INDIAN INSTITUTE OF INFORMATION TECHNOLOGY

Dharwad
ज्ञानेन विकासः

Cloud Regulatory, Privacy, and Security

Dr. Animesh Chaturvedi

Assistant Professor: IIIT Dharwad

Young Researcher: Heidelberg Laureate Forum

Postdoc: King's College London & The Alan Turing Institute

PhD: IIT Indore MTech: IIITDM Jabalpur

HEIDELBERG LAUREATE FORUM

KING'S College LONDON

Indian Institute of Technology Indore
भारतीय प्रौद्योगिकी संस्थान इंदौर

PDPM
Indian Institute of Information Technology, Design and Manufacturing, Jabalpur

The Alan Turing Institute

Regulatory Issues

Regulating Issues

Now almost every part of computer science is influenced by Cloud Computing. Concerns related to

1. Infrastructure
2. Access control, Identity management & Integrity control
3. Risk management
4. Legislative compliance & Jurisdiction
5. Auditing and logging
6. Loss of control over data, data protection, international data transfer (specially sensitive data).
7. Dependence on the Cloud Computing provider & Vendor dependent risks.
8. Fair information practices

Hölbl, Marko. "Cloud Computing Security and Privacy Issues."
The Council of European Professional Information Societies (CEPIS) (2011).

10 Obstacles and Opportunities

1. Availability of Service
2. Data Lock-In
3. Data Confidentiality and Auditability
4. Data Transfer Bottlenecks
5. Performance Unpredictability
6. Scalable Storage
7. Bugs in Large-Scale Distributed Systems
8. Scaling Quickly
9. Reputation Fate Sharing
10. Software Licensing

Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." *National Institute of Standards and Technology* 53.6 (2009): 50.

Availability of a Service

- Successful concept "no single source of failure", but single company is in fact a single point of failure.
- What if the company may even go out of business?
  - Then Multiple datacenters in different regions does not work.
- Thus, Cloud vendor must fulfill a business-continuity strategy agreements.
- A **distributed denial-of-service** (**DDoS**) attack is one in which a multitude of compromised systems attack a single target, thereby causing **denial of service** for users of the targeted system.

Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." *National Institute of Standards and Technology* 53.6 (2009): 50.

Data Lock-In

- Customers cannot easily extract their data and programs from one site to run on another. Concern about the difficult of extracting data from the cloud is preventing some organizations from adopting Cloud Computing.
- Suppose an online storage service is shut down user will loss access to its data.
- Solution: Standardize the APIs so that a SaaS developer could deploy services and data across. Put the data on multiple cloud providers so that the failure of a single company would not take all copies of customer data.
- The solution will result in "reduction in cloud pricing and flatten the profits". But still the quality of a service matters as well as the price.
- Standard API will result in usage of same software in a Private Cloud and Public Cloud.

Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." *National Institute of Standards and Technology* 53.6 (2009): 50.

Data Confidentiality and Audit

- Organization sensitive data are rarely in cloud.
- Need of proper encrypted storage, Virtual Local Area Networks, and network middleboxes (e.g. firewalls, packet filters).
- Encrypt data before placing it in a Cloud may be even more secure than unencrypted data in a local data center.
- Auditability could be added as an additional layer.
- Many nations have laws requiring SaaS providers to keep customer data and copyrighted material within national boundaries.
- Some businesses may not like the ability of a country to get access to their data.
- European customer might be concerned about using SaaS in the United States.
- Flexibility to place the storage. Like Amazon allowing providers to keep data in whichever they choose physically in United States and Europe,.

Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." *National Institute of Standards and Technology* 53.6 (2009): 50.

Data Transfer Bottlenecks

For data-intensive application, data placement and transport across the boundaries of clouds, may be complicate.

Data transfer costs is an important issue

- Overcome the high cost of Internet transfers is to ship disks.
  - Assume that we want to ship 10 TB from X to Y. Suppose measured bandwidth average found to be 20 Mbit/sec.

  It would take
  10 * 10^12 Bytes /(20 × 10^6 bits/second)
  = (8 × 10^13) /(2 × 10^7) seconds = 4,000,000 seconds,
  = 45 plus days.

