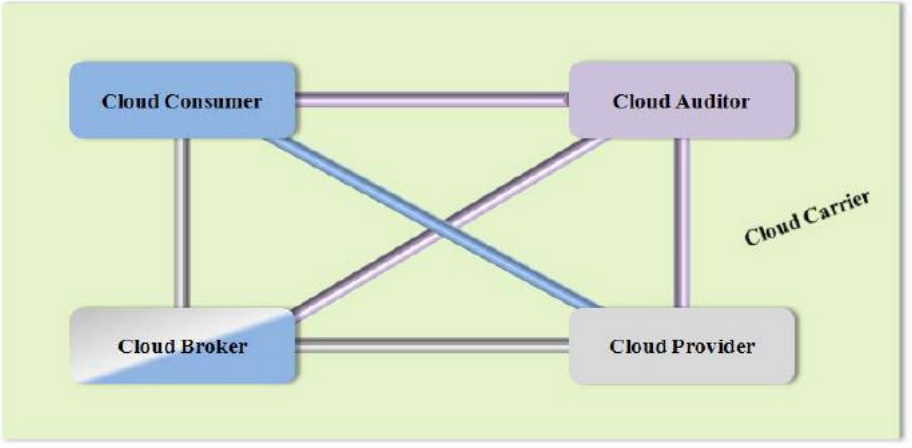
- Four Deployment Model
  - Private Cloud, Public Cloud, Community Cloud
  - **Hybrid Cloud**
    - The **cloud infrastructure** is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are **bound together** by standardized or proprietary technology that enable data and application portability (e.g. cloud bursting for load balancing between clouds)

The NIST Cloud Computing Roadmap

- Actors in Cloud Computing
- Cloud Computing Definition and Reference architecture
- Cloud Computing Use Cases and Requirements
- Cloud Computing and Gap Analysis
- High-Priority Security Requirements
- Other Related Works
  - Cloud Data Issues
  - Service-Level Agreement Taxonomy
  - Reliability Research in Cloud-Based Complex System

NIST Cloud Actor Definitions: Actors

- **Cloud Consumer; Cloud Provider; Cloud Auditor; Cloud Broker; Cloud Carrier**
- **Figure 1. Interaction between actors in Cloud Computing**



NIST Cloud Actor Definitions

- Cloud Consumer
  - **Person or organization that maintains a business relationship with, and use service from, Cloud Providers.**
- Cloud Provider
  - **Person, organization, or entity responsible for making a service available to Cloud Consumers.**
- Cloud Auditor
  - **A party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementation.**
- Cloud Broker
- Cloud Carrier

NIST Cloud Actor Definitions

- Cloud Broker
  - **An entity that manages the use, performance, and delivery of cloud services, and negotiates relationships between Cloud Providers and Cloud Consumers.**
- Cloud Carrier
  - **The intermediary that provides connectivity and transport of cloud services from Cloud Providers to Cloud Consumers.**

Cloud Consumer & Cloud Provider Activities

Source: Table 2 of **NIST Cloud Computing Standards Roadmap**

Type	Consumer Activities	Provider Activities
SaaS	Uses application/service for business process operations.	Install, manages, maintains, and supports the software application on a cloud infrastructure.
PaaS	Develops, tests, deploys, and manages applications hosted in a cloud environment.	Provisions and manages cloud infrastructure and middleware for the platform consumers; provides development, deployment, and administration tools to platform consumers.
IaaS	Creates/installs, manages, and monitors services for IT infrastructure operations.	Provisions and manages the physical processing, storage, networking, and the hosting environment and cloud infrastructure for IaaS consumers.

