Cloud Computing:

Outsourcing Computation without Outsourcing Control

Richard Chow, PARC

Philippe Golle, PARC

Markus Jakobsson, PARC

Ryusuke Masuoka, Fujitsu

Jesus Molina, Fujitsu

Elaine Shi, PARC

Jessica Staddon, PARC

Outline

- Cloud Hype?
- Cloud Fear
- New Directions

Cloud Hype?

Larry Ellison: “What the Hell Is Cloud Computing?”

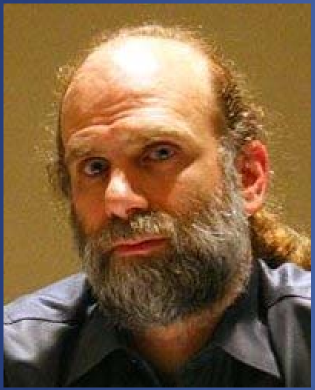
Larry Ellison - What The Hell Is Cloud Computing?

★★★★

Oracle CEO Larry Ellison

"What The Hell Is Cloud Computing?"

Richard Stallman: “It’s stupidity. It’s worse than stupidity: it’s a marketing hype campaign.”



Bruce Schneier: “Cloud computing is nothing new.”

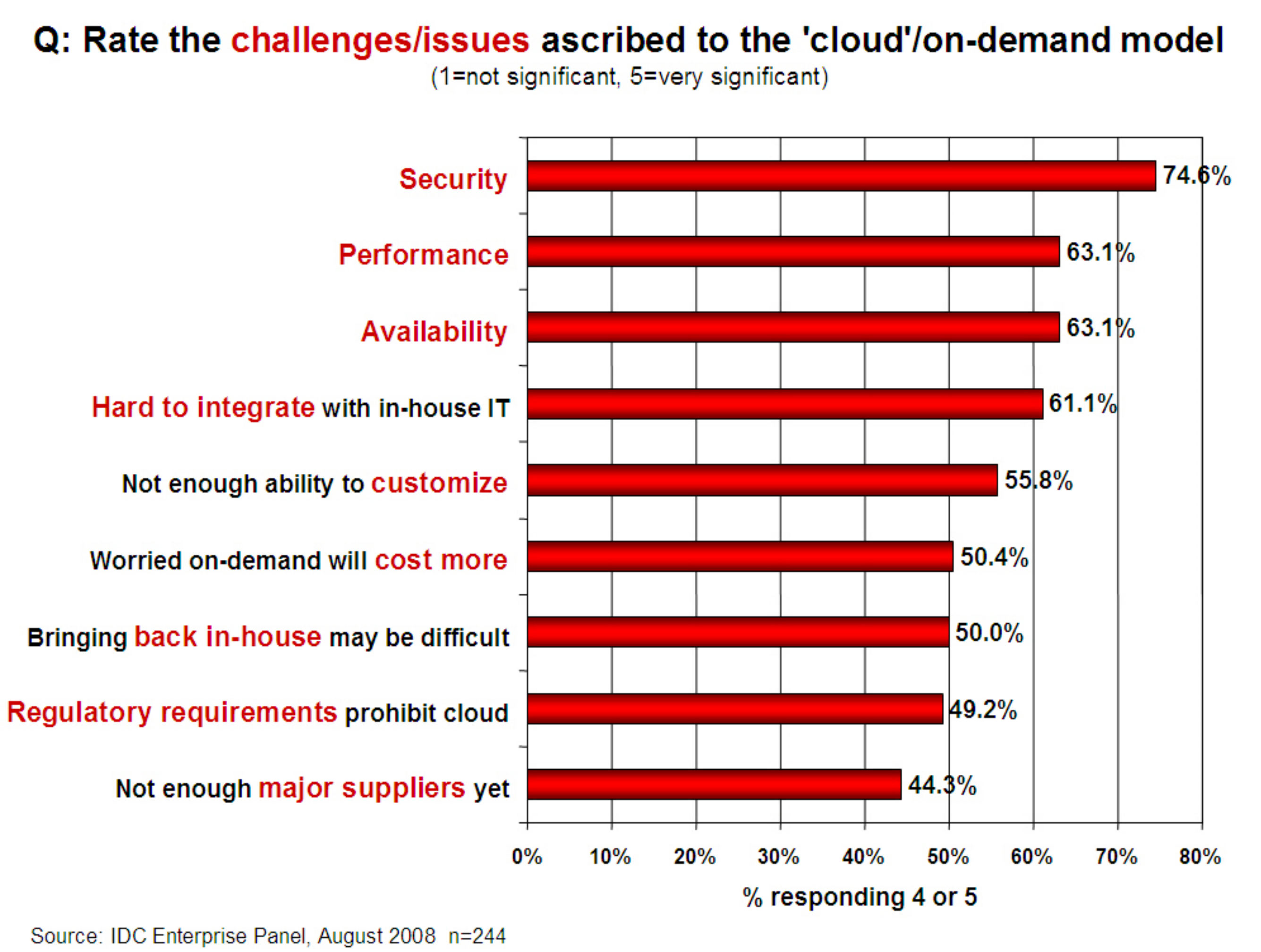
Ron Rivest: “[Cloud computing will become a] focal point in our work in security. I’m optimistic…”

