Inria Saclay-IDF
November 7th, 2016
Colloque Inria CAPPRIS

Personal & Trusted Cloud

Nicolas Anciaux, SMIS team, Inria Saclay-IDF/UVSQ

Towards a personal and trusted cloud

Current model wrt. management personal data

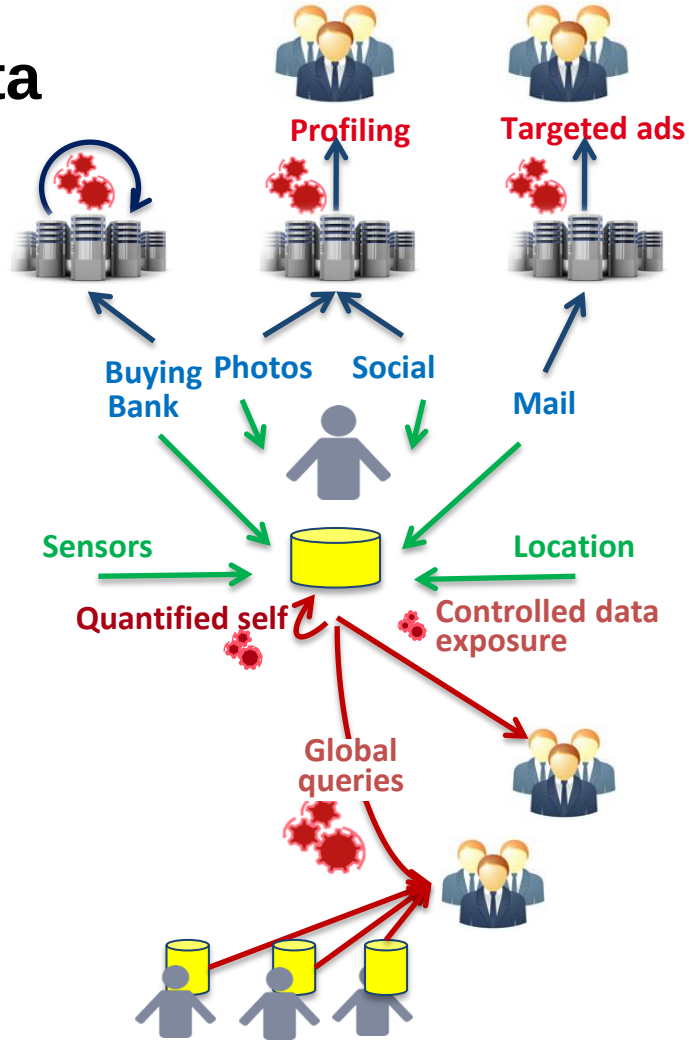
- Delegation ➔ privacy issue
- Centralization ➔ security issue
- Fragmentation ➔ completeness issue

New trend: return data to individuals

- smart disclosure / self-data, personal cloud
- ➔ Completeness de facto
- ➔ Controlled data exposure
- ➔ Collaborative/anonymous global queries

How to give back data to users ?

- A difficult problem…

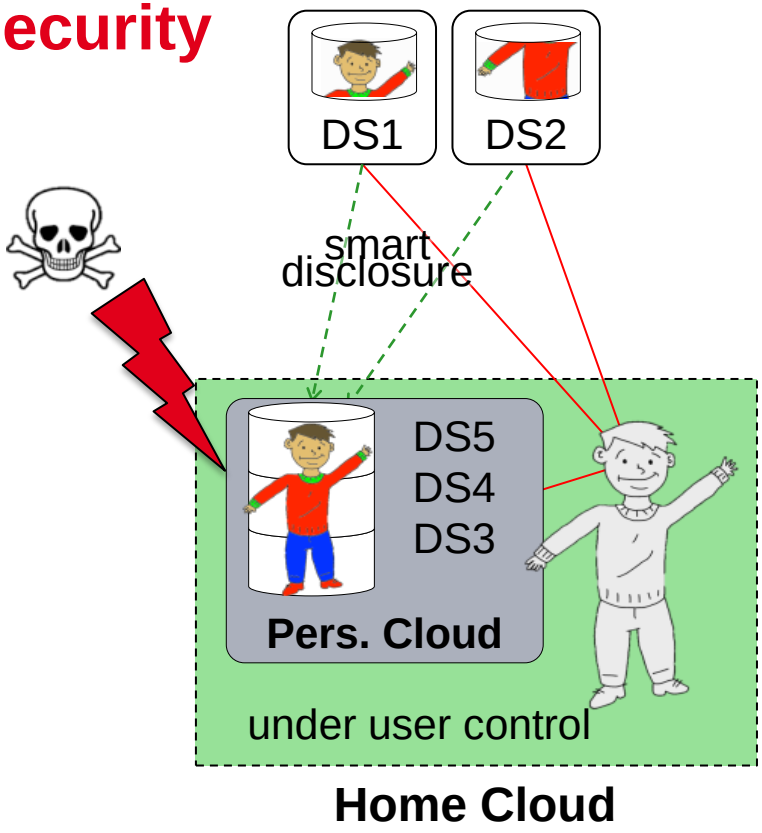


How to give back data to users ?