Figure 2. Example of Services Available to a Cloud Consumer

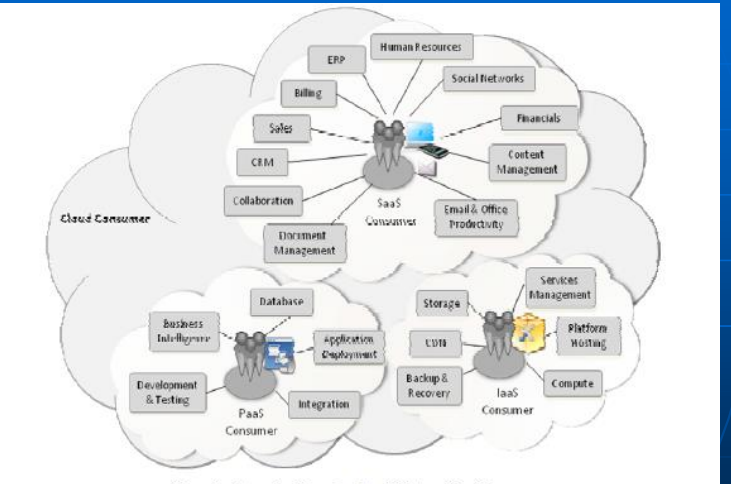
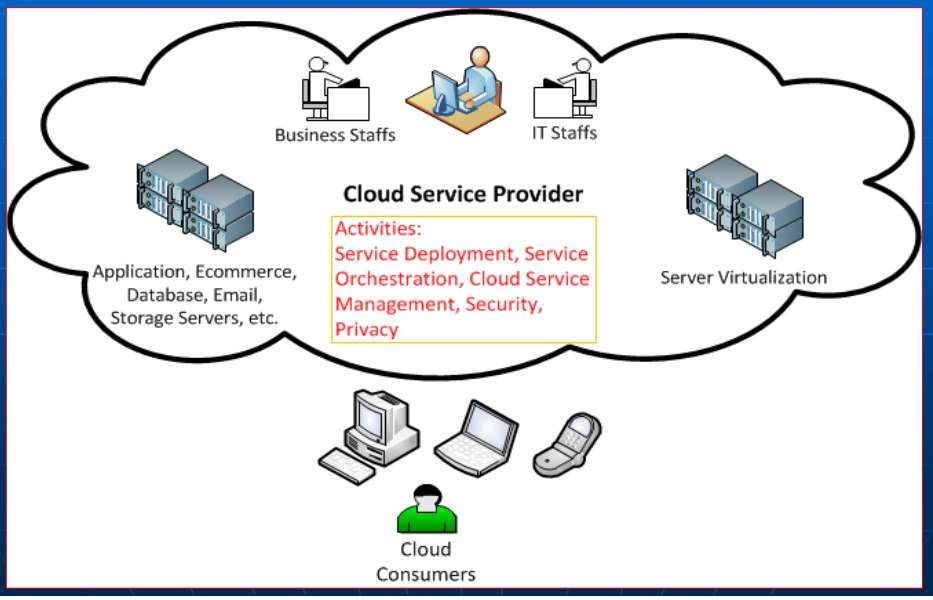


Figure 2 – Example of Services Available to a Cloud Consumer

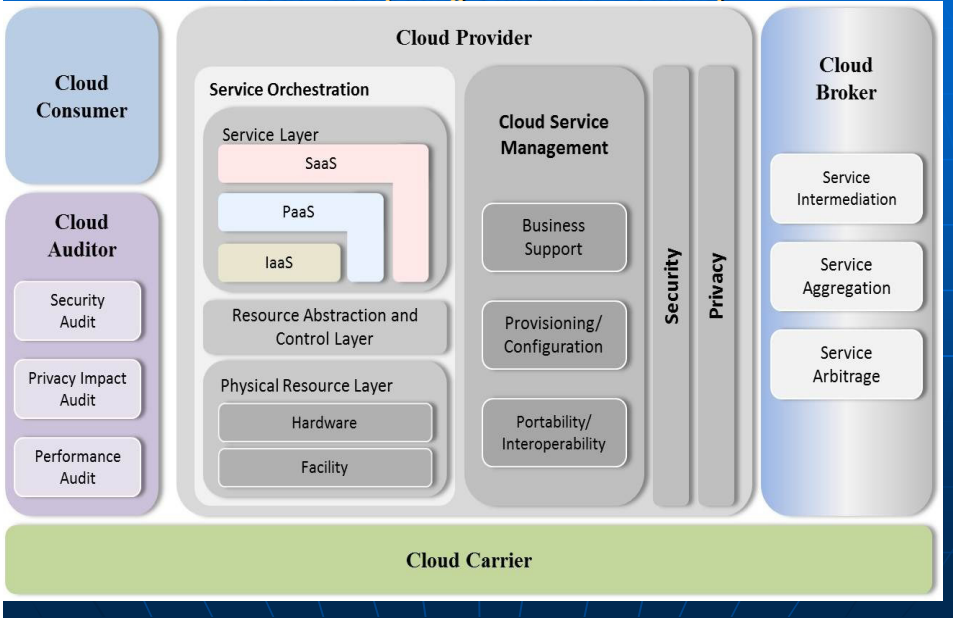
Cloud Consumer & Cloud Provider Activities

