



# Presentations summary

## □ Pros presented

- **Cope with peak load without having to invest in resources for short peak load period eg. French treasury during fiscal year finalisation**
- **resiliency and duplication are among the greatest benefits of using cloud data centers**
- **Need to differentiate between Trust and Security: some technologies are available for Security elements; however, the client is dependent on the cloud provider using the right technologies in a right way, which makes Trust very difficult to achieve.**

## □ Cons presented

- **It doesn't make problems go away, but can exacerbate them eg. adds new trust and security challenges**
  - **Failures and non- transparency of cloud management systems**
  - **Protecting personally identifiable data against misuse in the cloud**
  - **Isolation breach between multiple cloud customers**
  - **Insider attacks by cloud administrators**
  - **Data transport through jurisdictions without proper law/regulations**
  - **Once data is in there, how do you guarantee to get it out? What about the 'right to be forgotten' in the cloud?**

# Research challenges for trust in the cloud

- ❑ **Challenge 1. Identify specific constraints/limitations of being in the cloud.**
  - Virtualised machines with replication leading to data leakage
  - Traceability difficult as cloud is massive in design, with a lot of interactions, so we cannot know what is going on in a cloud and it is susceptible to things like interception and analysis
  - Privacy infrastructure complexity - exacerbation of problem of digital trails
  - **Managing the transparency of inter-process communications in the cloud**
    - Where is the data passing through?
    - What laws and regulations apply?
    - Who is responsible?
    - Can the user customise routing based on their preferences?
    - .....
- ❑ **Challenge 2. As a research community, how to address these constraints/limitations in order for cloud based services to be trustworthy?**
  - **Examples of different trust levels were presented:**
    - having explicit, provable trust in provider
    - having ability to see how provider is handling data
    - having the ability to actually control and monitor data and data flows.
  - **Measurement and metrics for around and inside clouds are needed to compute or estimate whether you can trust this cloud**
  - **Policy accountability and enforcement mechanisms for cloud are needed**
  - **The need for strict bilateral contracts between the client and the cloud providers as well as contractual relationships between cloud providers and indemnity providers (eg. Insurance)**
    - This will require a level of abstraction that can be understood and will convince and demonstrate to the clients and indemnity providers of the cloud environments operational integrity.
- ❑ Full report can be found at <http://www.future-internet.eu/publications/view/article/fia-ghent-report.html> pp. 62-68.
- ❑ Other references:
  - Scalable and Adaptive Internet Solutions (SAIL) <http://www.sail-project.eu/>
  - TClouds project: <http://www.tclouds-project.eu/>
  - The DG INFSO Unit F5 study on [The Cloud: Understanding the Security, Privacy and Trust Challenges](http://cordis.europa.eu/fp7/ict/security/) available from <http://cordis.europa.eu/fp7/ict/security/>