Data Privacy and Cloud Computing

Patricia Serrano Alvarado
Université de Nantes
LINA Laboratory
http://www.univ-nantes.fr/serrano-p

Outline

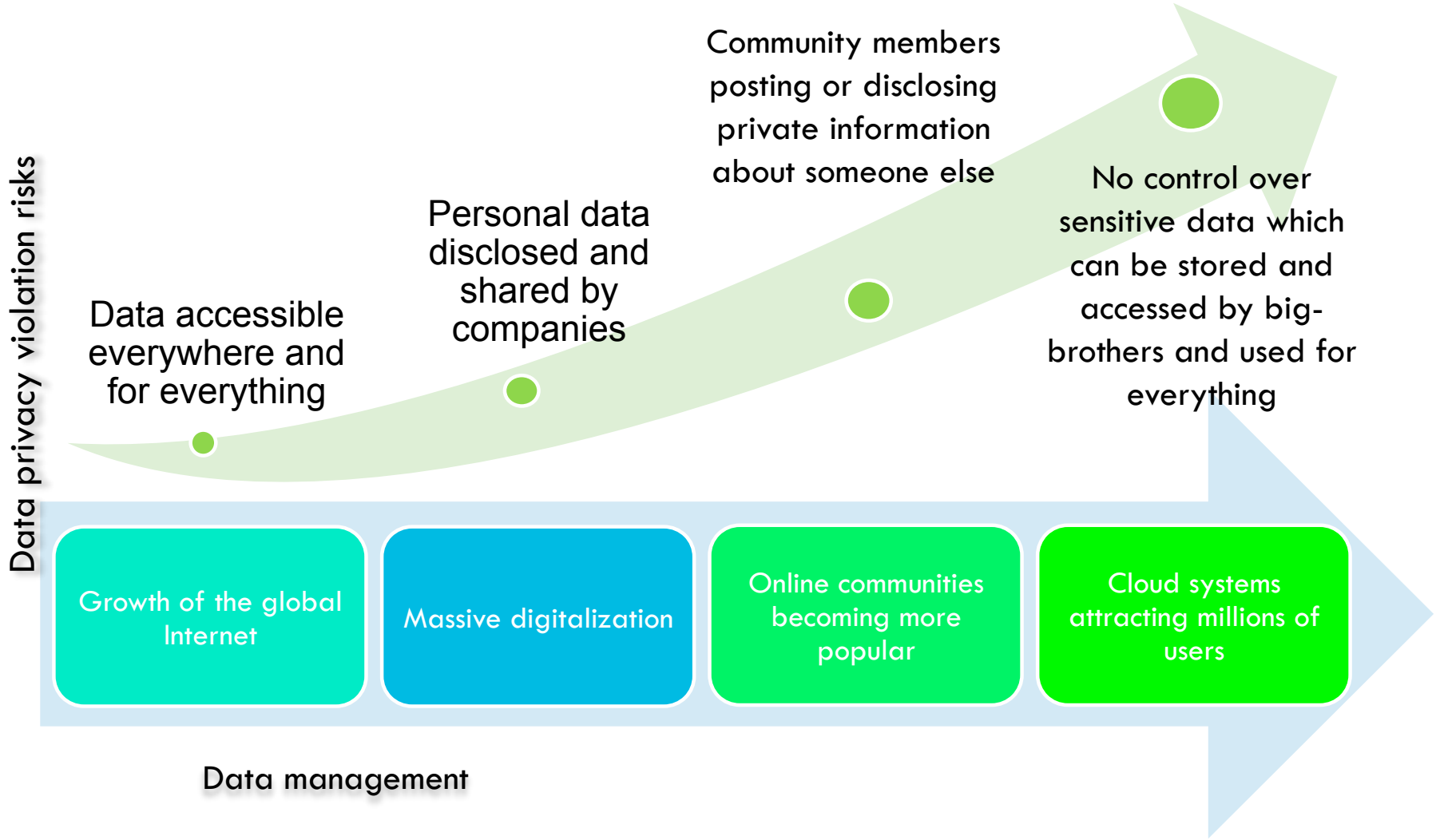
- Data privacy needs
- Cloud Computing at a glance
- Cloud computing : opportunities and challenges