Revised based on Figure 3 of NIST Cloud Computing Standards Roadmap



The NIST Cloud Conceptual Model

Figure 12 The Combined Conceptual Reference Diagram, NIST Cloud Computing Standards Roadmap



IT Standards Development and Life Cycle (pp. 31)

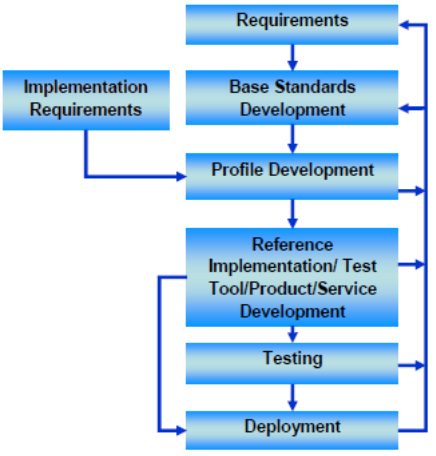


Figure 7 – IT Standards Life Cycle

Cloud Computing Standards (pp. 43-45)

- **Security Standards Mapping**
  - Authentication & Authorization
  - Confidentiality
  - Integrity
  - Identity Management
  - Security Monitoring & Incident Response
  - Security Policy Management
  - Availability
- Interoperability Standards Mapping
- Portability Standards Mapping

Definitions – Appendix B (pp. 60-76)
Source: American National Standard Dictionary of Information Technology (ANSDIT)

- Information Technology (IT) – Encompasses all technologies for the capture, storage, retrieval, processing, display, representation, organization, management, security, transfer, and interchange of data and information.
- Data Migration: The periodic transfer of data from one hardware or software configuration to another or from one generation of computer technology to a subsequent generation. Migration is necessary action for retaining the integrity of the data and for allowing users to search, retrieve, and make use of data in the face of constantly changing technology (source: http://www.ischool.utexas.edu/~scisco/lis3891.5/email/gloss.html)

Definitions – Appendix B (pp. 60-76)
Source: American National Standard Dictionary of Information Technology (ANSDIT)

- Interoperability: The capability to communicate, execute programs, or transfer data among various functional units under specified conditions.
- Maintainability: A measure of the ease with which maintenance of a functional unit can be performed using prescribed procedures and resources. Synonymous with serviceability.
- Portability: The capability of a program to be executed on various types of data processing systems with little or no modification and without converting the program to a different language.
-

Definitions – Appendix B (pp. 60-76)
Source: American National Standard Dictionary of Information Technology (ANSDIT)

- Reliability: A measure of the ability of a functional unit to perform a required function under given conditions for a given interval.
- Network Resilience: A computing infrastructure that provides continuous business operation (i.e.., highly resistant to disruption and able to operate in a degraded mode if damaged), rapid recovery if failure does occur, and the ability to scale to meet rapid or unpredictable demands. [source: The Committee on National Security Systems Instruction No. 4009, "National Information Assurance Glossary." CNSSI-4009]

Cloud Computing Standards

- Cloud Computing Standards for Interoperability
- Functional Interface:
  - The interface provided to/by what is resident in the cloud
  - For Iaas Functional Interface is a virtualized CPU, memory, I/O used by an OS
- Management Interface:
  - Cloud user managers their use of the cloud services
  - Starting, Stopping, Manipulation of VM images and associated resources

