

Introduction to Cloud Security and Privacy

Bharat Bhargava
bbshail@purdue.edu
Computer Science
Purdue University

Anya Kim
anya.kim@nrl.navy.mil
Naval Research Lab

YounSun Cho
cho52@cs.purdue.edu
Computer Science
Purdue University



Overview

- Cloud Computing Background
- Cloud Models
- Why do you still hesitate to use cloud computing?
- Causes of Problems Associated with Cloud Computing
- Taxonomy of Fear
- Threat Model



Cloud Computing Background

- **Features**

- Use of internet-based services to support business process
- Rent IT-services on a utility-like basis

- **Attributes**

- Rapid deployment
- Low startup costs/ capital investments
- Costs based on usage or subscription
- Multi-tenant sharing of services/ resources

- **Essential characteristics**

- On demand self-service
- Ubiquitous network access
- Location independent resource pooling
- Rapid elasticity
- Measured service

- “Cloud computing is a compilation of existing techniques and technologies, packaged within a new infrastructure paradigm that offers improved scalability, elasticity, business agility, faster startup time, reduced management costs, and just-in-time availability of resources”



A Massive Concentration of Resources

- Also a massive concentration of risk
 - expected loss from a single breach can be significantly larger
 - concentration of “users” represents a concentration of threats
- “Ultimately, you can outsource responsibility but you can’t outsource accountability.”



From [2] John McDermott, ACSAC 09

Cloud Computing: who should use it?

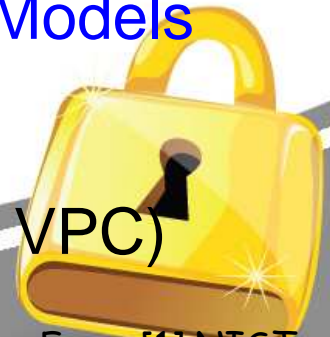
- Cloud computing definitely makes sense if your own security is weak, missing features, or below average.
- Ultimately, if
 - the cloud provider's security people are “better” than yours (and leveraged at least as efficiently),
 - the web-services interfaces don't introduce too many new vulnerabilities, and
 - the cloud provider aims at least as high as you do, at security goals,then cloud computing has better security.