On personal computers ?

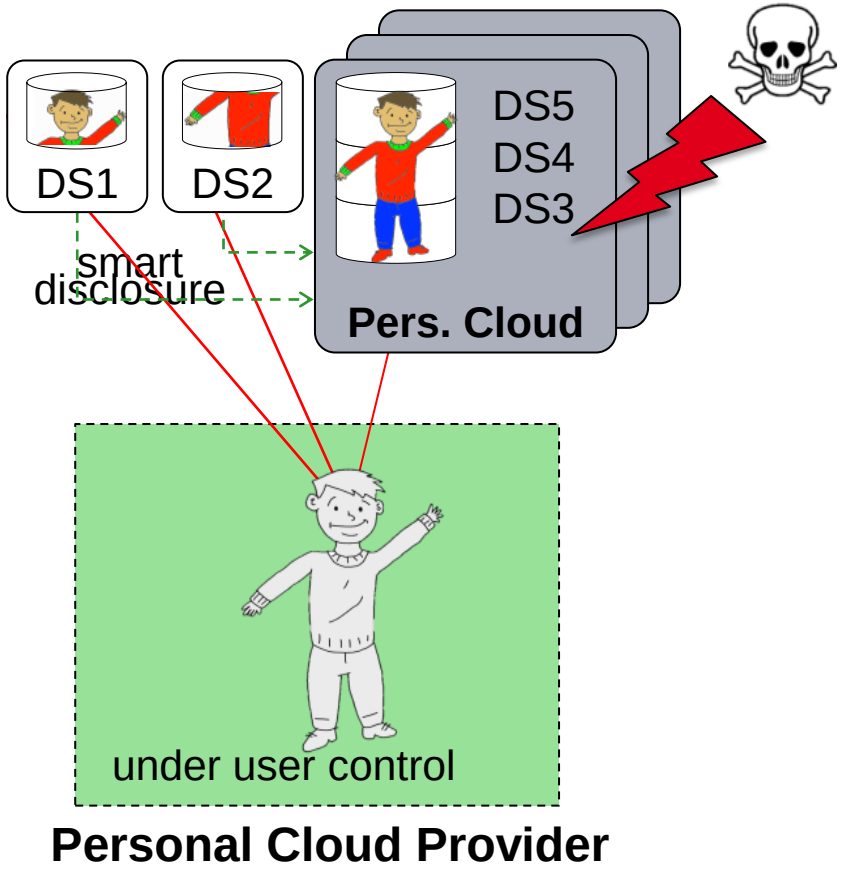
Self-administration

& security



On a cloud service ?

May worsen the privacy problem…



Our goal: turn the personal cloud promise into reality

Personal cloud principles

Sovereignty

Enlightened decision

No delegation

Risk isolation

Avoid “large scale” attacks

Enforcement

Strong guarantee

against active/passive attacks

Extended data processing

Cross-data computations

On single/multiple individuals

Our approach

Secure personal cloud architecture (risk Isolation & enforcement)

Secure hardware (tamper resistant), isolated enclaves (Trustzone/SGX), formal methods

Sovereign administration models (sovereignty & enforcement)