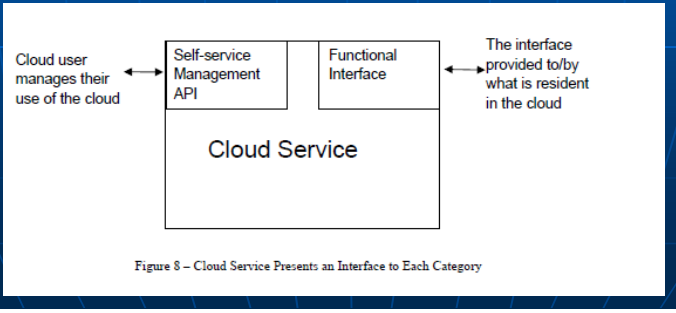


Figure 8 – Cloud Service Presents an Interface to Each Category

Cloud Computing Standards for Interoperability (page 34)

- IaaS Interface:
  - **Functional Interface:**
    - **The VM and disk interfaces that the OS stack runs on**
  - **Management Interface**
    - **Cloud user manages their use (VM life cycle, etc.) of the infrastructure**

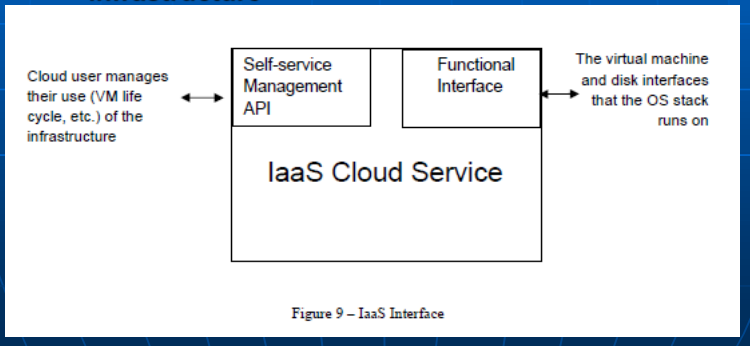


Figure 9 – IaaS Interface

Cloud Computing Standards for Interoperability (page 34)

- PaaS Interface:
  - **Functional Interface:**
    - **The interfaces (service and library)to which the application is written.**
  - **Management Interface**
    - **Cloud user manages their use (application life cycle, etc.) of the platform.**

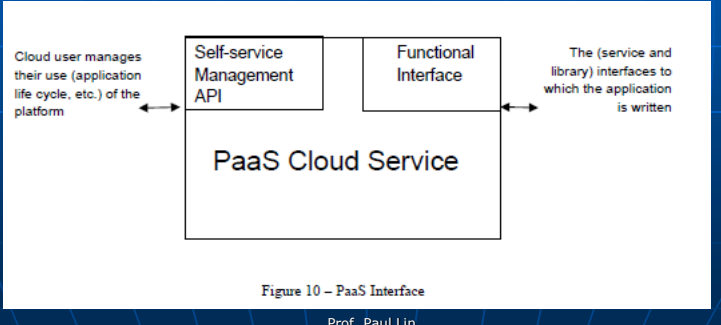


Figure 10 – PaaS Interface

Cloud Computing Standards for Interoperability (page 35)

- SaaS Interface:
  - **Functional Interface:**
    - **The user or Web services interface of the application**
  - **Management Interface**
    - **Cloud user manages their use (Number of users, etc.) of the application**

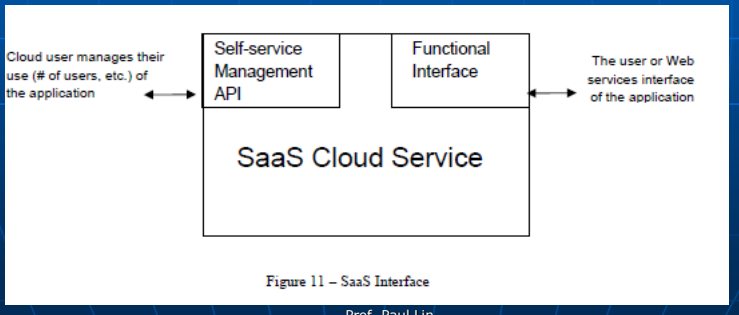


Figure 11 – SaaS Interface

Cloud Computing Standards (pp. 43-45)