UC Berkeley’s RAD Lab
Above the Clouds: A Berkeley View of Cloud Computing

“Cloud Computing is likely to have the same impact on software that foundries have had on the hardware industry”

“developers would be wise to design their next generation of systems to be deployed into Cloud Computing. “

Cloud Fear



Source: IDC Enterprise Panel, August 2008 n=244

Interviews by PARC

- Representatives from cloud ecosystem
- Concentrated on:
  - Cloud security problems
  - Security concerns of customers

Ecosystem Piece	Company	Interviewee
Cloud Provider	Amazon Web Services	Senior Manager Carl Moses
Cloud Application Builder	Model Metrics	CTO John Barnes
Cloud Application Platform	Startup	Architect
Cloud Monitoring Service	Hyperic	CEO Javier Soltero
Cloud User (Hybrid)	Fortune 500	Security Architect
Cloud User (Private)	Fortune 500	Security Architect

Interview Key Findings

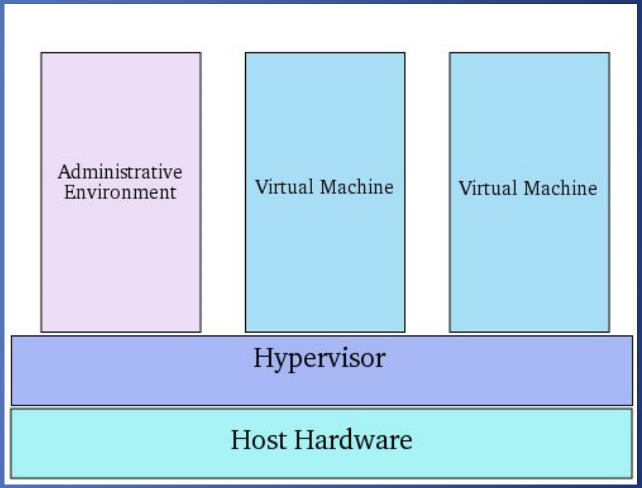
- Larger enterprises still cautious
  - Testing the waters with less sensitive data
- Uncertainty - early days of cloud computing
  - What will the new security problems be?
  - What will be the rules around regulatory compliance?
- General fear of loss of control in the cloud
  - Credibility and trust of cloud provider is critical

Taxonomy of Fear

- Traditional Security
  - Computer and network attacks made possible or easier after moving to cloud
- Availability
  - Applications and data being available for access
- Control of data by third-party
  - Lack of control and transparency when a third party holds the data

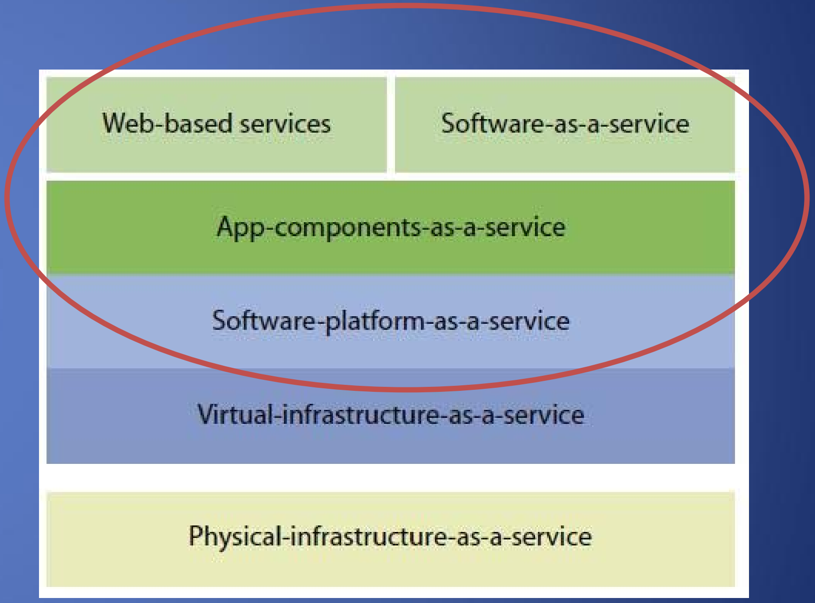
Traditional Security: VM-level Attacks

- Potential vulnerabilities in hypervisor or VMM
- Bigger problem in multi-tenant architectures
- Vulnerabilities have appeared in VMWare, Xen, and Microsoft's Virtual PC and Virtual Server



Traditional Security: Cloud Application

- Platform may have issues
  - SQL-injection or cross-site scripting vulnerability in salesforce.com or Google Apps
- Application itself may have issues
  - IBM repositioned Rational AppScan (vulnerability scanner for web services) as a cloud security service


Web-based services
Software-as-a-service
App-components-as-a-service
Software-platform-as-a-service
Virtual-infrastructure-as-a-service
Physical-infrastructure-as-a-service

Traditional Security: Phishing Cloud Provider

- New attack vector for social engineers: cloud provider employees

> We learned that a salesforce.com employee had been the victim of a phishing scam that allowed a salesforce.com customer contact list to be copied. To be clear, a phisher tricked someone into disclosing a password, but this intrusion did not stem from a security flaw in our application or database. Information in the contact list included first and last names, company names, email addresses, telephone numbers of salesforce.com customers……

salesforce.com e-mail to its customers

Traditional Security: Expanded Network Attack Surface

- Need to protect infrastructure used to connect and interact with the cloud
- Difficulty: Cloud is outside the firewall in many cases

Traditional Security: Authentication and Authorization

- How to extend authentication and authorization framework into cloud?
- How to merge cloud security data (if available) with your own?