From [2] John McDermott, ACSAC 09

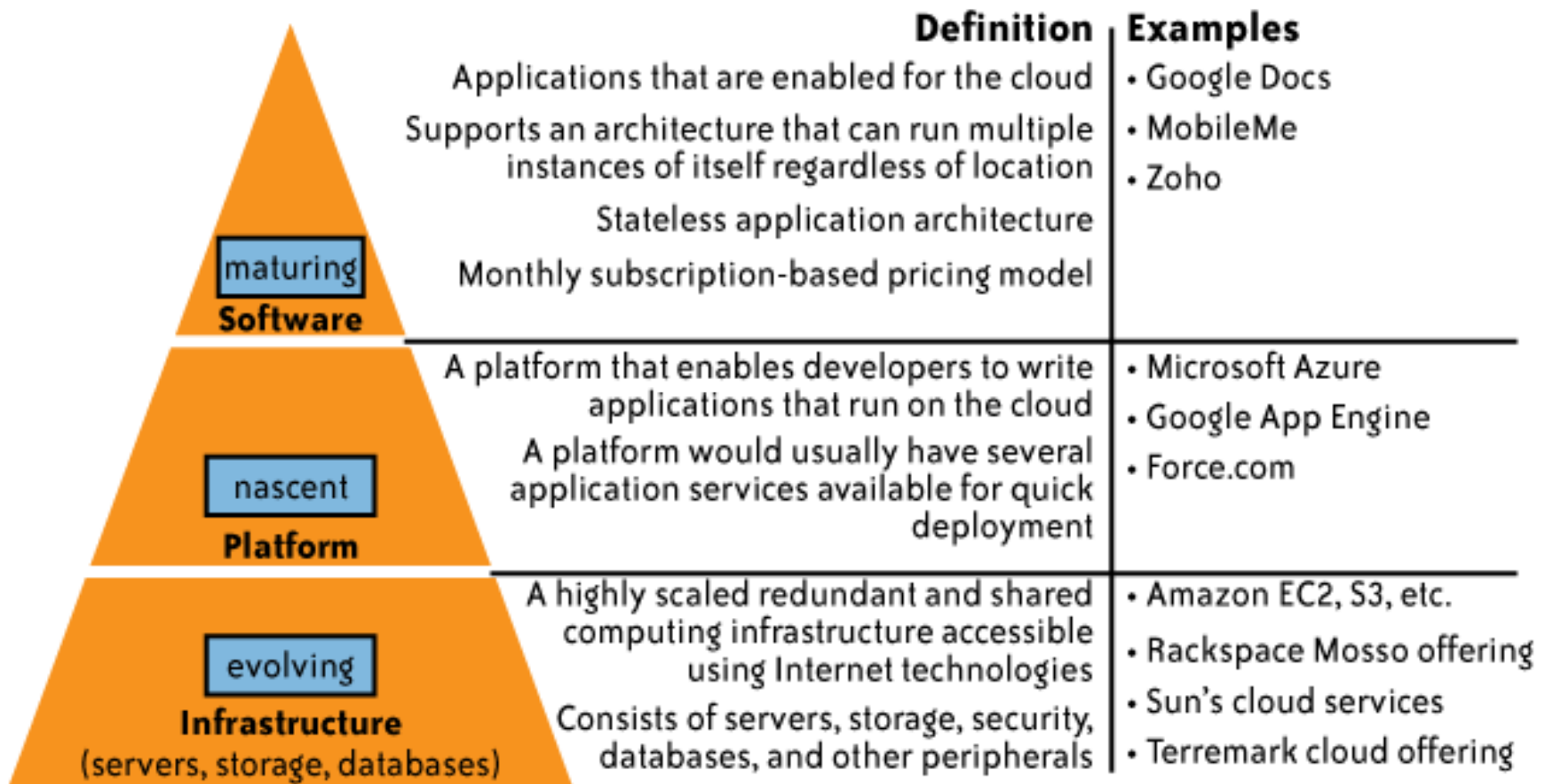
Cloud Models

- **Delivery Models**
 - SaaS
 - PaaS
 - IaaS
- **Deployment Models**
 - Private cloud
 - Community cloud
 - Public cloud
 - Hybrid cloud
- We propose one more Model: **Management Models** (trust and tenancy issues)
 - Self-managed
 - 3rd party managed (e.g. public clouds and VPC)



From [1] NIST

Delivery Models

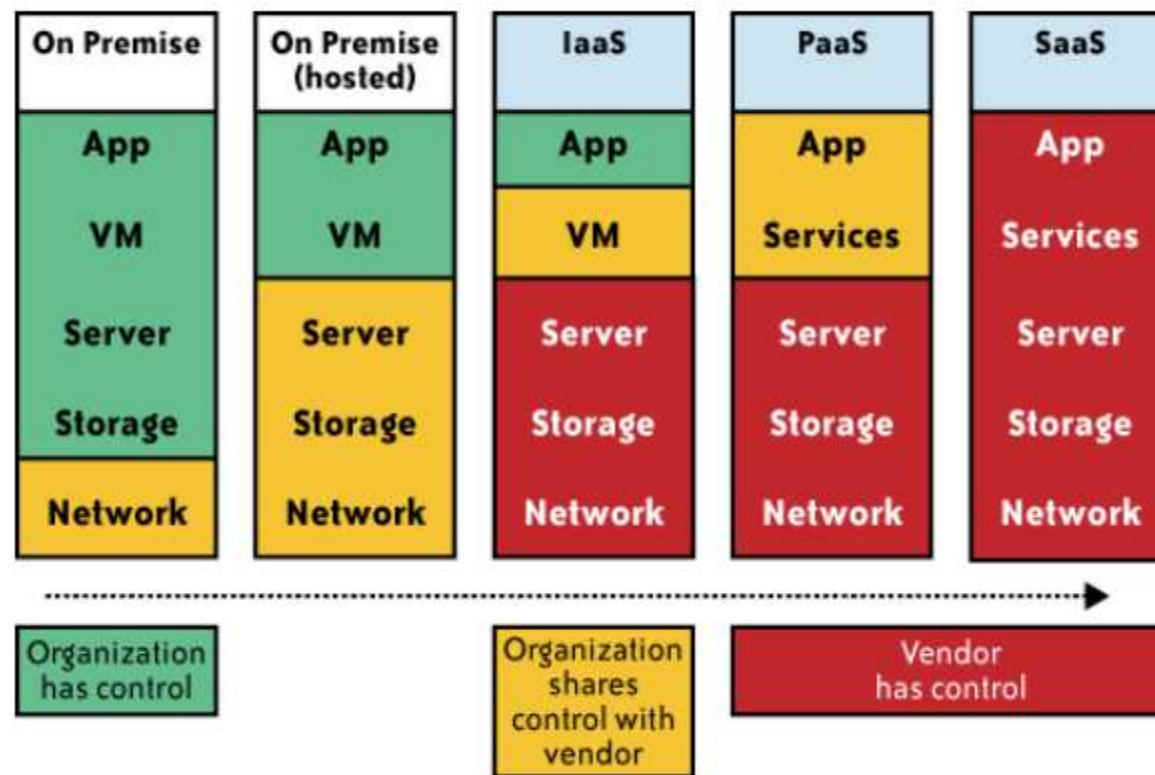


While cloud-based software services are maturing,
Cloud platform and infrastructure offering are still in their early stages !