- Security Standards Mapping
- **Interoperability Standards Mapping (Service Interoperability)**
  - **Open Cloud Computer Interface** (OCCI), http://occi-wg.org/ ; Open Grid Forum (approved standard) , https://www.ogf.org/ogf/doku.php
  - **Cloud Data Management Interface** (CDMI); Storage Networking Industry Association, SNIA (approved), http://www.snia.org/cdmi
  - IEEE P2301, Draft Guide for Cloud Portability and Interoperability Profiles (CPIP), IEEE, (under development), http://standards.ieee.org/develop/project/2301.html
  - IEEE P2302, Draft Standard for Intercloud Interoperability and Federation (SIIF), IEEE (under development), http://standards.ieee.org/develop/project/2302.html
- Portability Standards Mapping

Cloud Computing Standards (pp. 43-45)

- Security Standards Mapping
- Interoperability Standards Mapping (Service Interoperability)
- **Portability Standards Mapping**
  - **System Portability**
    - **Open Virtualization Format (OVF): DMTF (Distributed Management Task Force, www.dmtf.org , approved standard, market acceptance**
    - **IEEE P2301, Draft Guide for Cloud Portability and Interoperability Profiles (CPIP), IEEE, (under development)**

Cloud Computing Standards (pp. 43-45)

- **Portability Standards Mapping**
  - **Data Portability**
    - **Cloud Data Management Interface (CDMI): SNIA (**Storage Networking Industry Association, http://www.snia.org/cdmi, **approved standard**
  - **Workload Portability**

Use Case Analysis (candidates for standardization)

- Management APIs
- Data Exchange Formats
- Federated Identity and Security Policy APIs
- Resource Descriptions
- Data Storage APIs

10 Use Cases

- **6.4.1 Creating, accessing, updating, deleting data objects in clouds**
- **6.4.2 Moving VMs and virtual appliances between clouds**
- **6.4.3. Selecting the best IaaS cloud vendor, public or private**
- **6.4.4 Portable tools for monitoring and managing clouds**

10 Use Cases (cont.)

- 6.4.5 Moving data between clouds
- 6.4.6 Single sign-on access to multiple clouds
- 6.4.7 Orchestrated processes across clouds and Enterprise Systems
- 6.4.8 Discovering cloud resources
- 6.4.9 Evaluating SLAs and penalties
- 6.4.10 Auditing clouds

6.4.1 Use Case: Creating, Accessing, Updating, Deleting data objects in clouds

- Benefits: Cross-cloud applications
- Deployment Mode Considerations
  - Basic Create-Read-Update-Delete (CRUD) operations on data objects
- Standardizations Needed
  - Standard interface to metadata and data objects
- Possible Standards: CDMI (Cloud Data Management Interface) from SNIA (Storage Networking Industry Association)

6.4.2 Use Case: Moving VMs and virtual appliances between clouds

- Benefits: Hybrid Clouds, Disaster Recovery, Cloud Bursting
- Deployment Mode Considerations
  - When moving a VM out of one cloud and into another as two separate actions, conceivably two different ID management systems can be used.
  - When moving VMs in a truly hybrid cloud, however, federated ID management standards will ne needed.
- Standardizations Needed
  - Common VM description format
- Possible Standards: OVM (Open Virtualization Format Specification, 2013) from DMTF (Distributed Management Task Force, www.dmtf.org) ; OpenID, Oauth

6.4.3 Use Case: Selecting the best IaaS cloud vendor, public or private

- Benefits: Provide cost-effective reliable deployments
- Deployment Mode Considerations
  - When considering hybrid or distributed (inter) cloud deployments, uniform and consistent resources, performance, and policy descriptions are needed.
- Standardizations Needed
  - Resource and performance requirements description languages
- Possible Standards:
  - For basic resource descriptions, DMTF CIM (Common Information Model), http://www.dmtf.org/standards/cim and OGF GLUE (Open Grid Forum) are candidates. Other more extensive description languages for performance or policy enforcement are to be determined.