Privacy

- Is the right of individuals to determine for themselves when, how and to what extent information about them is communicated to others

Alain Westin, Professor Emeritus
of Public Law and Government, Columbia University
Westin, A.F.: Privacy and Freedom. Atheneum, New York, USA (1967)

Growth of privacy concerns



Some privacy-related guidelines and legislations

- The OECD Privacy Guidelines in Europe
- Directive 95/46/EC of the European Parliament
- *Loi Informatique et Libertés* n°78-17
- The CNIL in France
- The Canadian Privacy Act and the Personal Information Protection and Electronic Documents Act
- The Health Insurance Portability and Accountability Act (HIPAA)
- Gramm-Leach-Bliley Consumer Privacy Rule

OECD guidelines

- 8 principles
  1. Collection Limitation Principle
  2. Data Quality Principle
  3. Purpose Specification Principle
  4. Use Limitation Principle
  5. Security Safeguards Principle
  6. Openness Principle
  7. Individual Participation Principle
  8. Accountability Principle

Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)
http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

"OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" since 1980.

CNIL

Personal Data : definition

What is personal data?

According to the law, **personal data means any information relating to an identified or identifiable individual**; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number (e.g. social security number) or one or more factors specific to his physical, physiological, mental, economic, cultural or social identity (e.g. name and first name, date of birth, biometrics data, fingerprints, DNA…)

Definition

To define personal data, account must be taken of all the means available to the "data controller" to determine whether a person is identifiable.

Personal data are any anonymous data that can be double checked to identify a specific individual (e.g. fingerprints, DNA, or information such as "the son of the doctor living at 11 Belleville St. in Montpellier does not perform well at school").

Information and communication technology generate a growing amount of increasingly accurate data about us (credit card payment, calls made from a cell phone allowing to identify with a 430 yards accuracy the place where the caller is, an internet connection)

Personal data represent a great deal of commercial worth. As a result they are increasingly sought after : files are bought and sold, commercial groups may be tempted to identify and group in one file "good clients" of each of their subsidiaries, or "bad clients".

The "traces" left by IT uses are increasingly easy to exploit, due to software improvements (e.g. internet search engine technology, or data "searching" software).

CNIL

Official Texts

French legislation

ACT N°78-17

ACT N°78-17 Amended by the act of 6 august 2004 relating to the protection of individuals with regard to the processing of personal data

(last update : Ordinance No.2011-1012 dated 24/08/2011)

Decree No 2005-1309

Decree No 2005-1309 of 20 October 2005 enacted for the application of Act No 78-17 of 6 January 1978 on Data Processing, Files and Individual Liberties amended by Act No 2004-801 of 6 August 2004

European legislation

Directive 95/46/EC

Directive 95/48/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

Directive 2009/136/EC

Directive 2009/136/EC of the European Parliament and of the council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws (Text with EEA relevance)

Convention 108

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

CNIL

Guides

La CNIL en bref
PDF - 461 Ko

© CNIL 2013

Guide "Gestion des risques vie privée"
Partie I : Méthode pour gérer les risques - PDF - 2.7 Mo

© CNIL 2012

Mesurer pour progresser vers l'égalité des chances
Version feuilletable

© CNIL, défenseur des droits 2012

Guide "Gestion des risques vie privée"
Partie II : catalogue de mesures - PDF - 2.8 Mo