Traditional Security: Forensics

- Standard practice
  - – Seize equipment
  - – Perform detailed analysis on the media
- Differences
  - – Scale of the cloud
  - – Rate of overwriting data

Availability

- Often-voiced concern
  - Although cloud providers argue their downtime compares well with cloud user’s own data centers
- Would cloud scale well-enough?

> *There are certain things that you cannot run in the cloud because the cloud would collapse…Don't believe that any utility company is going to run its billing for 50 million consumers in the cloud*

SAP CEO Leo Apotheker

Control of Data: Legal

- Due diligence
  - Can cloud provider respond in required time-frame?
  - Can a cloud user be guaranteed that data has been deleted?
- Contractual obligations may be surprising

10.4. Non-Assertion. During and after the term of the Agreement, with respect to any of the Services that you elect to use, you will not assert, nor will you authorize, assist, or encourage any third party to assert, against us or any of our customers, end users, vendors, business partners (including third party sellers on websites operated by or on behalf of us), licensors, sublicensees or transferees, any patent infringement or other intellectual property infringement claim with respect to such Services.

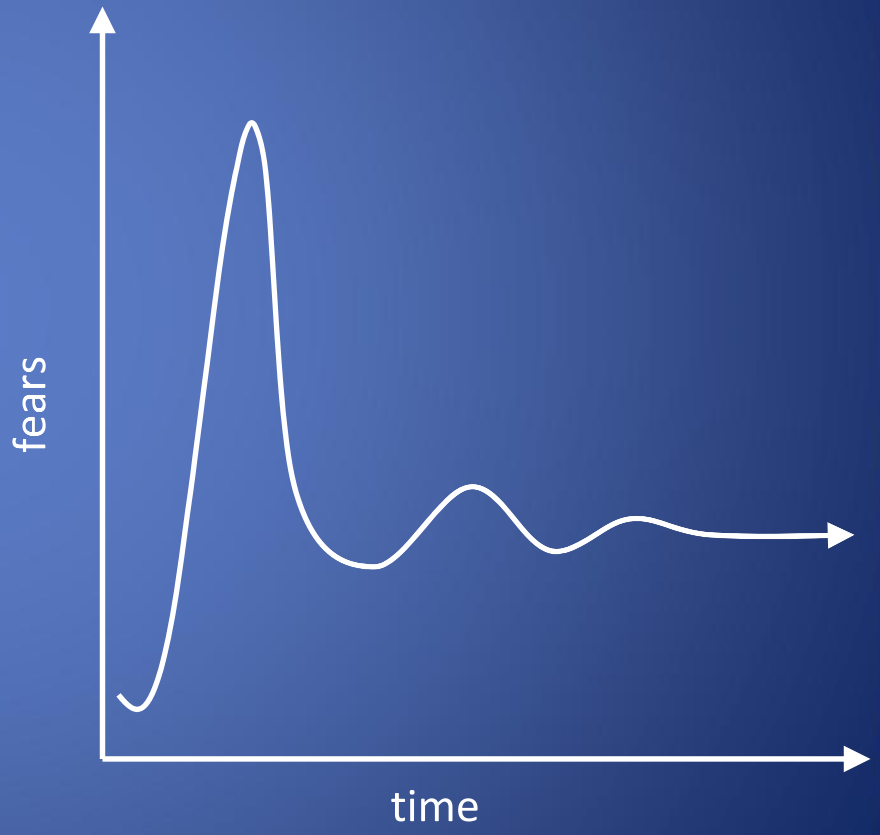
http://aws.amazon.com/agreement/

Control of Data: Auditability

- Transparency in operations for auditing purposes?
  - Currently, only by documentation and manual audits
- Lots of standards SAS 70 , SOX , HIPAA , FISMA, NIST, FIPS
  - Not written for the cloud
- Requirement for data and operations to remain in certain geographic locations

Control of Data: Theft by Cloud Provider

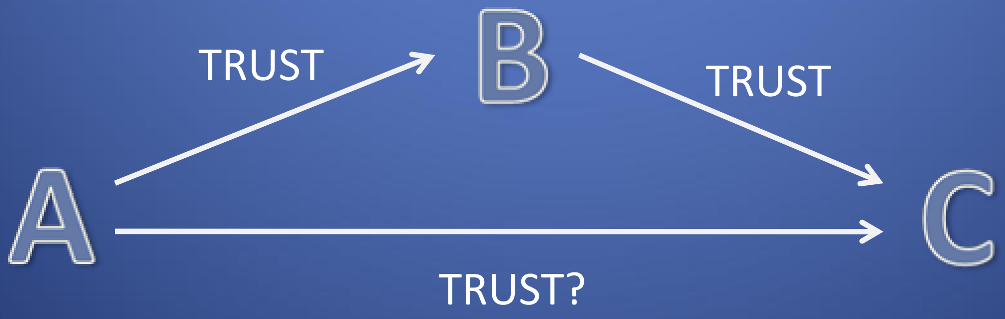
- Proprietary information in cloud
  - Corporate users of Google Gmail and Apps concerned about confidentiality of data
- Similar concerns for consumers seem to have faded
  - Dangers outweighed by value received



