Cloud Computing

Proposal on Data Security & Privacy

Dr. Jaydip Sen

Innovation Lab

Tata Consultancy Services, Kolkata

Email: Jaydip.Sen@tcs.com

Agenda

- Understanding Cloud Computing
- Five essential characteristics of cloud computing
- Cloud service models
- Cloud deployment models
- Security issues in cloud computing
- A specific proposal of work item for the SeON WG

Origin of the term “Cloud Computing”

- “Comes from the early days of the Internet where we drew the network as a cloud… we didn’t care where the messages went… the cloud hid it from us”
  – Kevin Marks, Google

- First cloud around networking (TCP/IP abstraction)

- Second cloud around documents (WWW data abstraction)

- The emerging cloud abstracts infrastructure complexities of servers, applications, data, and heterogeneous platforms
  – (“muck” as Amazon’s CEO Jeff Bezos calls it)

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**.

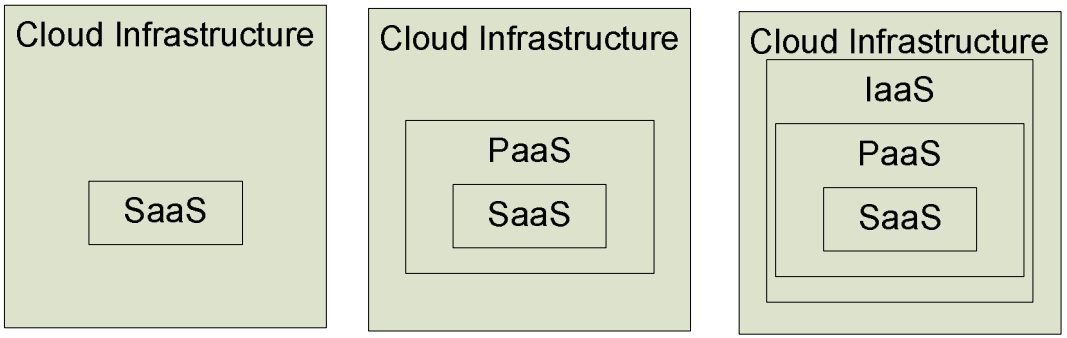
Five Essential Cloud Characteristics