From [6] Cloud Security and Privacy by Mather and Kumaraswamy

Impact of cloud computing on the governance structure of IT organizations



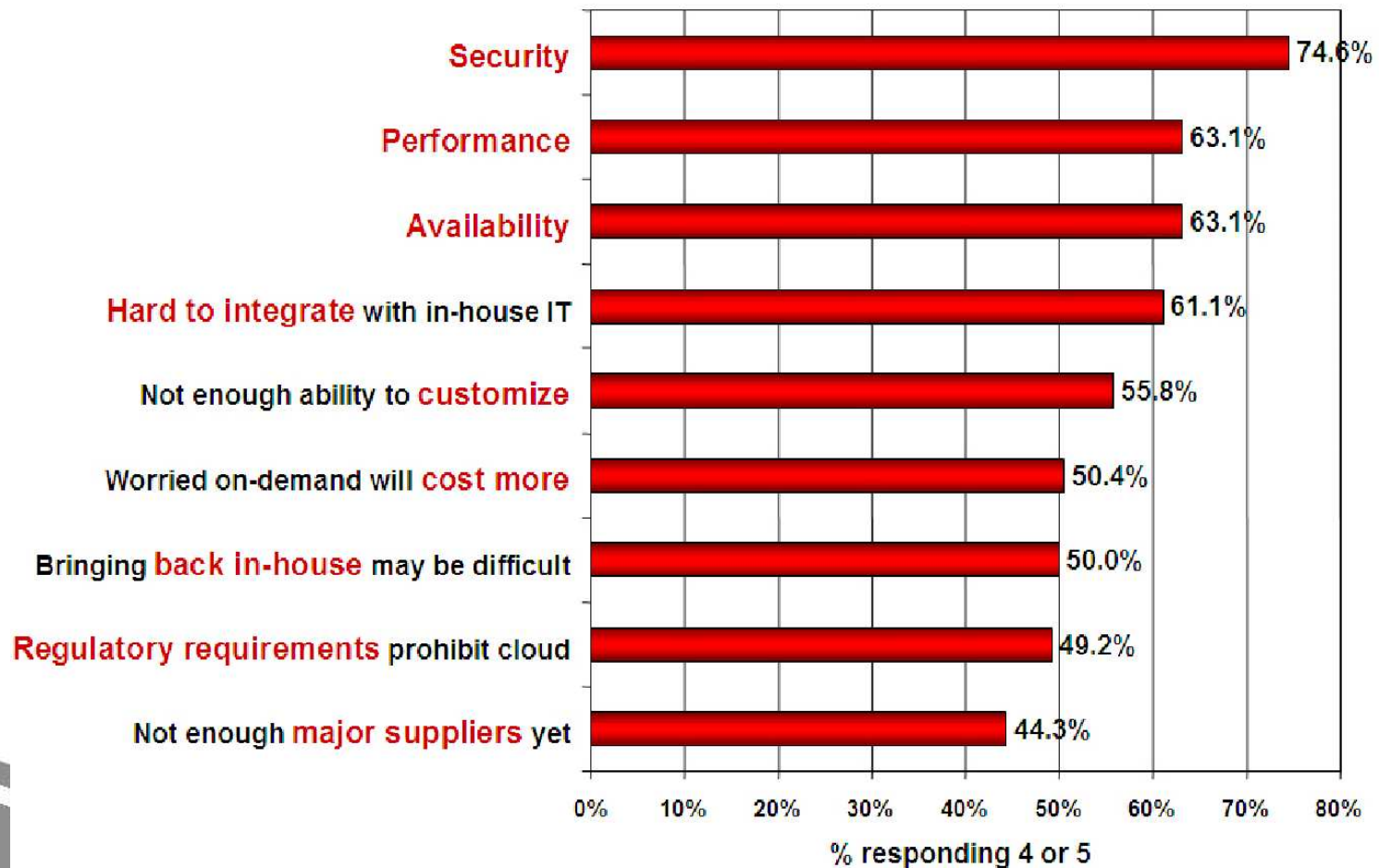
If cloud computing is so great, why isn't everyone doing it?

