Privacy and security in the cloud

Challenges and solutions for our future information society

—

"Building trust – the technical challenges"
Session of the WSIS FORUM 25-29 May 2015

Thomas Länger

Swiss Cybersecurity Advisory & Research Group
Université de Lausanne

28 May 2015 – 15:00-16:30

UNIL | Université de Lausanne

Talk outline

- **Cloud computing** is currently a "big thing" in ICT
- it is a **huge interdisciplinary arena** with many stakeholders.
- Following the ITU workshop aims, I will address:
  - cloud computing as a phenomenon and its environment
  - its relation to the "information infrastructure"
  - identification of stakeholders
  - its future between technical evolution and regulation
  - current situation in clouds standardisation
- These issues are currently addressed in H2020 project PrismaCloud, which has just started in Feb. 2015

UNIL | Université de Lausanne

Definition of cloud computing

There are no unique features or great novelties in 'cloud computing'. It is a collective term for, in the broadest sense, **modern internet information systems**.

Widely accepted definition by the NIST (Special Publication SP800-145, 7 pages; **emph.** by me):

> *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**. *This cloud model is composed of five essential characteristics, three service models, and four deployment models.*

UNIL | Université de Lausanne

This cloud model is composed of...

five essential characteristics:

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

three service models:

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

four deployment models:

- Private cloud, Community cloud
- Public cloud, Hybrid cloud (all SP800-145)

UNIL | Université de Lausanne

Cloud computing and information infrastructure

One could argue whether the term 'cloud computing'

- refers more to a new paradigm, or a 'clever' marketing strategy?

Cloud computing is possible and common, because of

- high level of computer availability facilitates ubiquity
- available wireless communication infrastructures
- with high bandwidth, especially also upstream

Applications on top of advanced information infrastructures are often referred to as being "cloud computing"

Cloud computing

- is currently a huge market (magnitude 3-digit billion USD),
- with influential market participants and stakeholders

UNIL | Université de Lausanne

Cloud market: A few figures

Management consulter Accenture sees 46% of the IT spending for 'cloud-related platforms and applications' by 2016

> *A Cloud Computing Forecast Summary for 2013 - 2017 from IDC, Gartner and KPMG; online: www.prweb.com/releases/2013/11/prweb11341594.htm, citing a study by Accenture (2013)*

The cloud computing market is by 2015 estimated to be in the region of USD 150 billion, and will probably grow by the year 2018 to around USD 200 billion

> *Transparency Market Research: Cloud Computing Services Market - Global Industry Size, Share, Trends, Analysis And Forecasts 2012 - 2018, online: www.transparencymarketresearch.com/cloud-computing-services-market.html*

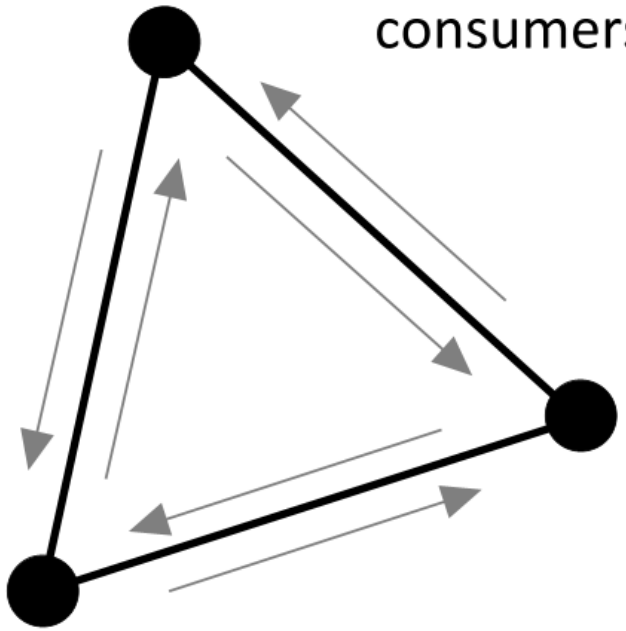
"Amazon Web Services is a $5 billion business and still growing fast"

> *Amazon quaterly earnings report Q1/2015 phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-newsArticle&ID=20395989*

UNIL | Université de Lausanne

Stakeholder groups with different interests

1: Cloud users. individuals, citizens, corporate users, administrations (both as service providers and consumers)



2: Corporations. marketing cloud services and content

3: Regulation (e.g. information privacy) and **standardisation**, policy

UNIL | Université de Lausanne

1: Cloud users

Individuals - Administrations - Companies

- individuals use cloud storage with smart phones
- and the huge computing clouds of social and comm. networks
- administrations use cloud-based e-government services
- businesses outsource their processing and services

We/They want to

- profit from convenience of ubiquitous cloud access
- get rid of backups and hardware management,
- consume a self-service which is: rapid, on-demand, elastic, pay-per-use
- they want privacy, integrity they had before the cloud

UNIL | Université de Lausanne

2. Corporations

Cloud service providers want to **offer and sell** cloud services:

- Google-Android-YouTube: (bought 181 companies 2001-2015)
- Facebook (bought 53 companies 2005-2015)
- Microsoft-Azure-Skype,
- Amazon AWS etc. etc.

