IIT KHARAGPUR

NPTEL ONLINE
CERTIFICATION COURSES

NPTEL

CLOUD COMPUTING

CLOUD SECURITY II

PROF. SOUMYA K. GHOSH

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

IIT KHARAGPUR

Cloud Computing

- **Cloud computing** is a new computing paradigm, involving data and/or computation outsourcing, with
  - Infinite and elastic resource scalability
  - On demand "just-in-time" provisioning
  - No upfront cost … pay-as-you-go
- Use as much or as less you need, use only when you want, and pay only what you use

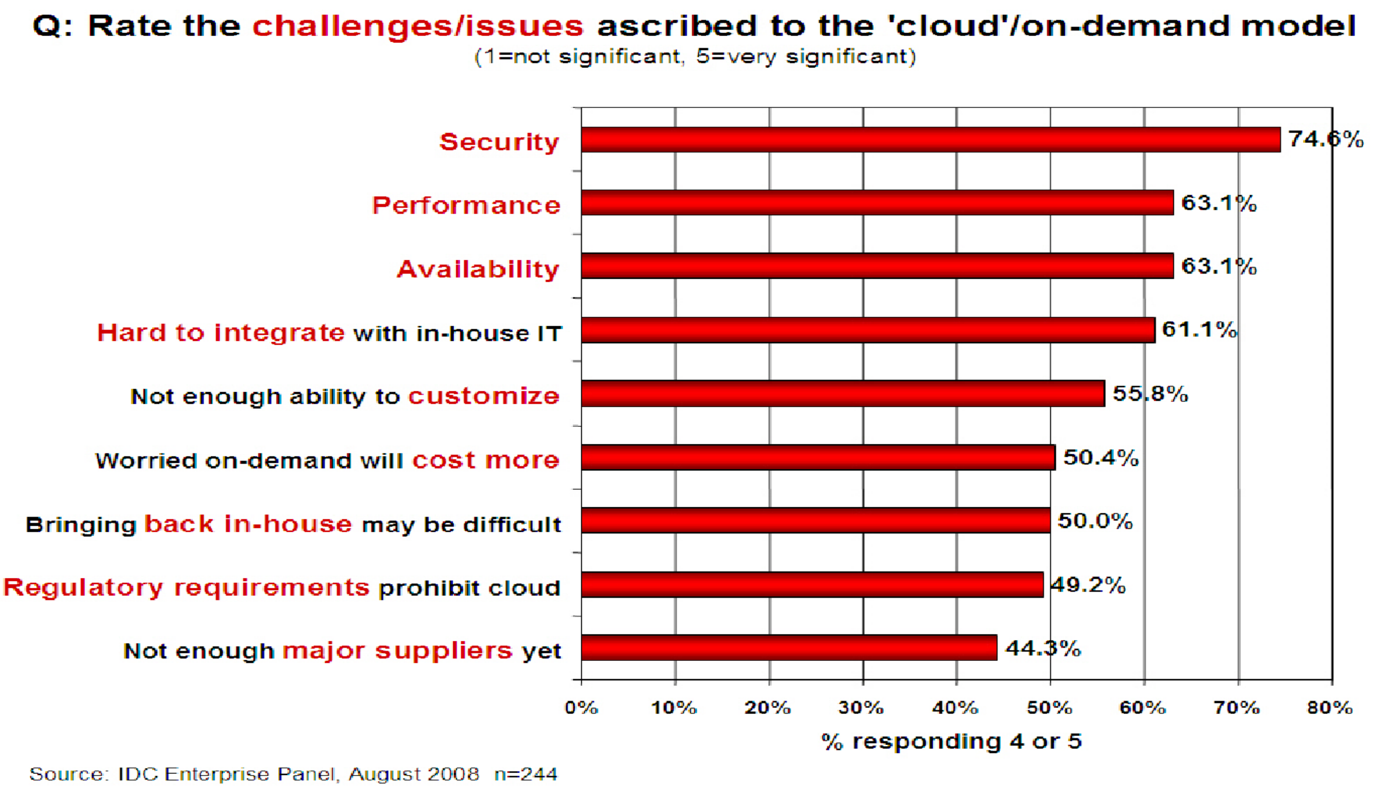
Economic Advantages of Cloud Computing

- For consumers:
  - No upfront commitment in buying/leasing hardware
  - Can scale usage according to demand
  - Minimizing start-up costs
    - Small scale companies and startups can reduce CAPEX (Capital Expenditure)
- For providers:
  - Increased utilization of datacenter resources

Why aren't Everyone using Cloud?