Control of Data: Transitivity

Cloud provider might use subcontractors, who also must be trusted

- The Linkup relied on Nirvanix (online storage company)
- Nirvanix lost their data, allegedly
- The Linkup shutdown



New Problem:
Cheap data and data analysis

- Enormous data sets monetized by applications such as advertising
- Clear impact to privacy - intense pressure on companies to anonymize their data
  - Fear of bad publicity from data breach
  - Fear of subpoenas
- Anonymizing data and retaining utility is difficult

New Problem:
Increased Demand for Authentication

- Authentication needs will increase
  - Personal, financial, medical data will now be hosted in the cloud
  - Software applications hosted in the cloud requires access control
- Need for higher-assurance authentication
  - Authentication in the cloud may mean authentication outside firewall
  - Limits of password authentication
    - Passwords are weak, not used, re-used, shared, lost, stolen, …
    - Password hard to type (limited input interface)
  - Mandates for two factor authentication
- Need for authentication from mobile devices with no/limited user involvement

Connect to

User name:

Password:

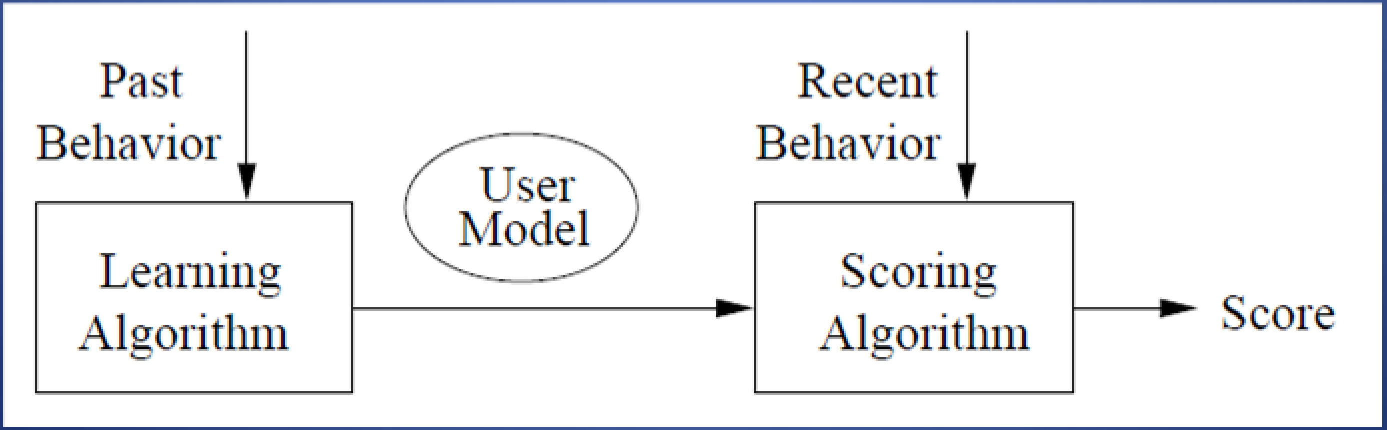
☑ Remember my password

Cloud Security Efforts

Implicit Authentication

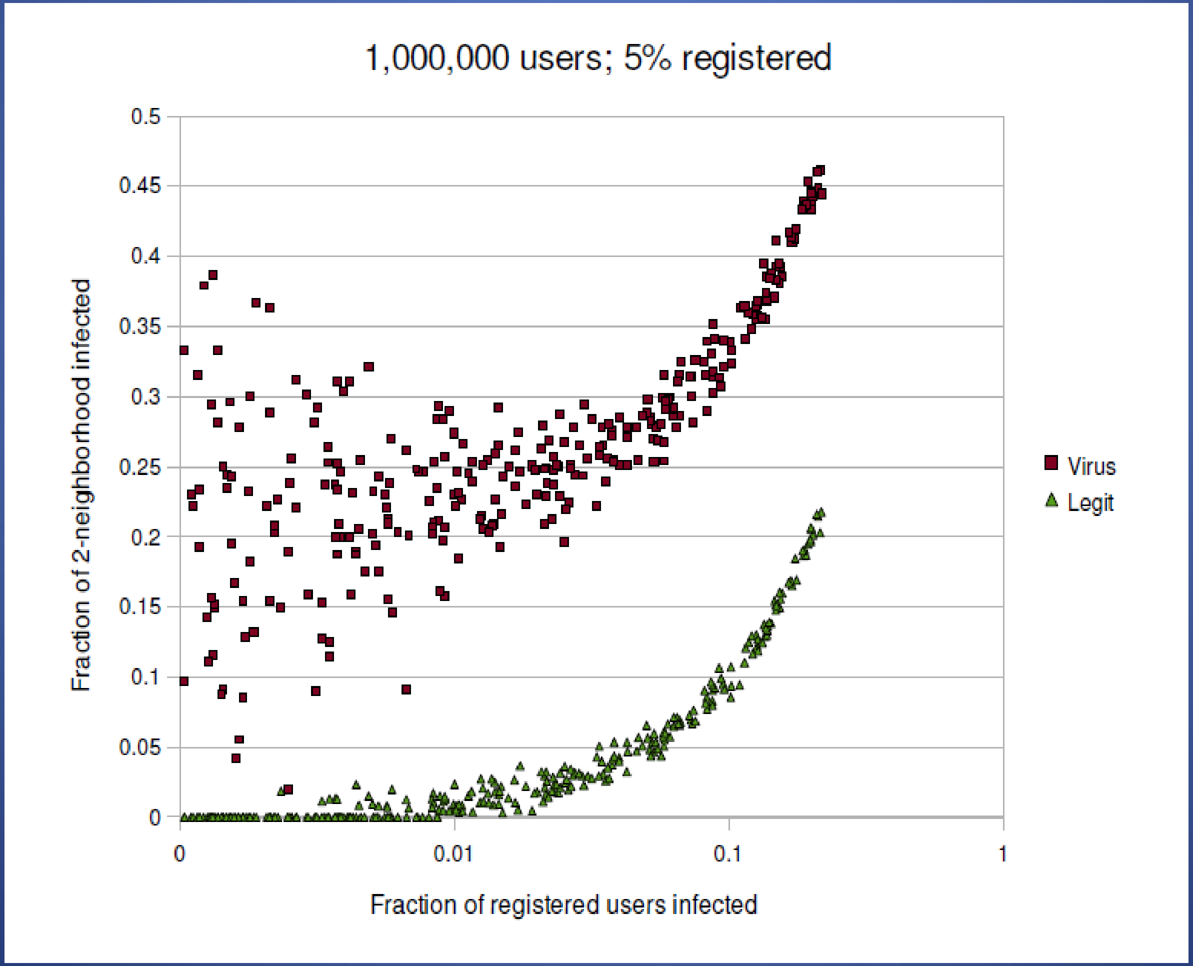
Vision: authenticate users implicitly based on observed behavior

- Location and co-location
- Application usage
- Biometric measurements
- Contextual data



Malware Detection through Cloud Data

Simulated propagation patterns:



Summary

- Cloud computing: most fashionable term in IT
  - But cloud fears remain
- Taxonomy of cloud fears
  - Traditional Security
  - Availability
  - Third-party possession of data
- Cloud brings new problems
  - Privacy and increased ease of data mining
  - Increased need for authentication
- Cloud Security Efforts
  - Implicit Authentication
  - Cloud Contextual Data

Questions or Comments?

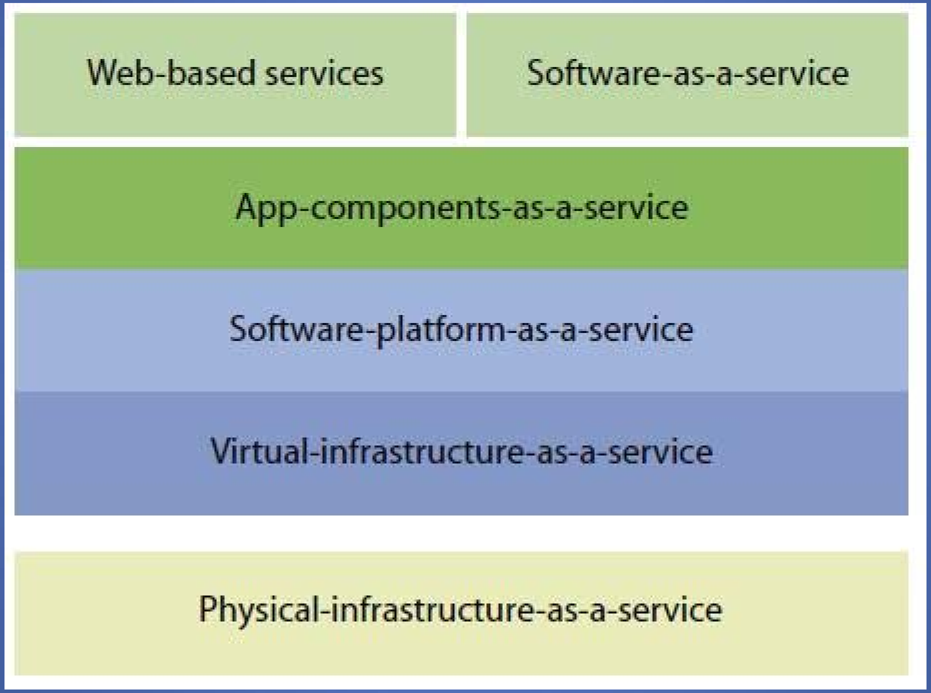
Backup

Clouds: Essential Characteristics

According to NIST

- On-demand self-service
- Broad network access
  - with standard protocols and heterogeneous platforms
- Resource pooling
- Rapid elasticity
- Measured services