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

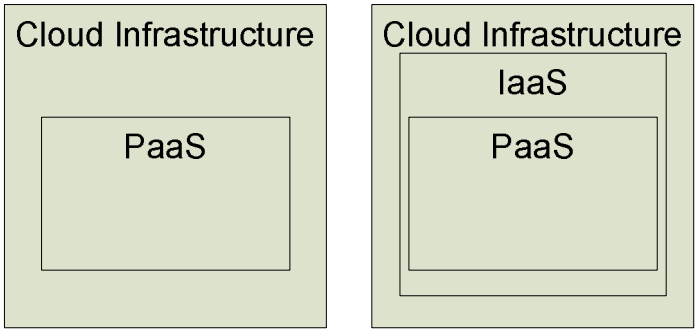
Three Cloud Service Models

- 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

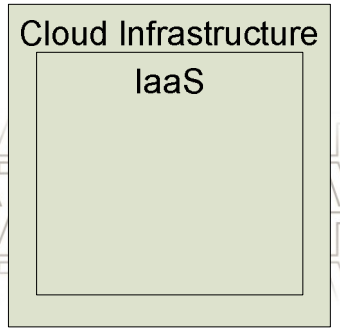
Service Model Architectures



Software as a Service (SaaS) Architectures



Platform as a Service (PaaS) Architectures



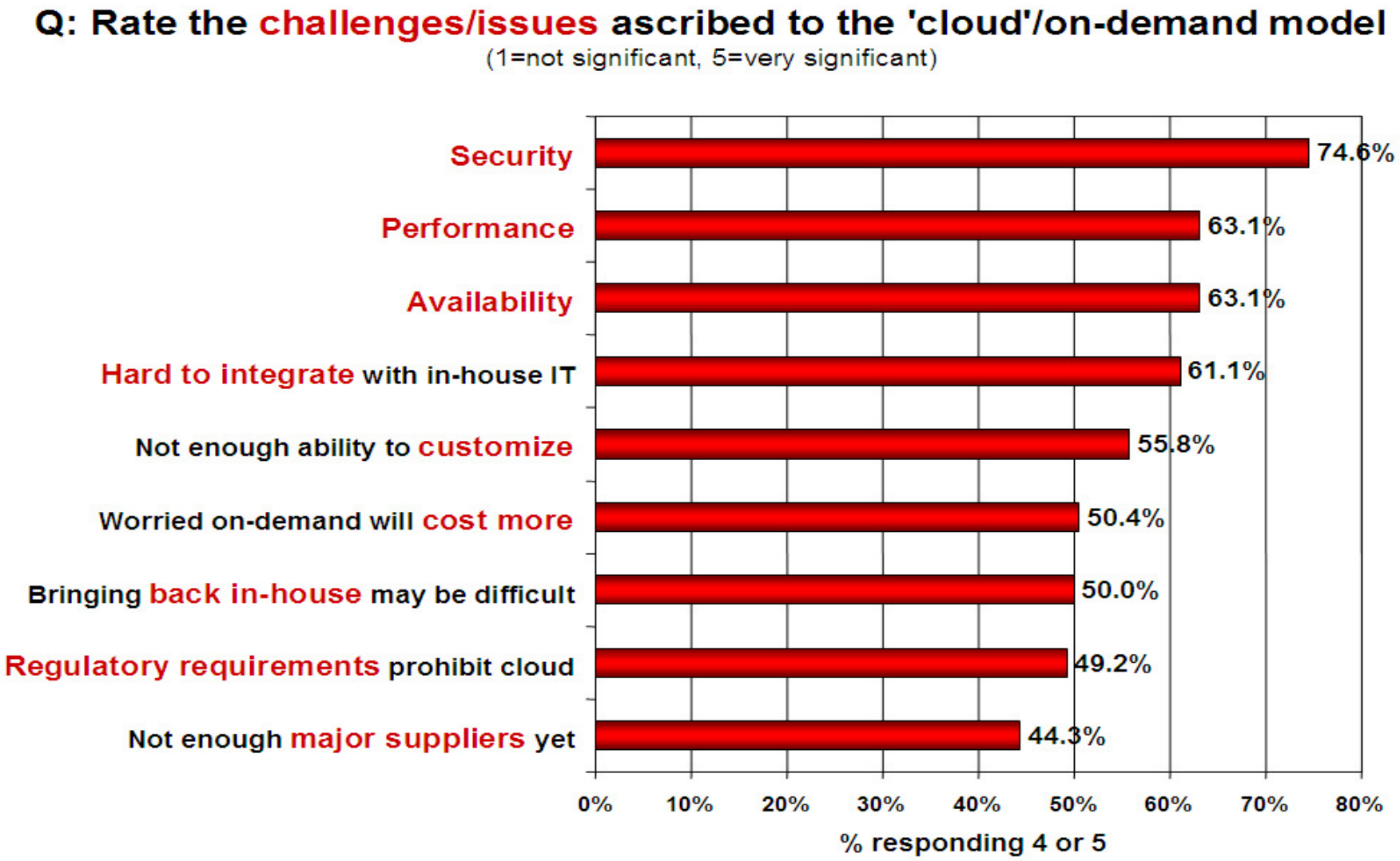
Infrastructure as a Service (IaaS) Architectures

Four 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

Cloud Computing Security

Security is the Major Issue



Source: IDC Enterprise Panel, August 2008 n=244

Analyzing Cloud Security

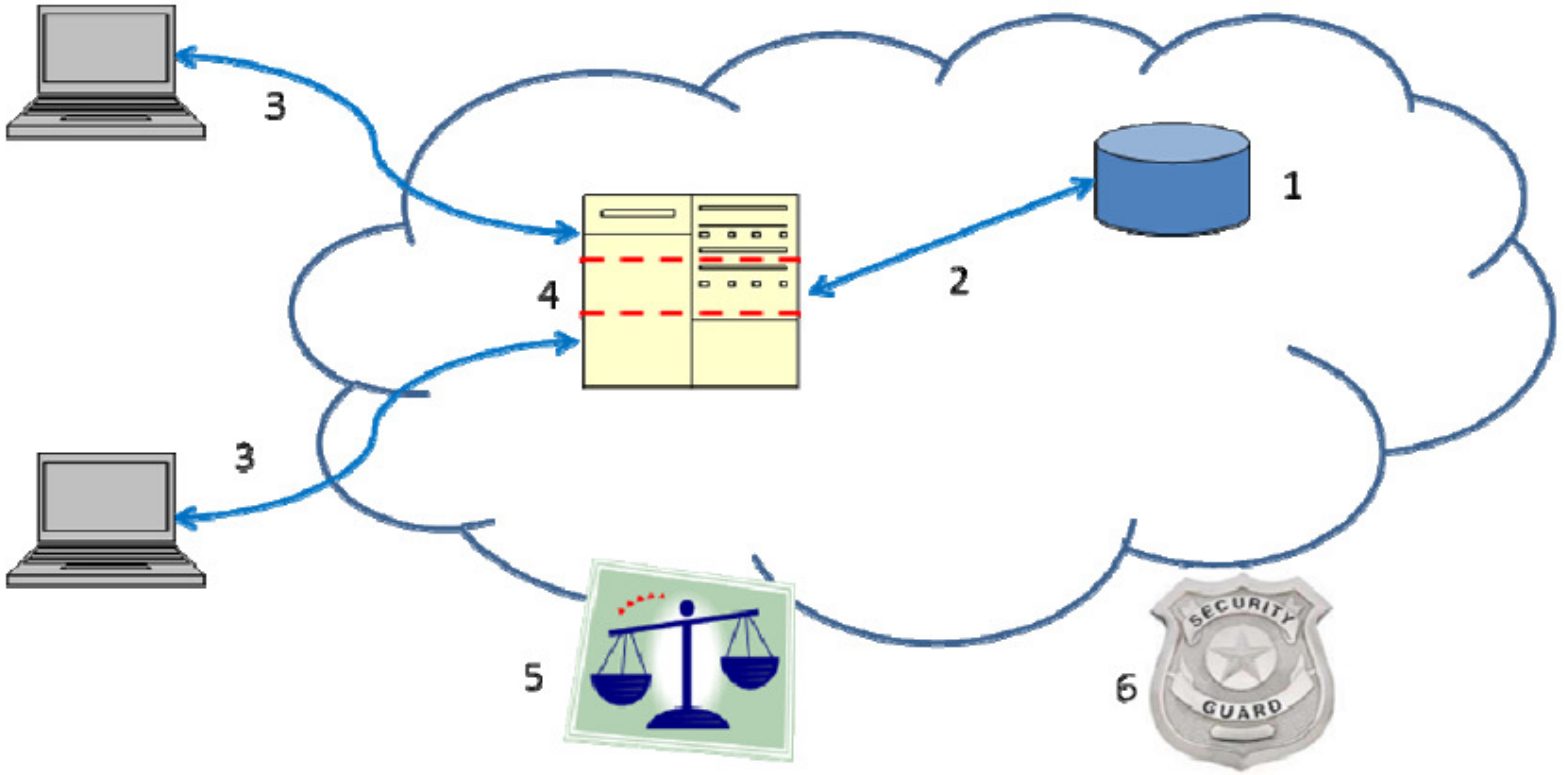
- Some key issues:
  - trust, multi-tenancy, encryption, compliance
- Clouds are massively **complex systems** can be reduced to **simple primitives** that are replicated thousands of times and **common functional units**
- Cloud security is a tractable problem
  - There are both advantages and challenges