  Very high network transfer fees for this data.

Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." *National Institute of Standards and Technology* 53.6 (2009): 50.

Data Transfer Bottlenecks cont..

Put data in cloud, provide services that needs to purchase of Cloud Computing cycles. Thus reduce bottlenecks, For example

1. **Host large public datasets** (like Census data, images etc) for free, these datasets may "attract" customers to purchase cloud computing cycles.
2. **For backup services.** Companies have more data to send than as compared they receive, in weekend they can move full backups by shipping physical disks.
3. **For archived data** is in the cloud, service could result in selling Cloud Computing cycles, like creating search index of archival data or performing image recognition on archived photos.

Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." *National Institute of Standards and Technology* 53.6 (2009): 50.

Performance Unpredictability

- Sharing of CPUs and memory through VM can be done easily, but when we need to share I/O efficiently, then it is not easy.
- Scope of improvement in interrupts and I/O management in Cloud Computing. Using flash (semiconductor memory) is a possible solution.
- Scope of improvement in batch processing deployment at VMs.
- Scope of implementation of a visual Cloud process monitor, that can show the running threads of a program concurrently.

Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." *National Institute of Standards and Technology* 53.6 (2009): 50.

Scalable Storage

- How to apply "*short-term usage, no up-front cost, and infinite capacity on-demand*" to Persistent storage.

1. Varying in the richness of the query and storage API's
2. Performance guarantees
3. Complexity of data structures that are directly supported by the storage system (e.g., schema-less blobs vs. column-oriented storage).
4. Create a storage system would not only meet these needs but combine them with the cloud advantages of scaling arbitrarily up and down on-demand, as well as meeting programmer expectations in regard to resource management for scalability, data durability, and high availability.

Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." *National Institute of Standards and Technology* 53.6 (2009): 50.

Bugs in Large-Scale Distributed Systems

- Difficult challenges in Cloud Computing is removing errors in these very large scale distributed systems.
- These bugs are not easily be reproduced in smaller configurations. Thus most of time debugging occur at datacenters.

Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." *National Institute of Standards and Technology* 53.6 (2009): 50.

Scaling Quickly

- Pay-as-you-go certainly applies to CPU, storage and network bandwidth. Scales in response to load increases or decreases without violating service level agreements.
- For example
  - Google AppEngine: users are charged by the cycles.
  - AWS user are charges by the hour for the number of instances.
- Reason for scaling is to conserve resources as well as money. Idle computer uses about two-thirds of the power of a busy computer. Thus, optimize idle computers can reduce datacenters cost.
- Programmers need to pay attention to efficiency per cycle.
- Sometime it is better to leave machines idle overnight to avoid reconfiguring the work next day.

Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." *National Institute of Standards and Technology* 53.6 (2009): 50.

Reputation Fate Sharing

- Bad behavior of a customer's can affect the reputation of the cloud.
- Create reputation-guarding services similar to the "trusted email" services.
- Company sending the spam should be held liable, not the cloud vendor.

Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." *National Institute of Standards and Technology* 53.6 (2009): 50.

Software Licensing

- Some Cloud providers are dependent on open source software because open source licensing model are more flexible than for commercial software.
- Licensing changes needed for open source or commercial software to remain popular with Cloud.
- Two companies may collaborate to offer pay-as-you-go software licensing on Cloud.

Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." *National Institute of Standards and Technology* 53.6 (2009): 50.

Opportunities in Cloud

1, 2, 3 are technical obstacles to *adopt* Cloud Computing, 4, 5, 6, 7, 8 are technical obstacles to the *growth* of Cloud Computing after adoption and 9, 10 are *policy and business* obstacles to the *adoption* of Cloud Computing.