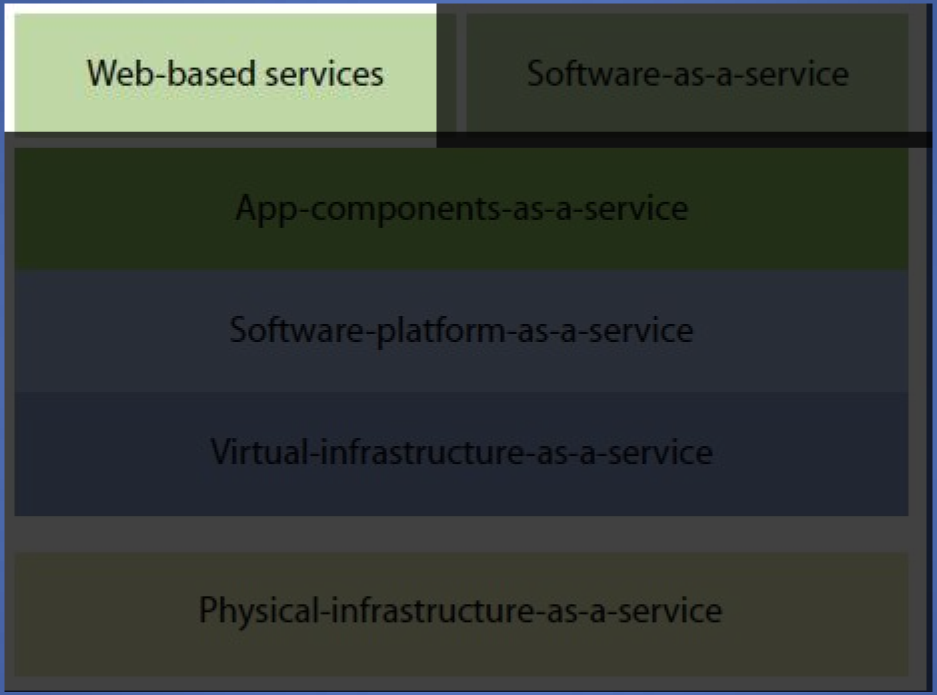
Service Models



Web-based services
Software-as-a-service
App-components-as-a-service
Software-platform-as-a-service
Virtual-infrastructure-as-a-service
Physical-infrastructure-as-a-service

Source: Forrester Research, Inc.