6.4.4 Use Case: Portable tools for monitoring and managing clouds

- Benefits: Simplifies operations as opposed to individual tools for each cloud
- Deployment Mode Considerations
  - Monitoring and managing are separated but closely related tasks. The standard required will differ depending on whether the monitoring and managing must be done across trust boundaries or across distributed environments.
- Standardizations Needed
  - Standard monitoring and management interfaces to **IaaS resource**
- Possible Standards:

6.4.4 Use Case: Portable tools for monitoring and managing cloud (continue)

- Possible Standards:
  - Basic monitoring standards exist, such as the Syslog Protocol (IETF RFC 5424, March 2009, https://tools.ietf.org/html/rfc5424), which can be used with the Transport Layer Security (TLS) Transport Mapping for Syslog (IETF RFC 5425).
  - Basic management standards include the Cloud Management WG (Work Group) from DMTF, and OCCI from OGF.

6.4.5 Use Case: Moving data between clouds

- Benefits: Migrate between Clouds, cross-cloud application and B2B integration
- Deployment Mode Considerations
  - Migrating data from one cloud to another in two separate moves through the client is a simple case.
  - Migrating data directly from one cloud to another will require standards for federated identity, delegation of trust, and secure third-part transfers.
- Standardizations Needed: Standard metadata/data format for movement between clouds
- Standardized query languages (NoSQL for IaaS)
- Possible Standards: AS4 (Application Statement), OAGIS (Open Application Group Integration Specification, http://www.oagi.org/oagis/9.0/) , NoSQL, GridFTP

6.4.6 Use Case: Single sign-on access to multiple clouds

- Benefits: Simplified access, Cross-cloud applications
- Deployment Mode Considerations
  - Single sign-on can mean the same credentials to access different clouds independently at different times.
  - Single sign-on to access an inter-cloud application that spans multiple clouds will require federated identity management, delegation of trust, and virtual organization.
- Standardizations Needed: Federated identity, authorization, and virtual organizations
- Possible Standards: OpenID (http://opened.net/ , Oauth (Open Standard to Authorization, http://oauth.net/2/ , SAML, WS-Federation and WS-Trust, CSA outputs; VOMS (Virtual Organization Management System)

6.4.6 Use Case: Single sign-on access to multiple clouds

- Possible Standards:
  - **OpenID http://opened.net/**
  - **Oauth (Open Standard to Authorization), http://oauth.net/2/**
  - **SAML (Security Assertion Markup Language), http://saml.xml.org/**
  - **WS-Federation (Web Service), http://docs.oasis-open.org/wsfed/federation/v1.2/os/ws-federation-1.2-spec-os.html**
  - **WS-Trust, http://docs.oasis-open.org/ws-sx/ws-trust/200512**
  - **CSA outputs;**
  - **VOMS (Virtual Organization Membership Service), http://toolkit.globus.org/grid_software/security/voms.php**

6.4.7 Use Case: Orchestrated processes across clouds and Enterprise Systems

- Benefits: Direct support for necessarily distributed systems
- Deployment Mode Considerations
  - This use case is inherently distributed and across trust boundaries. This can be generally termed Federated Resource Management and is a central concept in grid computing community. The term inter-cloud can also be used to denote this concept.

6.4.7 Use Case: Orchestrated processes across clouds and Enterprise Systems (cont.)

- Standardizations Needed: To address this use case complexity, an entire set of capabilities need to be standardized, e.g.,
  - Infrastructure services;
  - Execution Management services;
  - Data services;
  - Resource Management services;
  - Security services;
  - Self-management services; and
  - Information services.

6.4.7 Use Case: Orchestrated processes across clouds and Enterprise Systems (cont.)

- Possible Standards:
- SOA standards (such as WS-I) and grid standards (such as the OGSA WSRF (Open Grid Service Architecture, Web Services Resource Framework) Basic Profile, OGF GFD-R-P.072: Grid Forum Document) exist that cover these areas, but issues around stateful resources, callbacks/notifications, and remote content lifetime management has cause these to be eclipsed by the simplicity of Representational State Transfer (REST).
- Hence, standard, REST-based versions of these capabilities must be developed.
- Such work is being done in several organizations, including the IEEE.

6.4.7 Use Case: Orchestrated processes across clouds and Enterprise Systems (cont.)

- Possible Standards: DMTF (The Distributed Management Task Force, http://www.dmtf.org/) and OGF (Open Grid Forum, http://www.gridforum.org/gf/group_info/view.php?group=dcifed-wg)
- The OGF Distributed Computing Infrastructure Federations Working Group (DCI Federal [F=DCIfed]-WG) is addressing two usage scenarios: (1) delegation of workload from one domain into the other, covering job description, submission, and monitoring; and (2) leasing of resources, including resource definition, provisioning, and monitoring.