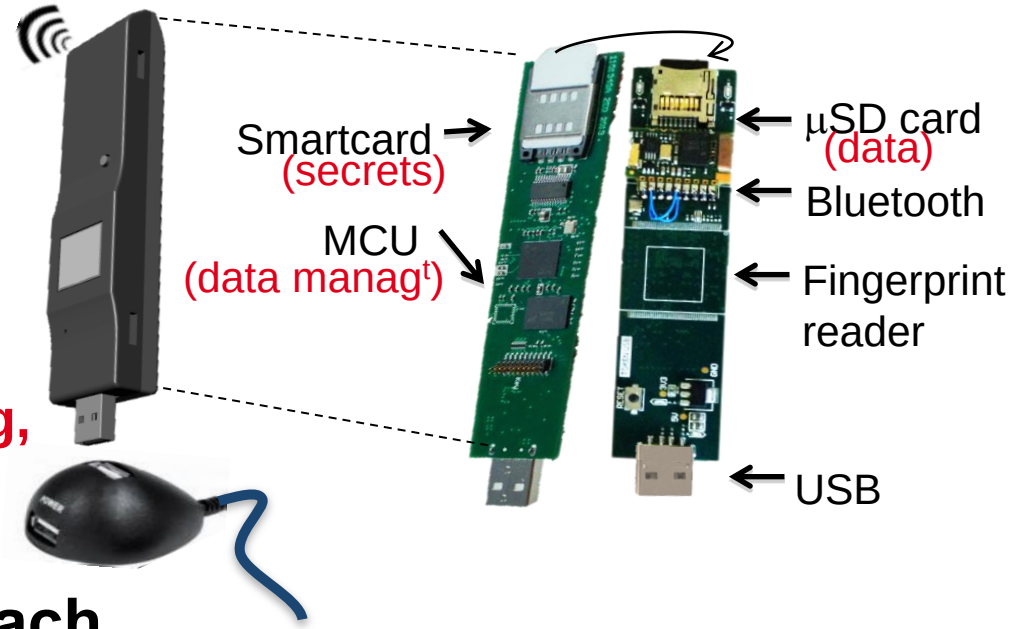
Ego-centered approach, secure hardware

Secure distributed computations (enforcement & extended data processing)

Consider risk, personalization, secure DB indexing

Multi disciplinary studies including laws and economics (adoption, impact)

Concrete platform: PlugDB



A Personal (home) Cloud…

interfaced with the users' devices

Data storage, indexing, query processing,

sharing policies, secure recovery

…with a 'security for privacy' approach

Software: isolated from applications, open source and small (can be proven)

Hardware: tamper resistant, open hardware

Applications

Secure personal cloud (with CozyCloud), Medical-social folder (with DC78)

Teaching and Fablab Platform (see Versailles Sciences Lab.)

Privacy-by-design courses & projects (ENSIIE, INSA & Univ. Versailles)

In vivo experiments with jurists and economists

Privacy preserving platform for behavioral economy

Demo1: Secure Personal Cloud (CozyCloud+PlugDB)