Web-based Services


Web-based services

Software-as-a-service

App-components-as-a-service

Software-platform-as-a-service

Virtual-infrastructure-as-a-service

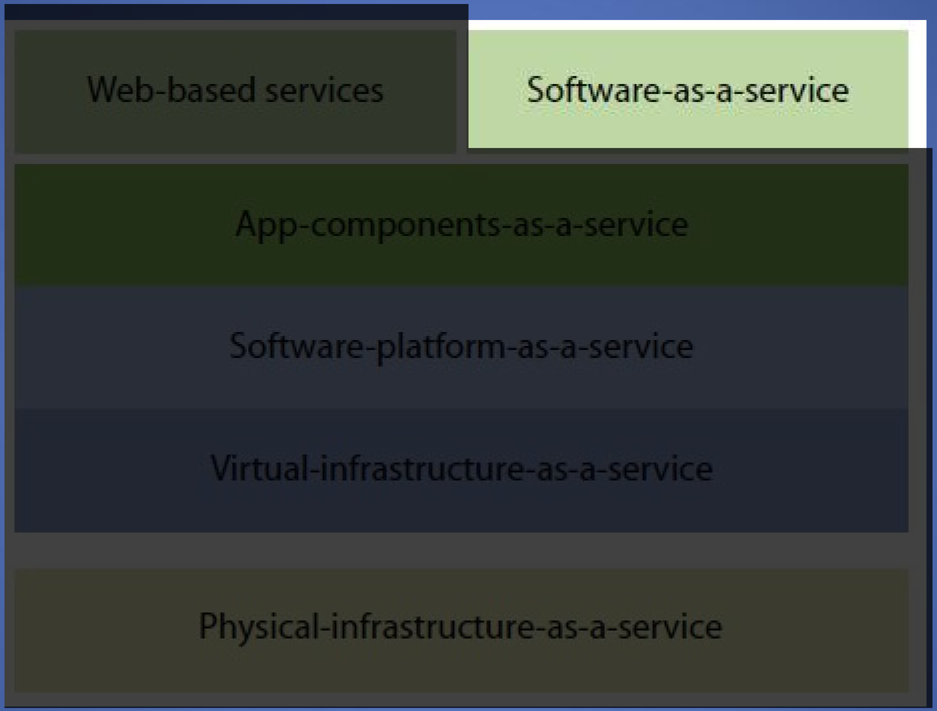
Physical-infrastructure-as-a-service

flickr™

facebook

Zillow.com®
Your Edge in Real Estate

Software-as-a-Service



Web-based services

Software-as-a-service

App-components-as-a-service

Software-platform-as-a-service

Virtual-infrastructure-as-a-service

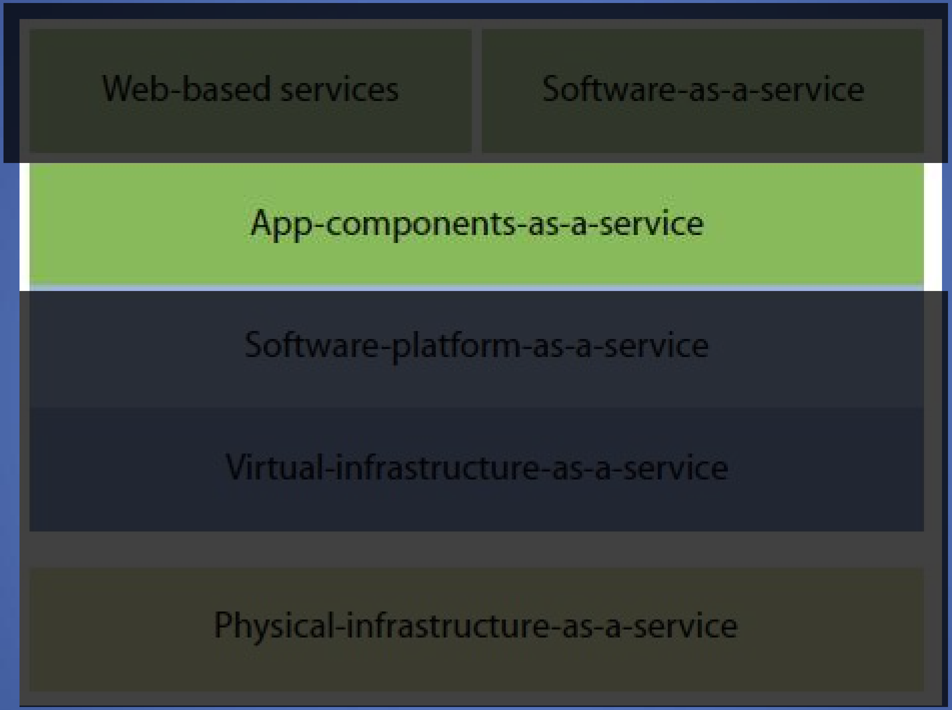
Physical-infrastructure-as-a-service

salesforce.com SOFTWARE Success On Demand.

webex weboffice

ZOHO Work. Online

App-Components-as-a-Service

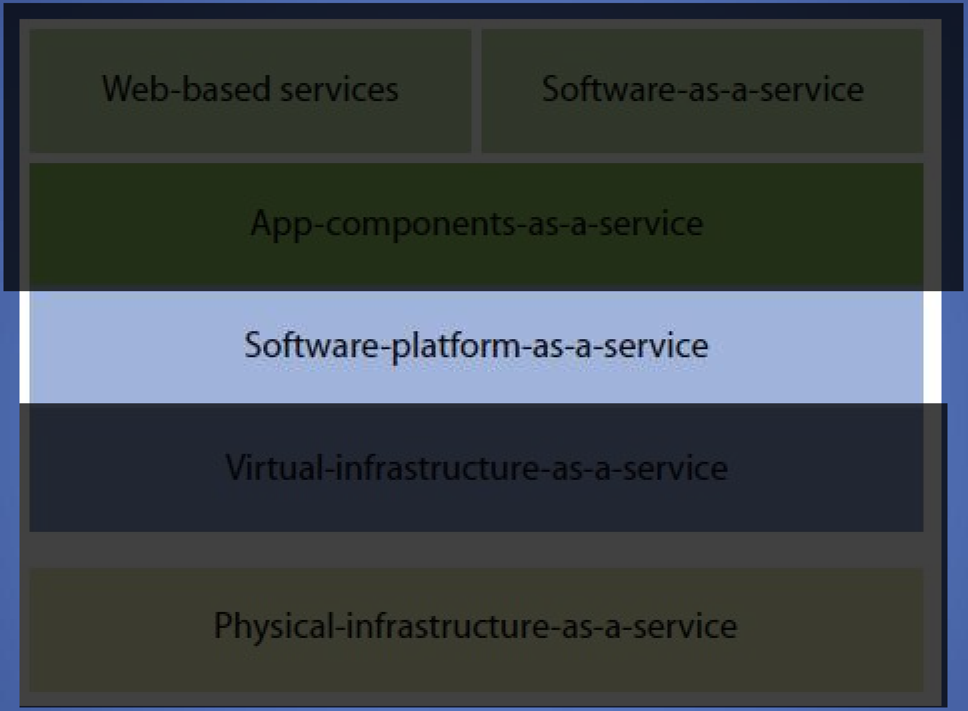

Web-based services
Software-as-a-service
App-components-as-a-service
Software-platform-as-a-service
Virtual-infrastructure-as-a-service
Physical-infrastructure-as-a-service

force.com Dream. Build. Succeed.