	Obstacle	Opportunity
1	Availability of Service	Use Multiple Cloud Providers to provide Business Continuity; Use Elasticity to Defend Against DDOS attacks
2	Data Lock-In	Standardize APIs; Make compatible software available to enable Surge Computing
3	Data Confidentiality and Auditability	Deploy Encryption, VLANs, and Firewalls; Accommodate National Laws via Geographical Data Storage
4	Data Transfer Bottlenecks	FedExing Disks; Data Backup/Archival; Lower WAN Router Costs; Higher Bandwidth LAN Switches
5	Performance Unpredictability	Improved Virtual Machine Support; Flash Memory; Gang Scheduling VMs for HPC apps
6	Scalable Storage	Invent Scalable Store
7	Bugs in Large-Scale Distributed Systems	Invent Debugger that relies on Distributed VMs
8	Scaling Quickly	Invent Auto-Scaler that relies on Machine Learning; Snapshots to encourage Cloud Computing Conservationism
9	Reputation Fate Sharing	Offer reputation-guarding services like those for email
10	Software Licensing	Pay-for-use licenses; Bulk use sales

Mell, Peter, and Tim Grance. "The NIST definition of cloud computing." *National Institute of Standards and Technology* 53.6 (2009): 50.

Privacy concerns

Cloud computing privacy concerns

- Service provider may access the data.
- Accidental or deliberated alteration or deletion of information.
- Many cloud providers may share information with third parties if necessary for purposes of law and order even without a informing clients. It is legal because client need to accept the privacy policies before they start using the cloud services.
- Possible solutions strict auditing and inclusion of privacy policy and legislation. Users can encrypt data before storing it in the cloud to prevent read operation.
- Legal ownership of the data (How is the owner of data cloud provider or consumer). Many terms of service agreements are required for this.

Cloud computing privacy concerns

- Physical control on the computers in private cloud is more secure than in public cloud.
- Public cloud service needs to make secure building to maintain secure services. Useful for small businesses (specially non-expertise in IT security).
- Naive users do not understand or read the terms of service and “Accept” the agreement.
- Private cloud is normally secure. But public cloud is flexible, on up-front cost and with less time to start.

NIST Guidelines, GDPR, CDN Security

NIST Guidelines: Security And Privacy

Carefully plan before engaging

- Organizational data, applications, and other resources should be in accord with the organization's security objectives.
- Consider security and privacy throughout the system life cycle
  - application development and service provisioning,
  - design, implementation, testing, use,
  - and monitoring of deployed or engaged services, then system disposition.

Radack, Shirley. *Guidelines For Improving Security And Privacy In Public Cloud Computing*. No. ITL Bulletin March 2012. National Institute of Standards and Technology, 2012.

NIST Guidelines: Security And Privacy

Public cloud computing environment

- Security and privacy issues after implementation and deployment is more difficult, expensive, and exposes unnecessary risk
- Assess the security and privacy risks, organizations should examine the policies, procedures, and technical controls used by a cloud provider,
- Continuous monitoring for risk management and helps organizations
  - to maintain security, vulnerabilities, and threats
  - to support organizational risk management decisions.

Radack, Shirley. *Guidelines For Improving Security And Privacy In Public Cloud Computing*. No. ITL Bulletin March 2012. National Institute of Standards and Technology, 2012.

NIST Guidelines: Security And Privacy

Satisfies organizational requirements

Negotiated agreements:

- vetting of employees,
- data ownership and
- exit rights,
- breach notification,
- isolation of tenant applications,
- data encryption and segregation,
- tracking and reporting service effectiveness,
- compliance with laws and regulations, and
- the use of validated products that meet federal or national standards.

Radack, Shirley. *Guidelines For Improving Security And Privacy In Public Cloud Computing*. No. ITL Bulletin March 2012. National Institute of Standards and Technology, 2012.

NIST Guidelines: Security And Privacy

Client-side requirements

- Following runs on a client device undermines the security and privacy of public cloud services as well as other Internet facing public services
  - A backdoor Trojan,
  - keystroke logger, or
  - other type of malware
- Organizations should
  - review measures of cloud computing security architecture and
  - employ additional measures needed to secure the client side.

Radack, Shirley. *Guidelines For Improving Security And Privacy In Public Cloud Computing*. No. ITL Bulletin March 2012. National Institute of Standards and Technology, 2012.