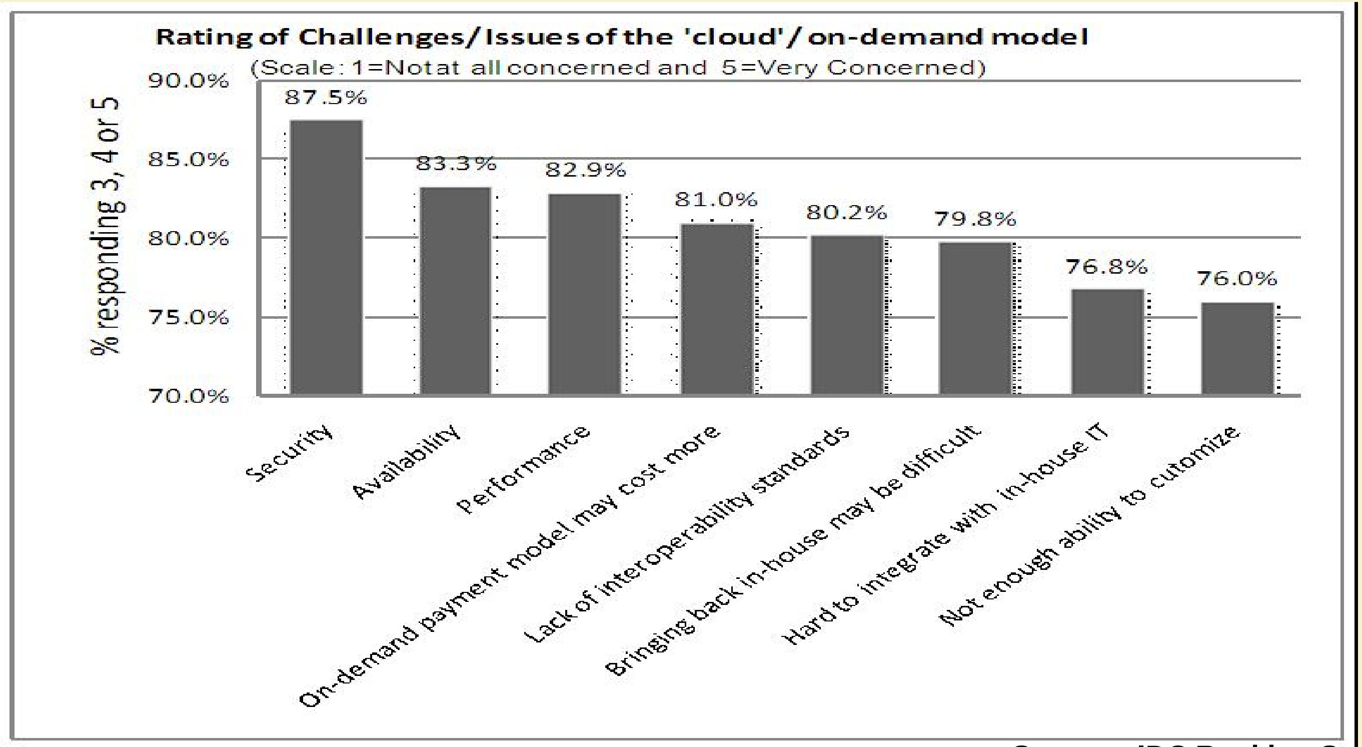
Clouds are still subject to traditional data confidentiality, integrity, availability, and privacy issues, plus some additional attacks