Google Apps

zembly

Software-Platform-as-a-Service



Web-based services

Software-as-a-service

App-components-as-a-service

Software-platform-as-a-service

Virtual-infrastructure-as-a-service

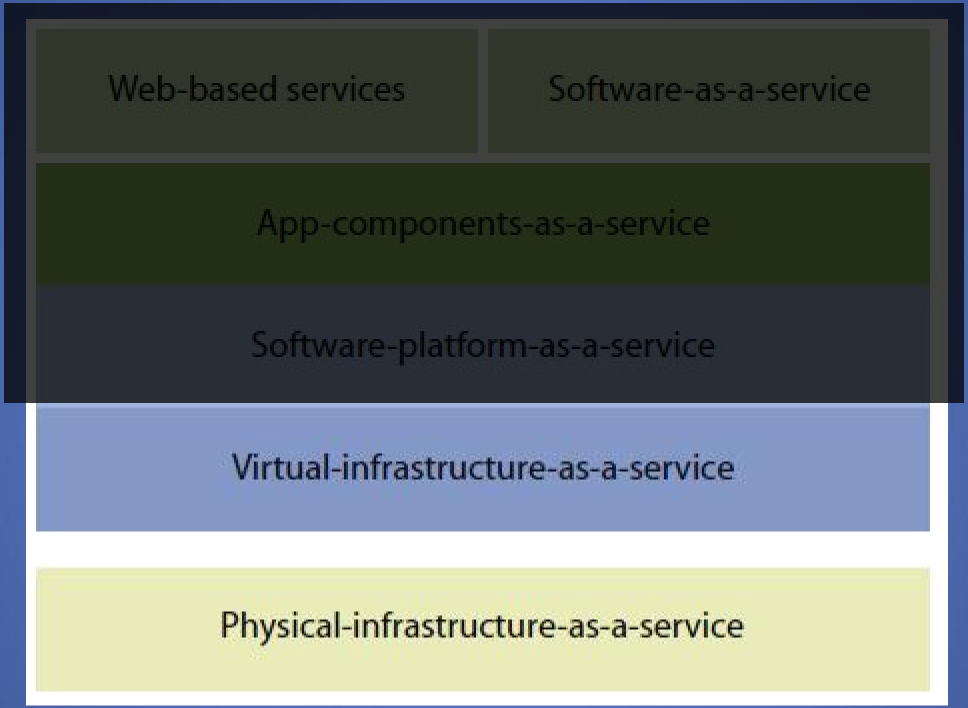
Physical-infrastructure-as-a-service

(Amazon S3)

(Google AppEngine)

(Microsoft Azure)

Infrastructure-as-a-Service



Web-based services

Software-as-a-service

App-components-as-a-service

Software-platform-as-a-service

Virtual-infrastructure-as-a-service

Physical-infrastructure-as-a-service

amazon web services™

(Amazon EC2)

MOSSO® the rackspace cloud

Other Players

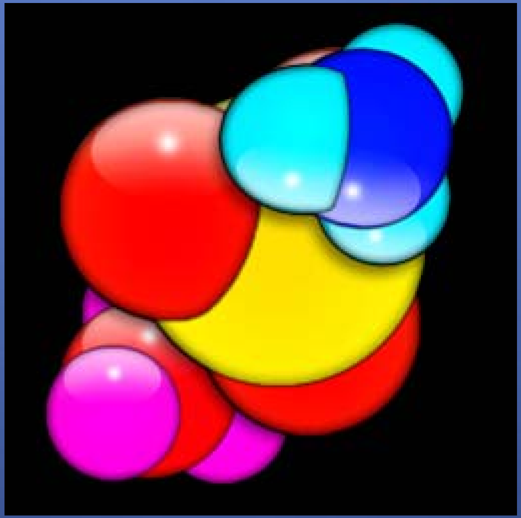
- Virtualization – server, network
- Storage
- Datacenter/ISP
- Optimization/Monitoring Tools
- Development Tools
- Services
- Industry Clouds
- R&D (Eucalyptus Public Cloud)

Deployment Models

- Public Cloud: Off-site, third-party provider
- Private Cloud: On premises, operated internally
- Hybrid Cloud: Multiple internal and/or external providers
  - “Typical for most enterprises”

Assurance of computational integrity

- Is cloud provider faithfully running hosted application?
- Example: Stanford's Folding@Home project gives same task to multiple clients



New Problem: Cost-effective availability

- Centralization of data implies more obvious attack targets and single points of failure – the cloud providers
- How to defend availability cheaply?

Applied Cryptography

- Old approach: Give cloud only encrypted data
- Issue: Limits uses for data, e.g. searching
- State-of-the-art cryptography offers new tools
  - Searchable encryption: respond to query without knowing query or data
  - Proofs of retrievability: prove all data correctly stored
  - Fully homomorphic encryption scheme: analysis of encrypted data without decrypting

Remote Server Integrity

- Higher assurance of cloud server integrity
  - Unalterable audit trails
  - Currently, only manual audit procedures
- Trusted Monitor to audit operations of cloud server
  - Based on Trusted Computing technology
  - Provides “proofs of compliance” to cloud user
  - Can be bootstrapped from Trusted Platform Module (TPM)
- Report back to cloud user securely with Remote Attestation
  - Uses Trusted Network Connect (TNC)