Privacy-preserving cloud based applications

Myrto Arapinis, Sergiu Bursuc, Mark Ryan
School of Computer Science, University of Birmingham

September 2, 2010

Tensions in cloud computing

Verifiability vs Privacy

Tensions in cloud computing

Verifiability
Functionality
Business logic
Security

vs Privacy

Tensions in cloud computing

Verifiability
Functionality
Business logic
Security

vs Privacy

Privacy in multi-user collaborative systems

Applications:

- Human resources
- Financial accounting
- Customer relationship management
- Conference management

Clouds: Google, Facebook, Amazon, Dropbox

Goal: design and verify protocols that

A. Respect the desired privacy policies

B. Achieve the desired functional requirements

Difficulty: A in tension with B

Refining the use of encryption

1. Meagre computation: encrypting the sensitive data
2. Layered computation
   - on inner layer: homomorphic encryption
   - on outer layer: searchable encryption
3. Spread computation: unlinking the sensitive data

Difficulty: sensitive data $\cap$ functional data $\neq \emptyset$

Refining the use of encryption

1. Meagre computation: encrypting the sensitive data
2. Layered computation
   - on inner layer: homomorphic encryption
   - on outer layer: searchable encryption
3. Spread computation: unlinking the sensitive data

Difficulty: sensitive data $\cap$ functional data $\neq \emptyset$

Case study: conference management system

Functional requirements

- A - write papers p
- R - write a review r and give a score s to p
- T - produces a ranking $\mathcal{O}$ according to s and r
- C - is the cloud that
  - Collects and stores all the data
  - Manages the information flow
  - Ranks papers according to scores
  - Notifies A of the outcome

Case study: conference management system

Functional requirements

- A - write papers p
- R - write a review r and give a score s to p
- T - produces a ranking $\mathcal{O}$ according to s and r
- C - is the cloud that
  - Collects and stores all the data
  - Manages the information flow
  - Ranks papers according to scores
  - Notifies A of the outcome

Privacy requirements

- C does not know p, rev
- C does not know the link $R \longleftrightarrow s$
- C does not know the link $A \longleftrightarrow s$
- C does not know the link $A \longleftrightarrow R$

Protocol for the case study

Future work

- Assess the amount of client-side computation
- Functional task + Privacy policy $\Longrightarrow$ Protocol
- Collateral tasks
- Formal specification and verification
- Verifiability of functional tasks