Concern…



Source: IDC Enterprise Panel, August 2008 n=244

Survey on Potential Cloud Barriers



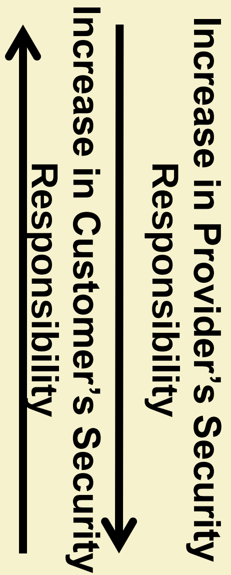
Source: IDC Ranking Security Challenges

Why Cloud Computing brings New Threats?

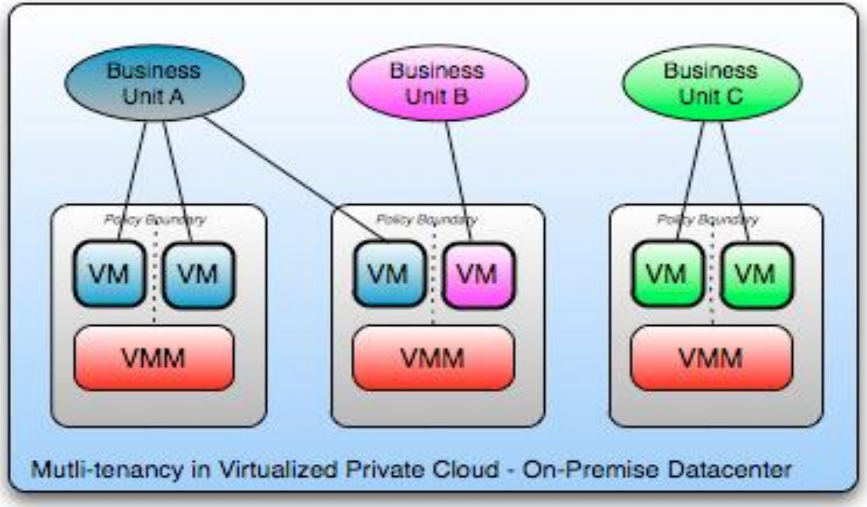
- Traditional system security mostly means keeping attackers out
- The attacker needs to either compromise the authentication/access control system, or impersonate existing users
- But cloud allows **co-tenancy**: Multiple independent users share the same physical infrastructure
  - An attacker can legitimately be in the same physical machine as the target
- Customer's **lack of control** over his own data and application.
- **Reputation fate-sharing**

Security Stack

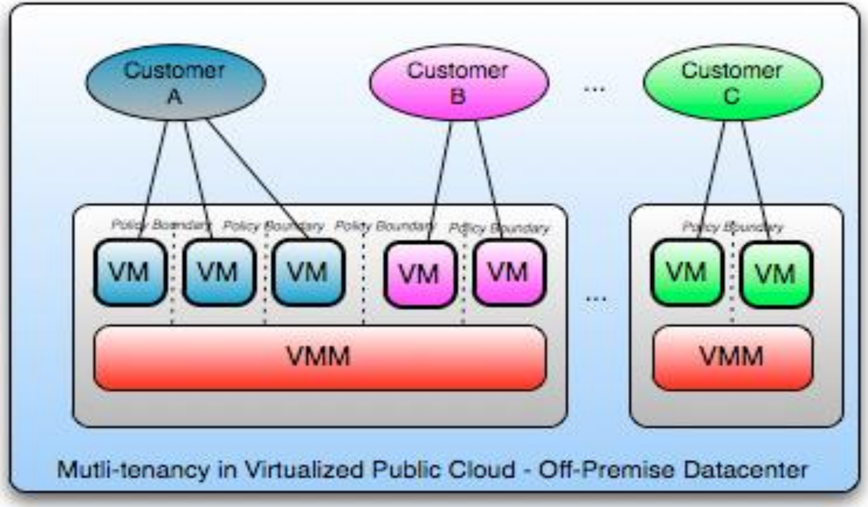
- **IaaS**: entire infrastructure from facilities to hardware
- **PaaS**: application, middleware, database, messaging supported by IaaS
  - Customer-side system administrator manages the same with provider handling platform, infrastructure security
- **SaaS**: self contained operating environment: content, presentation, apps, management
  - Service levels, security, governance, compliance, liability, expectations of the customer & provider are contractually defined