6.4.7 Use Case: Orchestrated processes across clouds and Enterprise Systems (cont.)

- Possible Standards:
- Existing standards to support this include
  - WS-Agreement, http://www.ogf.org/documents/GFD.107.pdf
  - Job Submission Description Language (JSDL), http://www.gridforum.org/documents/GFD.56.pdf
  - GLUE Information Model, http://redmine.ogf.org/dmsf_files/102
  - OGSA Basic Execution Service, http://www.ogf.org/documents/GFD.108.pdf

6.4.7 Use Case: Orchestrated processes across clouds and Enterprise Systems (cont.)

- Possible Standards:
- Existing standards to support this include
  - OCCI (Open Cloud Computing Interface) – Infrastructure, http://www.gridforum.org/documents/GFD.184.pdf, http://occi-wg.org/tag/specification/
  - Usage Record. https://www.ogf.org/documents/GFD.98.pdf
  - Specific Business application data formats may be supported by OAGIS.

6.4.7 Use Case: Orchestrated processes across clouds and Enterprise Systems (cont.)

- Possible Standards:
- **Workflow and workflow engines** will also need standardization and adoption in the cloud area. BPEL is one existing standards but extensions might be needed to efficiently support scientific and engineering workflows.
- (WS-BPEL 2.0, http://bpel.xml.org/specifications)

6.4.8 Use Case: Discovering cloud resources

- Benefits: Selection of appropriate cloud for applications
- Deployment Mode Considerations : To support inter-cloud resource discovery, secure federated catalog standards are needed.
- Standardizations Needed: Description languages for available resources, Catalog interfaces
- Possible Standards:
  - This use case actually requires two areas of standardization: (1) description language for the resources to be discovered, and (2) the discovery APIs for the discovery process itself.
  - Some existing standards and tools cover both areas:

6.4.8 Use Case: Discovering cloud resources (cont.)

- Possible Standards: …Some existing standards and tools cover both areas:
  - RFD (Resource Description Framework) is a standard formalism for describing resources as triples consisting of "subject-Predicate-Object". (http://www.w3.org/TR/rdf-concepts/)
  - The Dublin Core is a small, fundamental set of text elements for describing resources of all types.
  - It is commonly expressed in RDF. Since the Dublin Core is a "core" set, it is intended to be extensible for a broad range of application domains. Such work is being pursued by the Dublin Core Medatdata Initiative, http://dublincore.org/ .

6.4.8 Use Case: Discovering cloud resources (cont.)

- Possible Standards: …Some existing standards and tools cover both areas:
  - ebXML Registry Information Model (ebRIM) actually defined both a description language and a discovery method, ebXML Registry Services (ebRS); http://www.ebxml.org/
  - ID-WSF (Identity Web Service Framework), http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications/
  - LDAP (Lightweight Directory Access Protocol), http://www.rfc-editor.org/rfc/rfc4512.txt

6.4.8 Use Case: Discovering cloud resources (cont.)

- Possible Standards: …Some existing standards and tools cover both areas:
  - UDDI (Universal Description, Discovery, and Integration), https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=uddi-spec
  - CSW (Catalogue Service), OGC (Open Geospatial Consortium) standards, http://www.opengeospatial.org/standards/is

6.4.9 Use Case: Evaluating SLAs and penalties

- Benefits: Selection of appropriate cloud resources
- Deployment Mode Considerations: …
- Standardizations Needed: SLA description language
- Possible Standards:
  - WS-Agreement (GFD.107)
  - WS-Agreement Negotiation (OGF)

6.4.10 Use Case: Auditing clouds

- Benefits: Ensure regulatory compliance. Verify information assurance.
- Deployment Mode Considerations: …
- Standardizations Needed: Auditing standards and verification check lists
- Possible Standards:
  - CSA Cloud Audit
  - Guidelines for Auditing Grid Certificate Authorities (OGF GFD.169)

Summary & Conclusion