Former Intel CEO, Andy Grove: “only the paranoid survive”

General Security 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

Areas of Security Concerns in Cloud Computing



Security Mechanisms (1)

- 1. Security of data at rest
  - Cryptographic encryption is the best practice
  - Hard driver manufacturers are now shipping self-encrypting drives that implements TCG's Trusted Storage standards.
  - Self-encrypting drives build encryption hardware into the drive, providing automated encryption with minimal cost or performance impact
  - Software encryption can also be use. However, it is slower and less secure since the encryption key can be copied off the machine without detection.

- 2. Securing data in transit
  - Encryption techniques are used.
  - In addition, authentication and integrity protection ensure that data only goes where the customer wants it to go and is not modified in transit.
  - Well-established protocols such as SSL/TLS are be used here.

- 3. Authentication
  - Authentication and access control are more important than ever since the cloud and all of its data are accessible to anyone over the Internet. TPM can provide stronger authentication.

Security Mechanisms (2)

- 4. Separation between customers
  - Separation between a cloud provider's users (who may be competing companies) to avoid inadvertent or intentional access to sensitive information is an important issue.
  - Typically a cloud provider would use virtual machines (VMs) and a hypervisor to separate customers.
  - TPM can provide hardware-based verification of hypervisor and VM integrity.

- 5. Cloud legal and regulatory issues
  - To verify that a cloud provider has strong policies and practices that address legal and regulatory issues, each customer must have its legal and regulatory experts inspect cloud provider policies and practices to ensure their adequacy.
  - The issues to be considered include data security compliance, auditing, data retention, and destruction, and legal discovery.

- 6. Incident response
  - Customers need to plan for the possibility of cloud provider security breaches or user misbehavior.
  - An automated response or at least automated notification is the best solution.

Proposal

- The current proposal is for developing solutions for ensuring security of data at rest and for ensuring privacy of user data. The scope includes the following:
  - Identify requirements for security of data at rest. Also study whether there are specific requirements for India.
  - Perform gap analysis against existing standards and solutions.
  - Develop solutions to protect data and preserve user privacy
    - Technical solutions
    - Methods/recommendations
    - Develop guidelines for such protection
  - The group will also work towards the following:
    - Adopt existing standards if considered appropriate for India
    - Provide input to on-going standardization efforts.

Deliverables

- Three major deliverables envisioned from this activity includes the following:
  - Technical report on cloud computing with following focus:
    - Security issues of data at rest
    - Security issues of data in transit
    - User and application authentication
    - Secure separation of data of different user
    - Cloud legal and regulatory issues
    - Incident response
    - Potential solutions in the areas defined in the scope of the work
    - Thoughts on items to standardize (i.e., identity management, access control solutions, cryptographic and other protocols for ensuring security and privacy of user data etc.)
  - Specifications for technical solution (s) for security and user data privacy
  - Recommendations and guidelines preparation

Note: The proposed timelines and other details are available in the document submitted along with the presentation

Thank You!