Sémantique et optimisation dans le langage C2QL

Santiago Bautista

juin - juillet 2017

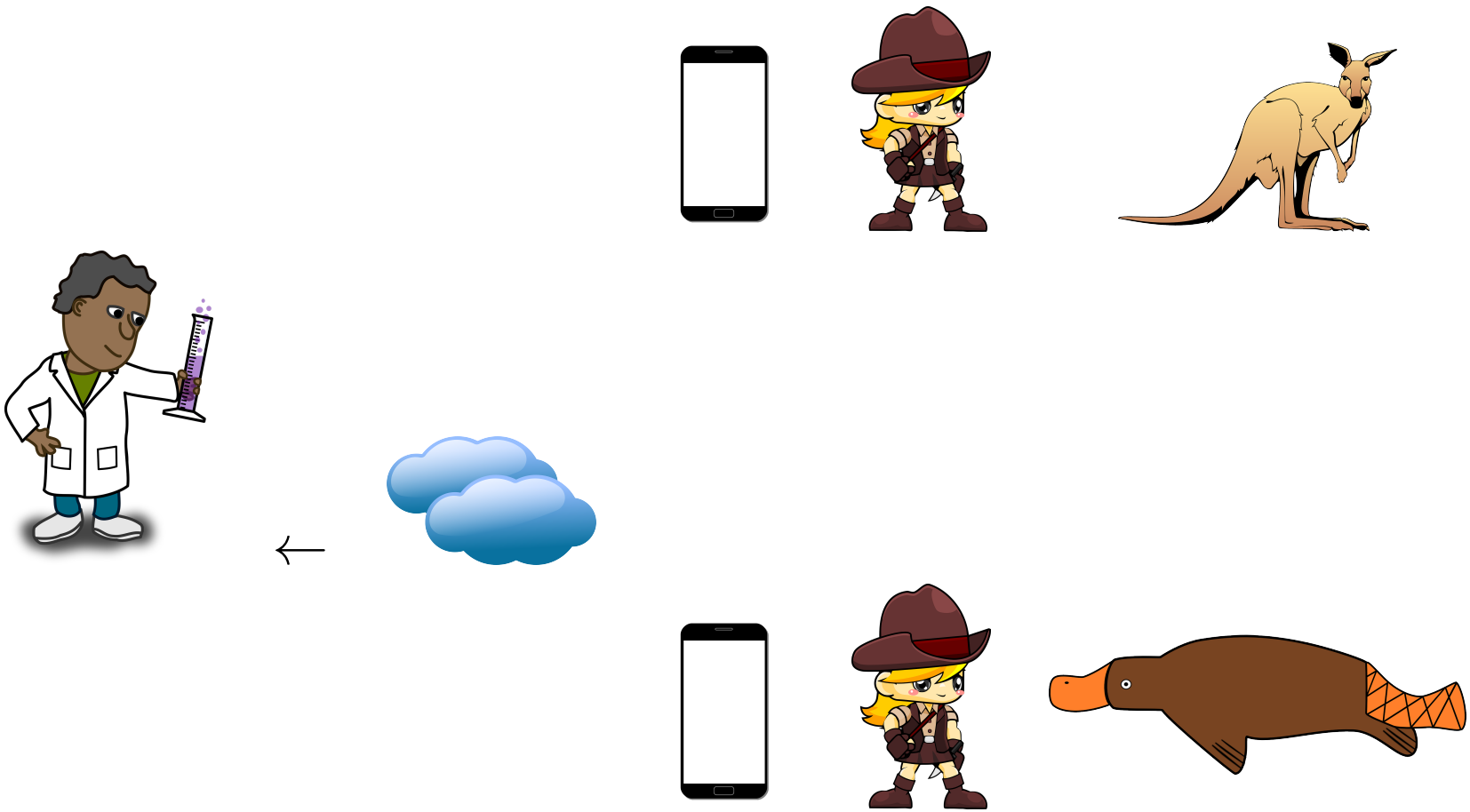
De plus en plus d'applications

$$\begin{cases} \text{Utilisent le nuage} \\ \text{Manipulent des données personnelles} \end{cases}$$

Problème

Comment protéger la confidentialité tout en privilégiant l'utilisation du nuage et les performances ?

Exemple fil rouge



Exemple fil rouge

Exemple de données collectées :

- Animal vu (kangourou, ornithorynque)
- Date
- Lieu
- Nom de l'aventurier
- ...

Confidentialité

Un problème de confidentialité est défini par

- Qu'est-ce qu'on veut protéger ?
- De qui veut-on le protéger ?