NIST Guidelines: Security And Privacy

Maintain accountability in public cloud

- Organizations should
  - monitor assets,
  - assess implementation of policies, standards, procedures, controls,
  - guidelines that establish and protect the confidentiality, integrity, and availability of information system resources.
- Continuous monitoring of security involves maintaining
  - awareness of privacy and security controls, vulnerabilities, and threats
- Monitoring of
  - the security of networks, information, and
  - systems can respond by accepting, avoiding, or
  - mitigating risk as situations change.

Radack, Shirley. *Guidelines For Improving Security And Privacy In Public Cloud Computing*. No. ITL Bulletin March 2012. National Institute of Standards and Technology, 2012.

General Data Protection Regulation (GDPR)

- GDPR is a regulation in European Union (EU) law on data protection and privacy in
  - the EU and
  - the European Economic Area (EEA).
- Addresses the transfer of personal data outside
  - the EU and
  - EEA areas.
- The GDPR's primary aim is to give control and individuals over their personal data
  - Made by European Parliament and
  - Council of the EU

https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
https://gdpr-info.eu/

General Data Protection Regulation (GDPR)

- Regulation applies to following based in the EU region
  - the data controller (an organization that collects data from EU residents), or
  - processor (an organization that processes data on behalf of a data controller like cloud service providers), or
  - the data subject (person).

https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
https://gdpr-info.eu/

General Data Protection Regulation (GDPR)

Unless a data subject has provided informed consent to data processing for one or more purposes, personal data may not be processed unless there is at least one legal basis to do so. **Article 6** States the lawful purposes are:

(a) If the data subject has given consent to the processing of his or her personal data;

(b) To fulfill contractual obligations with a data subject, or for tasks at the request of a data subject who is in the process of entering into a contract;

(c) To comply with a data controller's legal obligations;

(d) To protect the vital interests of a data subject or another individual;

(e) To perform a task in the public interest or in official authority;

(f) For the legitimate interests of a data controller or a third party, unless these interests are overridden by interests of the data subject or her or his rights according to the Charter of Fundamental Rights (especially in the case of children).

https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
https://gdpr-info.eu/

CDN Security and Privacy

- CDN provider's profit
  - either by content providers using their network,
  - or from the user analytics and tracking data:
- Threat 1:
  - Potential privacy intrusion to do behavioral targeting.
  - Same-Origin policy: "permits scripts if pages have the same *origin* (combination of URI scheme, host name, and port number)."

https://en.wikipedia.org/wiki/Content_delivery_network

CDN Security and Privacy

- CDN provider's profit
  - either by content providers using their network,
  - or from the user analytics and tracking data:
- Threat 2:
  - CDN networks serving JavaScript can be target to inject malicious code into content.
  - Subresource Integrity: ensures the content is known and constrained to a hash reference by the website.

https://en.wikipedia.org/wiki/Content_delivery_network

Conclusion

- How other technology had contributed in the evolution of cloud computing technology.
- Strength of hardware's & impact of new type of distributed software infrastructure's.
- Different clouds: private, public, hybrid and community.
- Various cloud services available in the public.
- Introduction of applications layer.
- Explored some risk issues with security and privacy involved with cloud.
- Regulatory issues in cloud with their limitations.
- Obstacle as well as opportunity in those obstacles.

https://sites.google.com/site/animeshchaturvedi07/academic-teaching/cloudcomputing

תודה רבה
Hebrew

Ευχαριστώ
Greek

Спасибо
Russian

Danke
German

धन्यवादः
Sanskrit

Merci
French

ধন্যবাদ
Bangla

நன்றி
Tamil

شكراً
Arabic

ಧನ್ಯವಾದಗಳು
Kannada

Thank You
English

നന്ദി
Malayalam

多謝
Traditional Chinese

Grazie
Italian

ధన్యవాదాలు
Telugu

આભાર
Gujarati

ਧੰਨਵਾਦ
Punjabi

धन्यवाद
Hindi & Marathi

多谢
Simplified Chinese

Gracias
Spanish

https://sites.google.com/site/animeshchaturvedi07

Obrigado
Portuguese

ありがとうございました
Japanese

ขอบคุณ
Thai

감사합니다
Korean