© CNIL 2012

Guide téléphonie
Version PDF

© CNIL 2012

Guide communication politique
Version PDF

© CNIL 2012

Guide La pub si je veux
Version feuilletable

© CNIL 2011

Guide des Avocats
PDF - 1.38 Mo - 68 pages

© CNIL 2011

Guide des professionnels de santé
PDF

© CNIL 2011

Guide Enseignement
PDF

© CNIL 2011

Guide Sécurité des données personnelles
Version PDF

© CNIL 2010

Guide droit d'accès
Version PDF

© CNIL 2010

CNIL - biomedical data

- Act No 74-17, Article 8
  - I. – The collection and processing of personal data that reveals, directly or indirectly, the racial and ethnic origins, the political, philosophical, religious opinions or trade union affiliation of persons, or which concern their health or sexual life, is prohibited.
  - II. – In so far as the purpose of the processing may so require in respect of certain categories of data, the prohibition provided for in Section I shall not apply to:
    - 6° processing that is necessary for the purposes of preventive medicine, medical diagnosis, provision of healthcare or treatment, or for the management of healthcare services and carried out by a member of a medical profession, or by any other person who, due to his functions, is bound by a duty of confidentiality as stipulated in Article 226-13 of the Criminal Code;
    - 8° processing necessary for medical research according to the conditions provided for in Chapter IX (processing of personal data for the purpose of medical research).

CNIL - actors and principles concerning biomedical data

Actors

- Concerned person (e.g., patient, analyzed subject)
- Professional (health care professional or researcher)
- Data controller (e.g., responsible of the health service or research laboratory)
- Recipients (e.g., outsourcing service)

5 principles

1. Purpose specification
2. Limitation of collection and computation
3. Right to be forgotten
4. Security and privacy
5. Right of concerned persons

CNIL - medical research

- Lift professional secrecy on biomedical data if concerned persons are informed
  - Purposes of the study, what data is used, how she can access and rectify her data, etc.
- Data for medical research, a particular procedure: Chapter IX Act No 78-17
  - E.g., epidemiological studies, cancer records, pharmaco-epidemiological studies
  - Data that directly identify persons should be well justified
- Used data follow a procedure to obtain the CNIL authorization for medical research
- Methodology for biomedical research on data that do not identify directly persons: MR001

CNIL - outsourcing storage of biomedical data

- Biomedical data can be outsourced to accredited enterprises
- Accreditation
  - for 3 years
  - for a particular service (there is no general accreditation)
  - given by the Minister for Health
  - CNIL analyses the candidature gives an opinion
- Duties of outsourcing enterprises
  - Security of data, traceability, persistency of data, availability, accountability, etc.

Cloud computing at a glance

Cloud computing

- « Is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction »

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

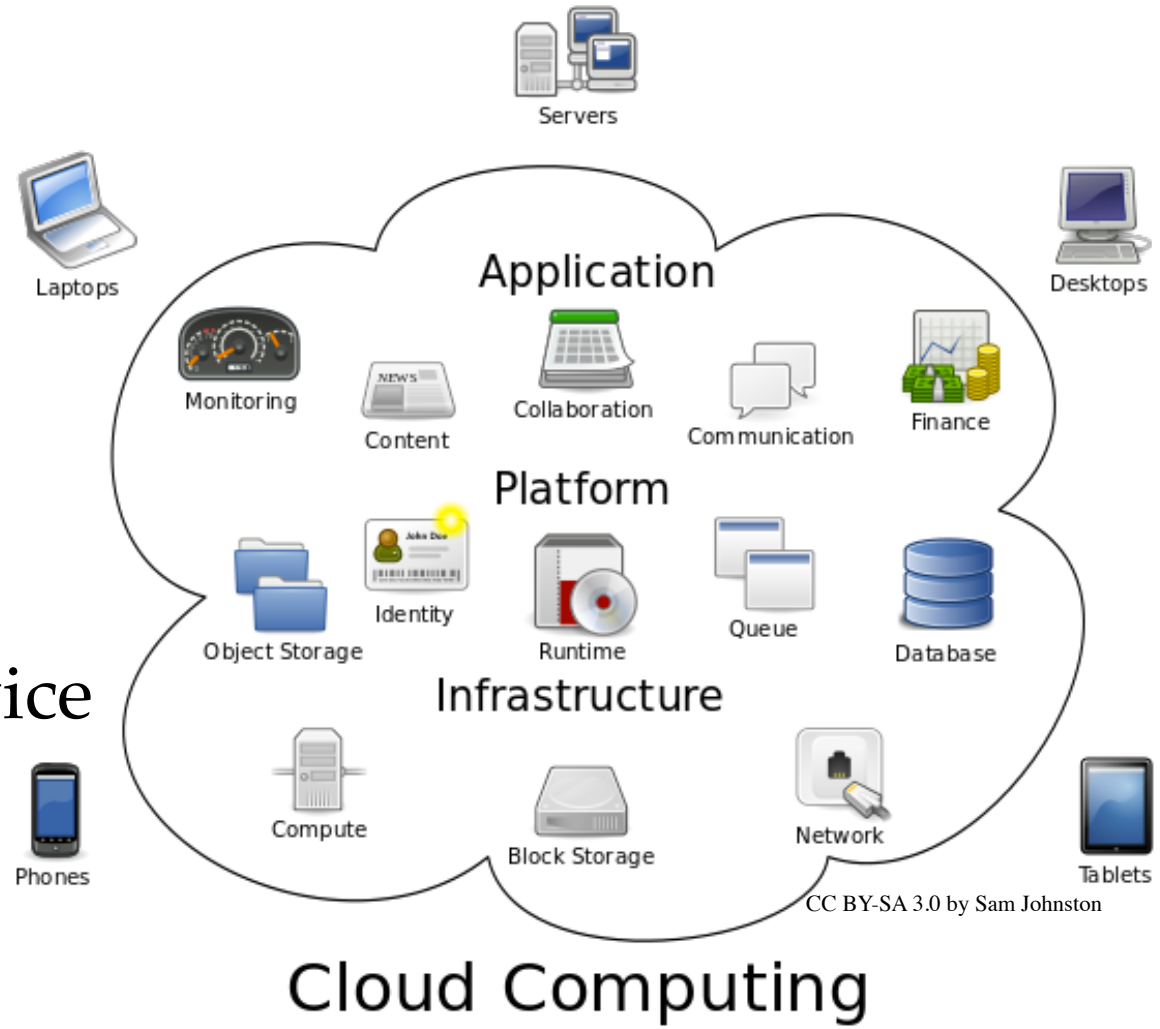
Five essential characteristics

- On-demand self-service
- Broad network access
- Resource pooling
- Rapid elasticity
- Measured service

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

Three service models

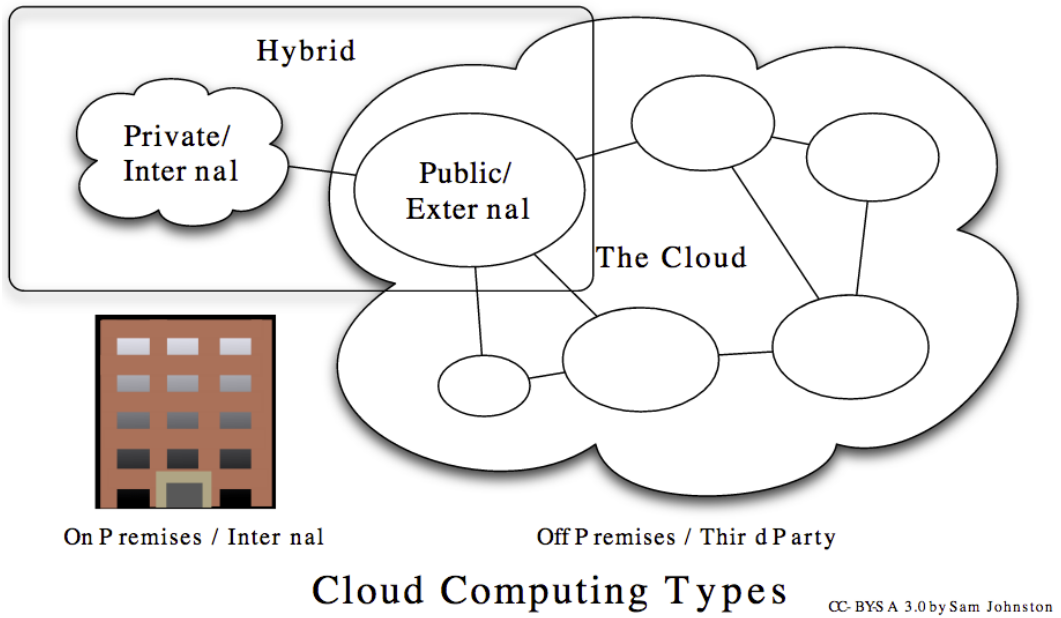
- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)



Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

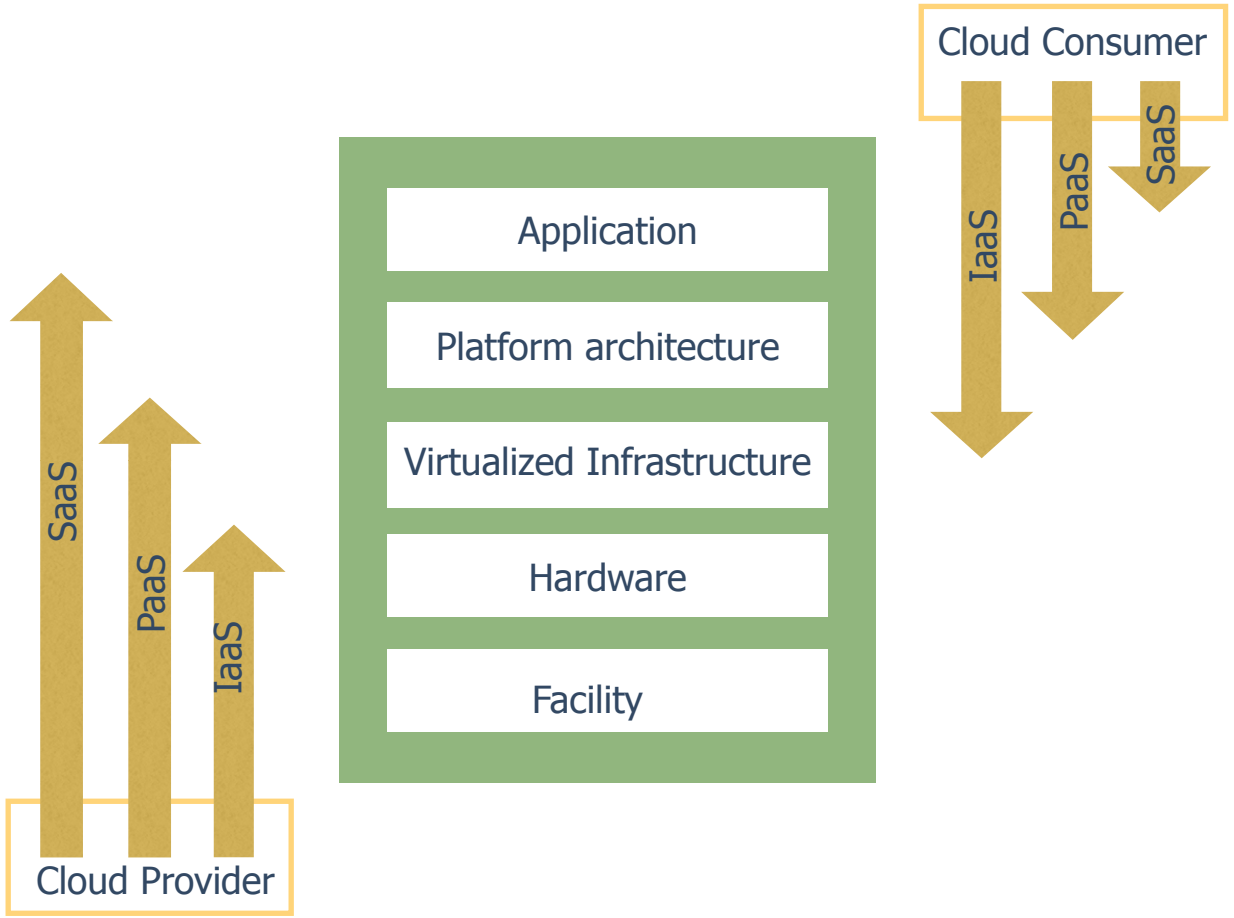
Four deployment models

- Private cloud
- Community cloud
- Public cloud
- Hybrid cloud



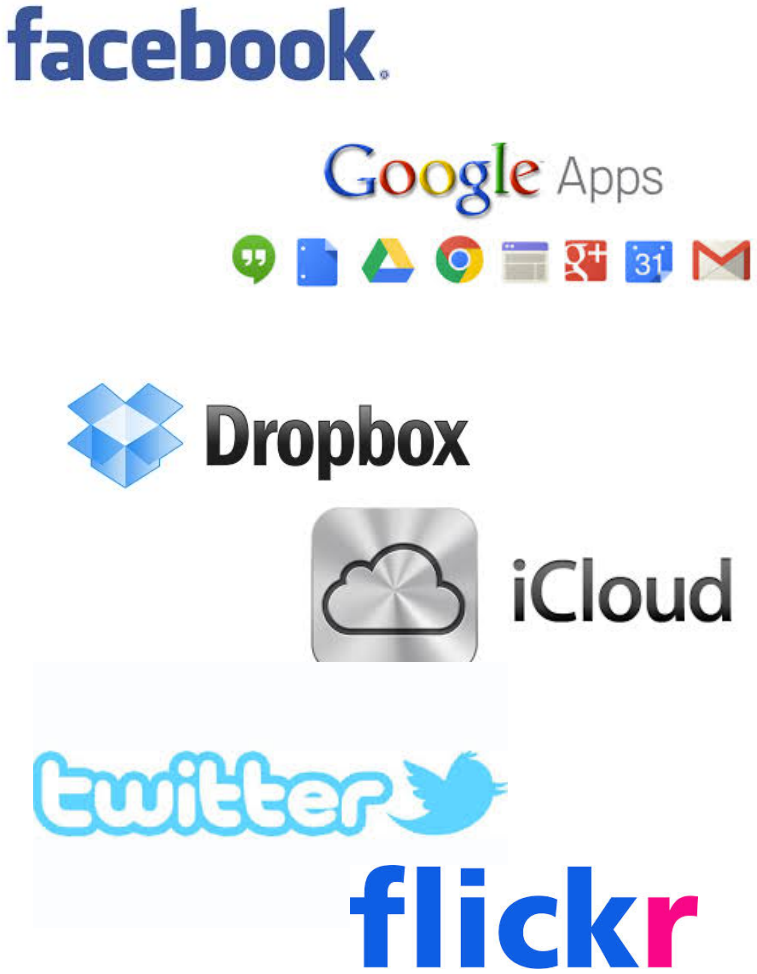
Mell, P., & Grance, T. (2011). The NIST definition of cloud computing.

Differences in scope and control among cloud service models



Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. NIST special publication, 800, 144.

Most used public cloud services



Top providers of cloud services

1. Salesforce.com, San Francisco, CA, USA
2. Amazon, Seattle, WA, USA
3. Microsoft, Redmond, WA, USA
4. Oracle, Redwood City, CA, USA
5. Google, Mountain View, CA, USA
6. SAP, Walldorf, Germany
7. SoftLayer (IBM), Dallas, TX, USA, etc.

Cloud computing

opportunities and challenges

Management

Opportunities

- Lower cost of new IT infrastructure
- Computing resources available on demand
- Payment of use on a short-term basis as needed

Challenges

- Lack of trust by health care professionals
- Cultural resistance
- Loss of governance

Kuo, A. M. H. (2011). Opportunities and challenges of cloud computing to improve health care services. Journal of medical Internet research, 13(3).

Technology

Opportunities

- Reduction of IT maintenance burdens
- Scalability and flexibility of infrastructure
- Advantage for green computing

Challenges

- Resource exhaustion issues
- Unpredictable performance
- Data lock-in
- Data transfer bottlenecks
- Bugs in large-scale distributed cloud systems

Kuo, A. M. H. (2011). Opportunities and challenges of cloud computing to improve health care services. Journal of medical Internet research, 13(3).

Security

Opportunities

- More resources available for data protection
- Replication of data in multiple locations increasing data security
- Dynamically scaled defensive resources strengthening resilience

Challenges

- Separation failure
- Public management interface issues
- Poor encryption key management
- Privilege abuse

Kuo, A. M. H. (2011). Opportunities and challenges of cloud computing to improve health care services. Journal of medical Internet research, 13(3).