Increase in Provider's Security Responsibility
Increase in Customer's Security Responsibility

Sample Clouds



Private Cloud of Company XYZ with 3 business units, each with different security, SLA, governance and chargeback policies on shared infrastructure



Public Cloud Provider with 3 business customers, each with different security, SLA, governance and billing policies on shared infrastructure

Source: "Security Guidance for Critical Areas of Focus in Cloud Computing" v2.1, p.18

Gartner's Seven Cloud Computing Security Risks

- Gartner:
  - http://www.gartner.com/technology/about.jsp
  - Cloud computing has "unique attributes that require risk assessment in areas such as data integrity, recovery and privacy, and an evaluation of legal issues in areas such as e-discovery, regulatory compliance and auditing," Gartner says
- Security Risks
  - Privileged User Access
  - Regulatory Compliance & Audit
  - Data Location
  - Data Segregation
  - Recovery
  - Investigative Support
  - Long-term Viability

Privileged User Access

- Sensitive data processed outside the enterprise brings with it an inherent level of risk
- Outsourced services bypass the “physical, logical and personnel controls” of traditional in-house deployments.
- Get as much information as you can about the people who manage your data
- “Ask providers to supply specific information on the hiring and oversight of privileged administrators, and the controls over their access,” Gartner says.

Regulatory Compliance & Audit

- Traditional service providers are subjected to external audits and security certifications.
- Cloud computing providers who refuse to undergo this scrutiny are “signaling that customers can only use them for the most trivial functions,” according to Gartner.
- Shared infrastructure – isolation of user-specific log
- No customer-side auditing facility
- Difficult to audit data held outside organization in a cloud
  - Forensics also made difficult since now clients don’t maintain data locally
- Trusted third-party auditor?

Data Location

- Hosting of data, jurisdiction?
- Data centers: located at geographically dispersed locations
- Different jurisdiction & regulations
  - Laws for cross border data flows
- Legal implications
  - Who is responsible for complying with regulations (e.g., SOX, HIPAA, etc.)?
  - If cloud provider subcontracts to third party clouds, will the data still be secure?

Data Segregation

- Data in the cloud is typically in a shared environment alongside data from other customers.
- Encryption is effective but isn't a cure-all. "Find out what is done to segregate data at rest," Gartner advises.
- Encrypt data in transit, needs to be decrypted at the time of processing
  - Possibility of interception
- Secure key store
  - Protect encryption keys
  - Limit access to key stores
  - Key backup & recoverability
- The cloud provider should provide evidence that encryption schemes were designed and tested by experienced specialists.
- "Encryption accidents can make data totally unusable, and even normal encryption can complicate availability," Gartner says.

Recovery

- Even if you don't know where your data is, a cloud provider should tell you what will happen to your data and service in case of a disaster.
- "Any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to a total failure," Gartner says. Ask your provider if it has "the ability to do a complete restoration, and how long it will take."
- **Recovery Point Objective (RPO)**: The maximum amount of data that will be lost following an interruption or disaster.
- **Recovery Time Objective (RTO):** The period of time allowed for recovery i.e., the time that is allowed to elapse between the disaster and the activation of the secondary site.
- Backup frequency
- Fault tolerance
  - **Replication**: mirroring/sharing data over disks which are located in separate physical locations to maintain consistency
  - **Redundancy**: duplication of critical components of a system with the intention of increasing reliability of the system, usually in the case of a backup or fail-safe.

Investigative Support

- Investigating inappropriate or illegal activity may be impossible in cloud computing
- Monitoring
  - To eliminate the conflict of interest between the provider and the consumer, a neural third-party organization is the best solution to monitor performance.
- Gartner warns. “Cloud services are especially difficult to investigate, because logging and data for multiple customers may be co-located and may also be spread across an ever-changing set of hosts and data centers.”