- The cloud acts as a big black box, nothing inside the cloud is visible to the clients
- Clients have no idea or control over what happens inside a cloud
- Even if the cloud provider is honest, it can have malicious system admins who can tamper with the VMs and violate confidentiality and integrity
- Clouds are still subject to traditional data confidentiality, integrity, availability, and privacy issues, plus some additional attacks



Companies are still afraid to use clouds

Q: Rate the **challenges/issues** ascribed to the 'cloud'/on-demand model
(1=not significant, 5=very significant)



Source: IDC Enterprise Panel, August 2008 n=244

Causes of Problems Associated with Cloud Computing

- Most security problems stem from:
 - **Loss of control**
 - **Lack of trust (mechanisms)**
 - **Multi-tenancy**
- These problems exist mainly in 3rd party management models
 - Self-managed clouds still have security issues, but not related to above



Loss of Control in the Cloud

- **Consumer's loss of control**
 - Data, applications, resources are located with provider
 - User identity management is handled by the cloud
 - User access control rules, security policies and enforcement are managed by the cloud provider
 - Consumer relies on provider to ensure
 - Data security and privacy
 - Resource availability
 - Monitoring and repairing of services/resources



Lack of Trust in the Cloud

- Trusting a third party requires taking risks
- Defining trust and risk
 - Opposite sides of the same coin (J. Camp)
- Chiles and McMakin (1996) define trust as increasing one's vulnerability to the risk of opportunistic **behavior** of **another** whose **behavior** is **not** under **one's control**.
- Trust here means mostly lack of accountability and verifiability
 - People only trust when it pays (Economist's view)
 - Need for trust arises only in risky situations
- Defunct (Invalid / Useless) third party management schemes
 - Hard to balance trust and risk.



Multi-tenancy Issues in the Cloud

- Conflict between tenants' opposing goals
 - Tenants share a pool of resources and have opposing goals
- How does multi-tenancy deal with conflict of interest?
 - Can tenants get along together and 'play nicely' ?
 - If they can't, can we isolate them?
- How to provide separation between tenants?
- Cloud Computing brings new threats
 - Multiple independent users share the same physical infrastructure
 - Thus an attacker can legitimately be in the same physical machine as the target



Taxonomy of Fear

- **Confidentiality**

- Fear of loss of control over data
 - Will the sensitive data stored on a cloud remain confidential?
 - Will cloud compromises leak confidential client 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?



From [5] www.cs.jhu.edu/~ragib/sp10/cs412

15

Taxonomy of Fear (cont.)

- **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?
- Would cloud scale well-enough?



From [5] www.cs.jhu.edu/~ragib/sp10/cs412

16

Taxonomy of Fear (cont.)

- **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
- **Increased attack surface**
 - Entity outside the organization now stores and computes data, and so
 - Attackers can now target the communication link between cloud provider and client
 - Cloud provider employees can be phished



From [5] www.cs.jhu.edu/~ragib/sp10/cs412

17

Taxonomy of Fear (cont.)

- **Audit-ability and forensics (out of control of data)**
 - Difficult to audit data held outside organization in a cloud
 - Forensics also made difficult since now clients don't maintain data locally
- **Legal quagmire (Dilemma) and transitive trust issues**
 - Who is responsible for complying with regulations?
 - e.g., SOX, HIPAA, GLBA ?
 - If cloud provider subcontracts to third party clouds, will the data still be secure?



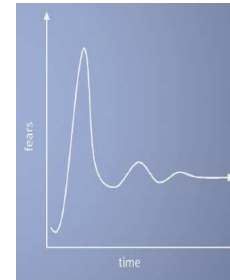
From [5] www.cs.jhu.edu/~ragib/sp10/cs412

18

Taxonomy of Fear (cont.)



Cloud Computing is a **security nightmare** and it can't be handled in traditional ways.
John Chambers
CISCO CEO



- Security is one of the most difficult task to implement in cloud computing.
 - Different forms of attacks in the application side and in the hardware components
 - Attacks with catastrophic effects only needs one security flaw.

(<http://www.exforsys.com/tutorials/cloud-computing/cloud-computing-security.html>)



Threat Model

- A threat model helps in analyzing a security problem, design mitigation strategies, and evaluate solutions
- Steps:
 - Identify attackers, assets, threats and other components
 - Rank the threats
 - Choose mitigation strategies
 - Build solutions based on the strategies



From [5] www.cs.jhu.edu/~ragib/sp10/cs412

20

Threat Model

- Basic components
 - Attacker modeling
 - Choose what attacker to consider
 - insider vs. outsider?
 - single vs. collaborator?
 - Attacker motivation and capabilities
 - Attacker goals
 - Vulnerabilities / threats



From [5] www.cs.jhu.edu/~ragib/sp10/cs412

21

What is the issue?