Legal

Opportunities

- Provider's commitments to protect customer's data and privacy
- Development of guidelines and technologies to enable the construction of trusted platforms by not-for-profit organizations
- Fostering of regulations by government for data and privacy protection

Challenges

- Data jurisdiction issues
- Privacy issues

Kuo, A. M. H. (2011). Opportunities and challenges of cloud computing to improve health care services. Journal of medical Internet research, 13(3).

The security and privacy upside

- Staff Specialization
- Platform Strength
- Resource Availability
- Backup and Recovery
- Mobile Endpoints
- Data Concentration

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. NIST special publication, 800, 144.

The security and privacy downside

- System Complexity
- Shared Multi-tenant Environment
- Internet-facing Services
- Loss of Control

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. NIST special publication, 800, 144.

Security and Privacy Issues and Recommendations

Areas	Recommendations
Governance	Extend organizational practices pertaining to the policies, procedures, and standards used for application development and service provisioning in the cloud, as well as the design, implementation, testing, use, and monitoring of deployed or engaged services. Put in place audit mechanisms and tools to ensure organizational practices are followed throughout the system lifecycle.
Compliance	Understand the various types of laws and regulations that impose security and privacy obligations on the organization and potentially impact cloud computing initiatives, particularly those involving data location, privacy and security controls, records management, and electronic discovery requirements. Review and assess the cloud provider's offerings with respect to the organizational requirements to be met and ensure that the contract terms adequately meet the requirements. Ensure that the cloud provider's electronic discovery capabilities and processes do not compromise the privacy or security of data and applications.

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. NIST special publication, 800, 144.

Security and Privacy Issues and Recommendations

Areas	Recommendations
Trust	Ensure that service arrangements have sufficient means to allow visibility into the security and privacy controls and processes employed by the cloud provider, and their performance over time. Establish clear, exclusive ownership rights over data. Institute a risk management program that is flexible enough to adapt to the constantly evolving and shifting risk landscape for the lifecycle of the system. Continuously monitor the security state of the information system to support on-going risk management decisions.
Architecture	Understand the underlying technologies that the cloud provider uses to provision services, including the implications that the technical controls involved have on the security and privacy of the system, over the full system lifecycle and across all system components.

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. NIST special publication, 800, 144.

Security and Privacy Issues and Recommendations

Areas	Recommendations
Identity and Access Management	Ensure that adequate safeguards are in place to secure authentication, authorization, and other identity and access management functions, and are suitable for the organization.
Software Isolation	Understand virtualization and other logical isolation techniques that the cloud provider employs in its multi-tenant software architecture, and assess the risks involved for the organization.
Data Protection	Evaluate the suitability of the cloud provider's data management solutions for the organizational data concerned and the ability to control access to data, to secure data while at rest, in transit, and in use, and to sanitize data. Take into consideration the risk of collating organizational data with that of other organizations whose threat profiles are high or whose data collectively represent significant concentrated value. Fully understand and weigh the risks involved in cryptographic key management with the facilities available in the cloud environment and the processes established by the cloud provider.

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. NIST special publication, 800, 144.

Security and Privacy Issues and Recommendations

Areas	Recommendations
Availability	Understand the contract provisions and procedures for availability, data backup and recovery, and disaster recovery, and ensure that they meet the organization's continuity and contingency planning requirements. Ensure that during an intermediate or prolonged disruption or a serious disaster, critical operations can be immediately resumed, and that all operations can be eventually reinstituted in a timely and organized manner.
Incident Response	Understand the contract provisions and procedures for incident response and ensure that they meet the requirements of the organization. Ensure that the cloud provider has a transparent response process in place and sufficient mechanisms to share information during and after an incident. Ensure that the organization can respond to incidents in a coordinated fashion with the cloud provider in accordance with their respective roles and responsibilities for the computing environment.

Jansen, W., & Grance, T. (2011). Guidelines on security and privacy in public cloud computing. NIST special publication, 800, 144.

Conclusion

- Cloud computing can facilitate health services and biomedical research
- BUT it is important to carefully negotiate security and privacy garanties

- Projects for a French Cloud « *Investissements d'avenir* »

Cloudwatt

NUMERGY
PRODUCTEUR D'ÉNERGIE NUMÉRIQUE

nu@ge

- Currently on the French market

ikoula
Hosting Services

hubiC

aruba CLOUD