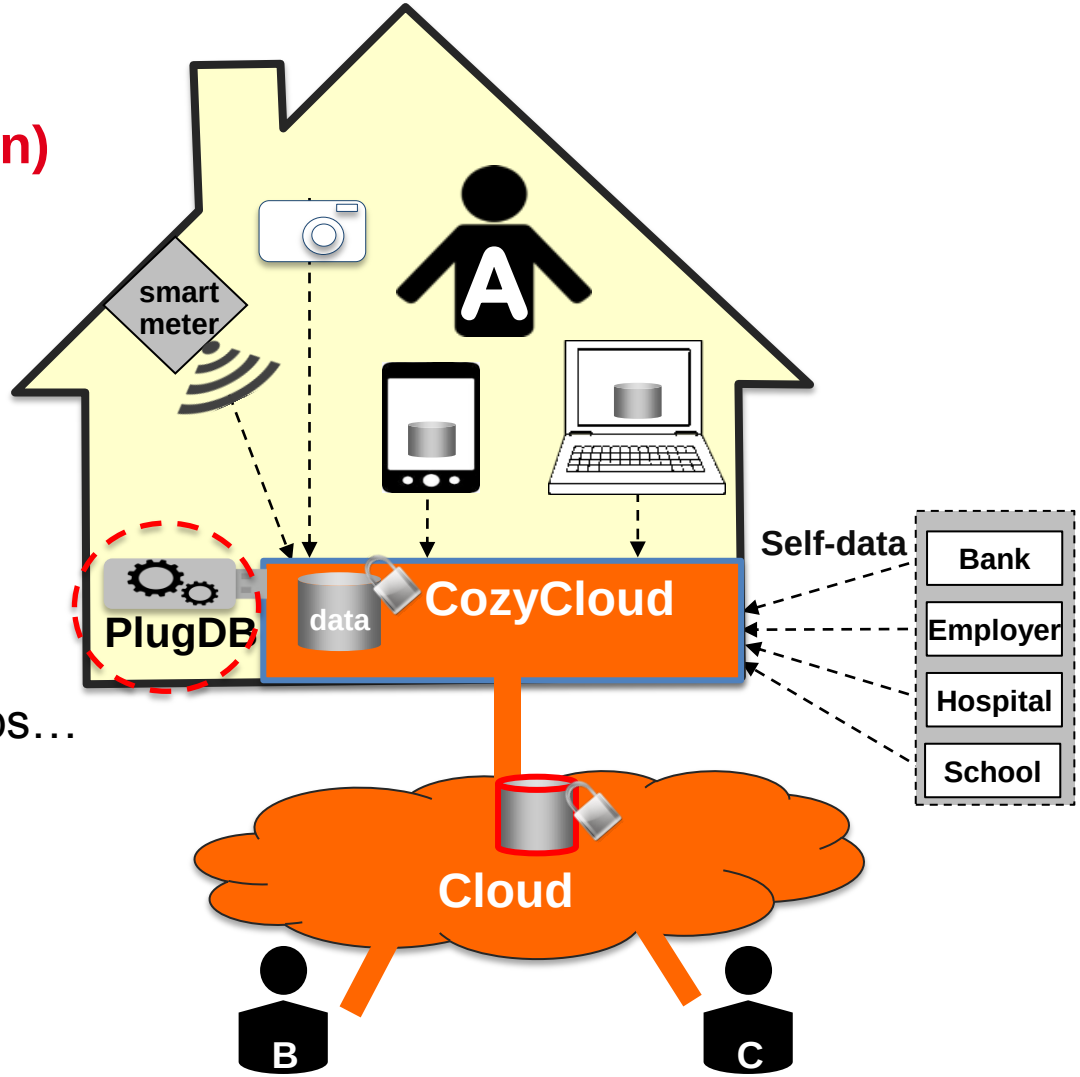
Collaboration with CozyCloud

- Secure sharing models (Paul Tran Van)
- Secure social queries (Julien Loudet)

SECSI (PIA) & PersoCloud (ANR)

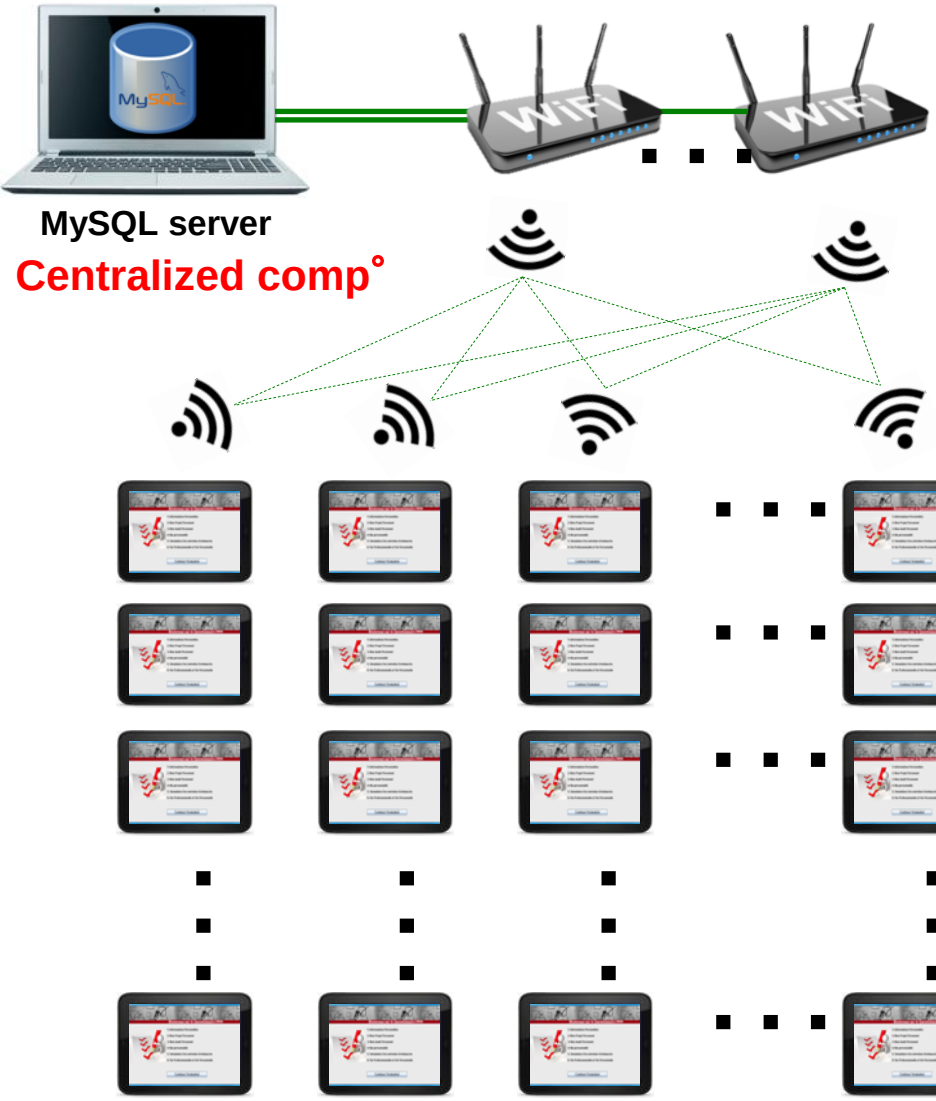
Demo : secure sharing model

- Administration by individuals
  - Not DBAs, decentralized & unstructured
  - Personal cloud knowledge => ACLs, groups…
- Enforced-by-default
  - Secure implementation
  - mixing CozyCloud & PlugDB