- The core issue here is the levels of trust
 - Many cloud computing providers trust their customers
 - Each customer is physically commingling its data with data from anybody else using the cloud while logically and virtually you have your own space
 - The way that the cloud provider implements security is typically focused on the fact that those outside of their cloud are evil, and those inside are good.
- But what if those inside are also evil?



From [5] www.cs.jhu.edu/~ragib/sp10/cs412

22

Attacker Capability: Malicious Insiders

- At client
 - Learn passwords/authentication information
 - Gain control of the VMs
- At cloud provider
 - Log client communication
 - Can read unencrypted data
 - Can possibly peek into VMs, or make copies of VMs
 - Can monitor network communication, application patterns
 - Why?
 - Gain information about client data
 - Gain information on client behavior
 - Sell the information or use itself



From [5] www.cs.jhu.edu/~ragib/sp10/cs412

23

Attacker Capability: Outside attacker

- What?
 - Listen to network traffic (passive)
 - Insert malicious traffic (active)
 - Probe cloud structure (active)
 - Launch DoS
- Goal?
 - Intrusion
 - Network analysis
 - Man in the middle
 - Cartography



From [5] www.cs.jhu.edu/~ragib/sp10/cs412

24

Challenges for the attacker

- How to find out where the target is located?
- How to be co-located with the target in the same (physical) machine?
- How to gather information about the target?



From [5] www.cs.jhu.edu/~ragib/sp10/cs412

25

References

1. NIST (Authors: P. Mell and T. Grance), "The NIST Definition of Cloud Computing (ver. 15)," National Institute of Standards and Technology, Information Technology Laboratory (October 7 2009).
2. J. McDermott, (2009) "Security Requirements for Virtualization in Cloud Computing," presented at the ACSAC Cloud Security Workshop, Honolulu, Hawaii, USA, 2009.
3. J. Camp. (2001), "Trust and Risk in Internet Commerce," MIT Press
4. T. Ristenpart et al. (2009) "Hey You Get Off My Cloud," Proceedings of the 16th ACM conference on Computer and communications security, Chicago, Illinois, USA
5. Security and Privacy in Cloud Computing, Dept. of CS at Johns Hopkins University. www.cs.jhu.edu/~ragib/sp10/cs412
6. Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance by Tim Mather and Subra Kumaraswamy
7. Afraid of outside cloud attacks? You're missing the real threat. <http://www.infoworld.com/d/cloud-computing/afraid-outside-cloud-attacks-youre-missing-real-threat-894>
8. **Amazon downplays report highlighting vulnerabilities in its cloud service.**
http://www.computerworld.com/s/article/9140074/Amazon_downplays_report_highlighting_vulnerabilities_in_its_cloud_service
9. **Targeted Attacks Possible in the Cloud, Researchers Warn.**
http://www.cio.com/article/506136/Targeted_Attacks_Possible_in_the_Cloud_Researchers_Warn
10. **Vulnerability Seen in Amazon's Cloud-Computing by David Talbot.**
<http://www.cs.sunysb.edu/~sion/research/sion2009mitTR.pdf>
11. **Cloud Computing Security Considerations by Roger Halbheer and Doug Cavit. January 2010.**
<http://blogs.technet.com/b/rhalbheer/archive/2010/01/30/cloud-security-paper-looking-for-feedback.aspx>
12. **Security in Cloud Computing Overview.**<http://www.halbheer.info/security/2010/01/30/cloud-security-paper-looking-for-feedback>
13. **Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds by T. Ristenpart, E. Tromer, H. Shacham and Stefan Savage. CCS'09**
14. **Cloud Computing Security.** <http://www.exforsys.com/tutorials/cloud-computing/cloud-computing-security.html>
15. **Update From Amazon Regarding Friday's S3 Downtime by Allen Stern. Feb. 16, 2008.**
<http://www.centernetworks.com/amazon-s3-downtime-update>
16. R. Ranchal, B. Bhargava, L.B. Othmane, L. Lilien, A. Kim, M. Kang, "Protection of Identity Information in Cloud Computing without Trusted Third Party," Third International Workshop on Dependable Network Computing and Mobile Systems (DNCMS) in conjunction with 29th IEEE Symposium on Reliable Distributed System (SRDS) 2010
17. P. Angin, B. Bhargava, R. Ranchal, N. Singh, L. Lilien, L.B. Othmane, "A User-Centric Approach for Privacy and Identity Management in Cloud Computing," 29th IEEE Symposium on Reliable Distributed System (SRDS) 2010
18. H. Khandelwal, *et al.*, "Cloud Monitoring Framework," Purdue University. Dec 2010.