Some of them also want to **'get a grip' on the data** or at least on the meta-data. Most public clouds reserve themselves access to

- who communicates with whom,
- and when, and where from (all these are metadata);
- establish detailed profiles of millions of individuals and dragnet or mine them for valuable information,
- identify potential 'targets' for marketing

UNIL | Université de Lausanne

3: Regulation

For **sensitive data**, like data in **critical infrastructures**, or private **personal data (e.g. health data)**, European legislation does not only reserve **ultimate control of the data to its owner** (which is in the case of the health case the patient), but also requires **data confidentiality for extended periods of time** (like 80 years into the future).

On the other hands, companies **move data between jurisdictions** and such prevent the enforcement of legal rights. Big corporations use loop-holes in legal systems and influence policy processes by extensive lobbying.

UNIL | Université de Lausanne

More pending risks in cloud computing

As the **cloud metaphor** already indicates, **you put your data into a cloud** – you can't 'see' it any longer. But that's just what you wanted to do: Give it to somebody else who should take care of it. This may be practical (see all the advantages), but **leads to a series of information risks**:

- Policy and organisational risks
  - lack of control
  - lack of information on processing
  - loss of governance (data moved to another legislation)
  - vendor lock in
- Technical risks
  - isolation failure
  - diverse data protection risks
  - data loss
  - abuse, malicious outsider and insider etc.

UNIL | Université de Lausanne

Diagnosis

Confidentiality of user data is one of the **most crucial problems** in current cloud offerings. Confidentiality is often only guaranteed on a **contractual basis** between cloud customer and the service provider.

- The **customer** of the cloud has **insufficient means** in hands, to **cryptographically protect** the data,
- whereas the **cloud provider cannot plausibly deny** that the entrusted data was not modified or illegally copied.

This is why individuals, companies and public administration **hesitate to entrust** valuable data to cloud services

UNIL | Université de Lausanne

Horizon 2020 project: PrismaCloud approach

A 3.5 year project with the goal to **enable end-to-end security for cloud users**, and to provide tools to **protect their privacy** with the best technical means – **by cryptography**

- Advance cryptography to support dynamicity and agility of cloud computing
  - Provide means to protect the results of computations
  - Protect privacy of users
  - Protect data at rest
  - Infrastructure attestation
- Make cryptography available, usable and economically relevant for clouds
- Evaluate its capabilities in real-life scenarios
- Put a focus on usability, policy, and standardisation

UNIL | Université de Lausanne

Standardisation in cloud computing

The **'standardisation landscape' of cloud computing** reflects the fast-growing, gold-rush style market, with a lagging behind technical capability and an uneven regulation:

- Probably more than 20 standards organisations and consortia are active in the field (see e.g. `http://cloud-standards.org`)
- Probably hundreds of publications are available, among them standards for **portability, interoperability, security, accessibility and performance**
- The European Commission's Cloud Computing Strategy identifies as Key Action 1 **"Cutting through the Jungle of Standards"** (European Commission: European cloud computing strategy "Unleashing the potential of cloud computing in Europe" (2012), `ec.europa.eu/digital-agenda/en/european-cloud-computing-strategy`)

UNIL | Université de Lausanne

H2020 Project PrismaCloud

- Call: H2020-ICT-2014-1
- Acronym: PRISMACLOUD
- Type of Action: RIA
- Number: 644962
- Partners: 16
- Duration: 42 months
- Start Date: 2015-02-01
- Estimated Project Cost: 8.5M€
- Requested EU Contrib.: 8M€
- Coordinator: Austrian Institute of Technology GmbH
- url: `www.prismacloud.eu`

UNIL | Université de Lausanne

PRISMACLOUD Partners

AIT Austrian Institute of Technology – Tomorrow Today

Karlstads Universitet

cea leti

etra I+D

Newcastle University

Atos

FCSR Fondazione Centro San Raffaele

IBM

Unil UNIL | Université de Lausanne

interoute from the ground to the cloud

Lombardia Informatica

MIKROPLAN

IAIK TU Graz

Universität Passau

Technische Universität Darmstadt

XITRUST Secure Technologies

About: Thomas Länger

Hello! I'm post-doc researcher at the **Swiss Cybersecurity Advisory & Research Group** of the Institute of Information Systems, Faculty of Business and Economics,
University of Lausanne.

Currently active in H2020 Project "PrismaCloud" 1 Feb 2015 + 42 month; 16 Partners, Project cost approx. 8.5M€ "Develop next-generation cryptographically secured services for the cloud." My tasks: cloud computing (cc) generic use cases; cc standardisation; impact analysis of cc. (v03)

UNIL | Université de Lausanne