Demo2: Secure and Mobile Lab. (with economists)

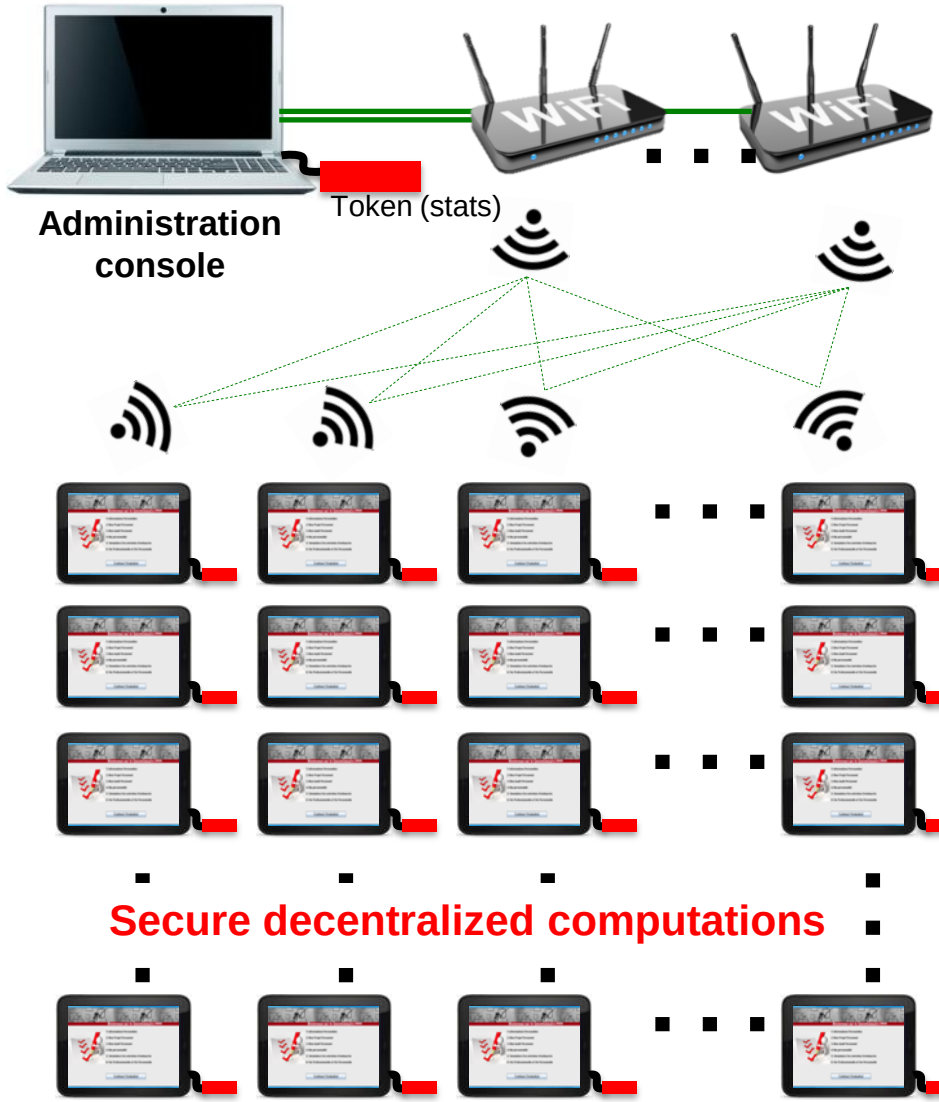
Centralized (classical setting)



MySQL server

Centralized comp°

Decentralized with secure tokens



Questions ?

References & links around PlugDB

PlugDB web site:
https://project.inria.fr/plugdb/

Some research papers:

MiloDB: a Personal, Secure and Portable Database Machine. DAPD 2014.
A Scalable Search Engine for Mass Storage Smart Objects. VLDB 2015.
Private and Scalable Execution of SQL Aggregates. TODS 2016.

Some demo. papers:

A Secure Search Engine for the Personal Cloud. SIGMOD 2015.
SQL/AA: Executing SQL on an Asymmetric Architecture. VLDB 2014.