Security and Privacy in Cloud Computing

Ragib Hasan
Johns Hopkins University
en.600.412 Spring 2010

Lecture 1
01/25/2010
Welcome to the class

Administrative details

When? : Monday 3pm-3.50pm
Where?: Shaffer 202
Web: http://www.cs.jhu.edu/~ragib/sp10/cs412
Instructor: Ragib Hasan, 324NEB, rhasan7@jhu.edu
Office hours: Monday 4pm-5pm (more TBA)
Goals of the course

- **Identify** the cloud computing security issues
- **Explore** cloud computing security issues
- **Learn** about latest research
Plan

Each week, we will

– Pick a different cloud computing security topic
– Discuss general issues on the topic
– Read one or two latest research paper on that topic
Evaluations

Based on paper reviews

– Students taking the course for credit will have to submit 1 paper review per week

– The reviews will be short, 1 page discussion of the paper’s pros and cons (format will be posted on the class webpage)
What is **Cloud Computing**?

Let’s hear from the “experts”
What is **Cloud Computing**?

The infinite wisdom of the crowds (via **Google Suggest**)
What is **Cloud Computing**?

We’ve redefined Cloud Computing to include *everything that we already do.* . . . I don’t understand what we would do differently in the light of Cloud Computing other than change the wording of some of our ads.

---

Larry Ellison, founder of Oracle
What is **Cloud Computing**?

It’s *stupidity*. It’s worse than *stupidity*: it’s a marketing hype campaign.

---

**Richard Stallman**

GNU
What is **Cloud Computing**?

Cloud Computing will become a focal point of our work in security. I’m optimistic …

**Ron Rivest**  
The **R** of RSA
So, What really is **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

That is, use as much or as less you need, use only when you want, and pay only what you use,
The **real** story

“Computing Utility” – holy grail of computer science in the 1960s. Code name: MULTICS

Why it failed?

• Ahead of time ... lack of communication tech. (In other words, there was NO (public) Internet)

• And personal computer became cheaper and stronger
Mid to late ’90s, Grid computing was proposed to link and share computing resources.
The real story ... continued

Post-dot-com bust, big companies ended up with large data centers, with low utilization

Solution: Throw in virtualization technology, and sell the excess computing power

And thus, Cloud Computing was born ...
Cloud computing provides numerous economic advantages

For clients:

– No upfront commitment in buying/leasing hardware
– Can scale usage according to demand
– Barriers to entry lowered for startups

For providers:

– Increased utilization of datacenter resources
Cloud computing means **selling “X as a service”**

**IaaS**: Infrastructure as a Service  
– Selling virtualized hardware

**PaaS**: Platform as a service  
– Access to a configurable platform/API

**SaaS**: Software as a service  
– Software that runs on top of a cloud
Cloud computing architecture

- **Users Interface**
  - **User Interface**
  - **Machine Interface**

- **Application**
  - **SaaS**, e.g., Google Docs
  - **PaaS**, e.g., Google AppEngine
  - **IaaS**, e.g., Amazon EC2

- **Platform**
- **Infrastructure**
  - **Compute**
  - **Network**
  - **Storage**
  - **Servers**

  - e.g., Web browser
Different types of cloud computing

IaaS

Amazon EC2
Clients can rent virtualized hardware, can control the software stack on the rented machines

Microsoft Azure
Clients can choose languages, but can’t change the operating system or runtime

PaaS

Google AppEngine
Provides a programmable platform that can scale easily
So, if cloud computing is so great, why aren’t everyone doing it?

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)

- **Security**: 74.6%
- **Performance**: 63.1%
- **Availability**: 63.1%
- **Hard to integrate with in-house IT**: 61.1%
- **Not enough ability to customize**: 55.8%
- **Worried on-demand will cost more**: 50.4%
- **Bringing back in-house may be difficult**: 50.0%
- **Regulatory requirements prohibit cloud**: 49.2%
- **Not enough major suppliers yet**: 44.3%

Source: IDC Enterprise Panel, August 2008  n=244
Anatomy of fear ...

Confidentiality

– Will the sensitive data stored on a cloud remain confidential? Will cloud compromises 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?
Anatomy of **fear** ...

**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?
Anatomy of fear ...

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?
Anatomy of fear ...

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
Anatomy of fear ...

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
Anatomy of fear ...

Auditability and forensics

– Difficult to audit data held outside organization in a cloud

– Forensics also made difficult since now clients don’t maintain data locally
Anatomy of fear ...

Legal quagmire 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?
What we need is to ... 

• Adapt well known techniques for resolving some cloud security issues
• Perform new research and innovate to make clouds secure
[Cloud Computing] is a security nightmare and it can't be handled in traditional ways.

John Chambers
CISCO CEO
Further Reading