Long-term Viability

- “Ask potential providers how you would get your data back and if it would be in a format that you could import into a replacement application,” Gartner says.
- When to switch cloud providers ?
  - Contract price increase
  - Provider bankruptcy
  - Provider service shutdown
  - Decrease in service quality
  - Business dispute
- Problem: vendor lock-in

Other Cloud Security Issues…

- Virtualization
- Access Control & Identity Management
- Application Security
- Data Life Cycle Management

Virtualization

- Components:
  - Virtual machine (VM)
  - Virtual machine manager (VMM) or hypervisor
- Two types:
  - **Full virtualization**: VMs run on hypervisor that interacts with the hardware
  - **Para virtualization**: VMs interact with the host OS.
- Major functionality: resource isolation
- Hypervisor vulnerabilities:
  - Shared clipboard technology– transferring malicious programs from VMs to host

Virtualization (contd...)

- Hypervisor vulnerabilities:
  - Keystroke logging: Some VM technologies enable the logging of keystrokes and screen updates to be passed across virtual terminals in the virtual machine, writing to host files and permitting the monitoring of encrypted terminal connections inside the VM.
  - Virtual machine backdoors: covert communication channel
  - ARP Poisoning: redirect packets going to or from the other VM.
- Hypervisor Risks
  - Rogue hypervisor rootkits
    - Initiate a 'rogue' hypervisor
    - Hide itself from normal malware detection systems
    - Create a covert channel to dump unauthorized code

Virtualization (contd...)

- Hypervisor Risks
  - External modification to the hypervisor
    - Poorly protected or designed hypervisor: source of attack
    - May be subjected to direct modification by the external intruder
  - VM escape
    - Improper configuration of VM
    - Allows malicious code to completely bypass the virtual environment, and obtain full root or kernel access to the physical host
    - Some vulnerable virtual machine applications: Vmchat, VMftp, Vmcat etc.
  - Denial-of-service risk
- Threats:
  - Unauthorized access to virtual resources – loss of confidentiality, integrity, availability

Access Control & Identity Management

- Access control: similar to traditional in-house IT network
- Proper access control: to address CIA tenets of information security
- Prevention of identity theft – major challenge
  - **Privacy issues** raised via massive data mining
    - Cloud now stores data from a lot of clients, and can run data mining algorithms to get large amounts of information on clients
- Identity Management (IDM) – authenticate users and services based on credentials and characteristics

Application Security

- Cloud applications – Web service based
- Similar attacks:
  - **Injection attacks**: introduce malicious code to change the course of execution
  - **XML Signature Element Wrapping**: By this attack, the original body of an XML message is moved to a newly inserted wrapping element inside the SOAP header, and a new body is created.
  - **Cross-Site Scripting (XSS)**: XSS enables attackers to inject client-side script into Web pages viewed by other users to bypass access controls.
  - **Flooding**: Attacker sending huge amount of request to a certain service and causing denial of service.
  - **DNS poisoning and phishing**: browser-based security issues
  - **Metadata (WSDL) spoofing attacks**: Such attack involves malicious reengineering of Web Services' metadata description
- Insecure communication channel

Data Life Cycle Management

- Data security
  - Confidentiality:
    - Will the sensitive data stored on a cloud remain confidential?
    - Will cloud compromise leak confidential client data (i.e., fear of loss of control over data)
    - Will the cloud provider itself be honest and won’t peek into the data?
  - Integrity:
    - How do I know that the cloud provider is doing the computations correctly?
    - How do I ensure that the cloud provider really stored my data without tampering with it?

Data Life Cycle Management (contd.)

- Availability
  - Will critical systems go down at the client, if the provider is attacked in a Denial of Service attack?
  - What happens if cloud provider goes out of business?
- Data Location
  - All copies, backups stored only at location allowed by contract, SLA and/or regulation
- Archive
- Access latency

Thank You!