Exécution de requêtes distribuées sous contraintes d'anonymat

Sur l'architecture des Trusted Cells

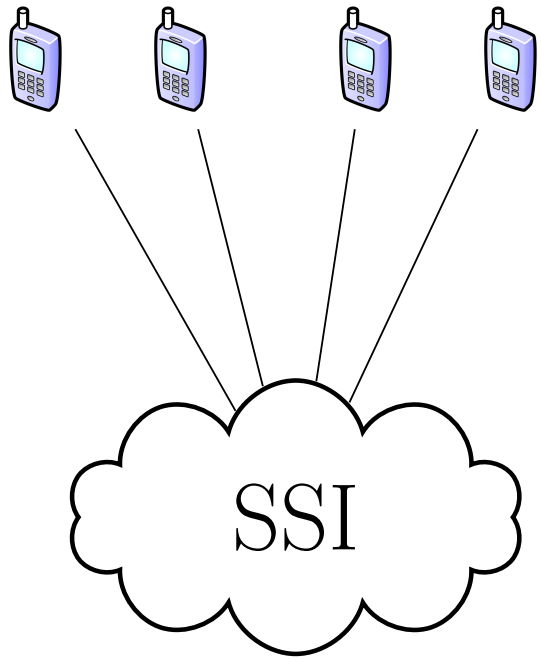
Axel Michel, Benjamin Nguyen

INSA-CVL, LIFO, France
Fname.Lname@insa-cvl.fr

4 mai 2016

Introduction

- Problématiques
  - Études statistiques **indispensables**
    - médicale : connaissances des maladies
    - énergie : efficacité des *smart-grids*
  - données **anonymisées** $\Rightarrow$ **agrégées**
  - données des utilisateurs parfois acquises **contre leur grés**
- Objectifs
  - basé sur la vision des **Trusted Cells** [All+10]
  - plus de **contrôle** aux utilisateurs sur leurs données
  - **garanties d'anonymat** et processus de **généralisation**



Contexte

Non-sensible		Sensible
Code postale	Âge	Condition
112**	> 25	Cancer
112**	> 25	Cancer
112**	> 25	Maladie cardiaque
1125*	*	Maladie cardiaque
1125*	*	Infection virale
1125*	*	Cancer

TABLE : Données médicales fictives 3−anonyme et 2−diverse

- Anonymisation
  - $k-$anonymat [Swe02]
  - $\ell-$diversité [Mac+06]
- SQL/AA [TNP14]
  - Protocole en 3 phases
  - Calculs de requêtes **sans fuite d'informations**

Questions ?

References

[All+10] Tristan Allard et al. "Secure Personal Data Servers : a Vision Paper". In : *PVLDB* (2010).

[Mac+06] Ashwin Machanavajjhala et al. "l-Diversity : Privacy Beyond k-Anonymity". In : *Proceedings of the 22nd International Conference on Data Engineering* (2006).

[Swe02] Latanya Sweeney. "k-Anonymity : A Model for Protecting Privacy". In : *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* (2002).

[TNP14] Quoc-Cuong To, Benjamin Nguyen et Philippe Pucheral. "SQL/AA : Executing SQL on an Asymmetric Architecture". In : *PVLDB* (2014).