Contraintes de confidentialité

Dans l'exemple on veut protéger

- L'association (date, lieu)
- Les noms des aventuriers

Hypothèses sur l'attaquant

On ne fait confiance

- Ni aux nuages utilisés
- Ni au réseau utilisé

On fait confiance

- A la machine de l'utilisateur.

Chiffrement

Définition

Transformer l'information intelligible en inintelligible de façon réversible pour les destinataires.

Chiffrement

Définition

Transformer l'information intelligible en inintelligible de façon réversible pour les destinataires.

Exemple

$\rightarrow$

Ana	Melton	4/8	LD6h736B	Melton	4/8
Fred	Tamworth	5/8	3ghjKrE	Tamworth	5/8
Ana	Orange	6/8	LD6h736B	Orange	6/8

$\leftarrow$

Fragmentation verticale

Définition

Séparer (géographiquement, par exemple) deux informations pour rendre inintelligible leur association.

Fragmentation verticale

Définition

Séparer (géographiquement, par exemple) deux informations pour rendre inintelligible leur association.

Exemple

Ana	Melton	9 août
Fred	Tamworth	10 août
Ana	Orange	11 août

Melton	Ana 9 août
Tamworth	Fred 10 août
Orange	Ana 11 août

Calculs côté utilisateur

On fait confiance à la machine de l'utilisateur

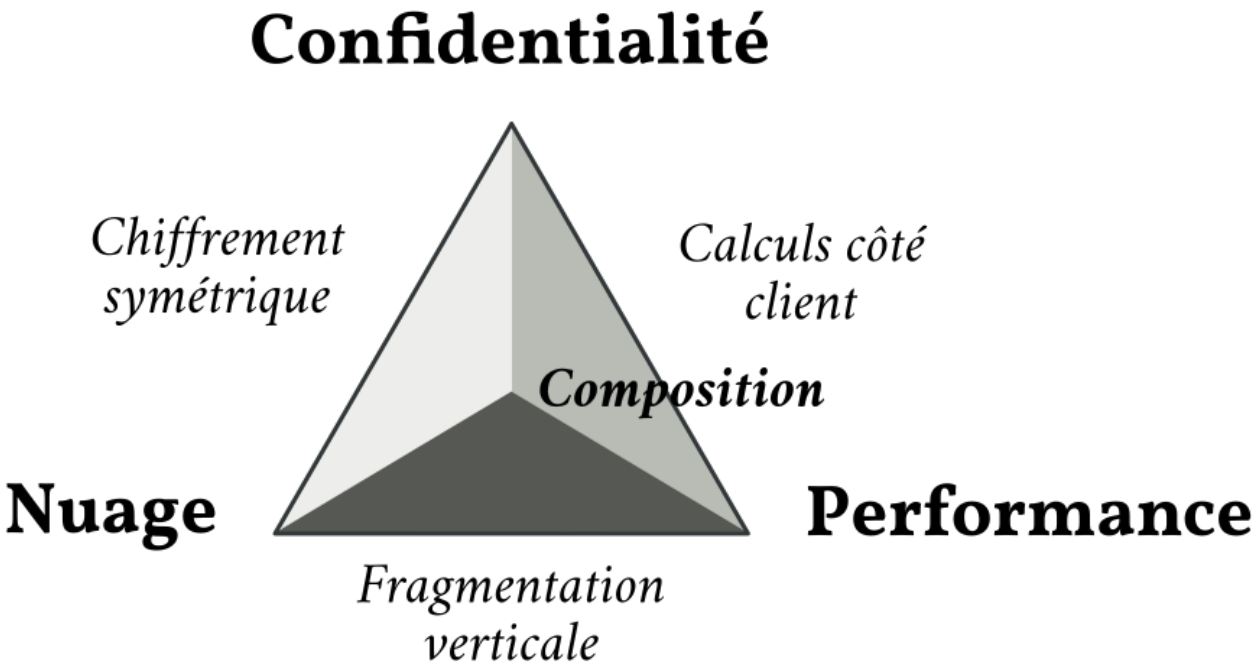
$\Downarrow$

Les informations traitées et stockées *localement*
sont supposées en sécurité

Enjeux d'une application utilisant le nuage

- Utilisation du nuage
  - Disponibilité
  - Passage à l'échelle automatisable
- Protection de la confidentialité
- Performances

Enjeux et protection de la confidentialité



Le langage C2QL

Relations

Ensemble des fonctions

Ensemble des fonctions étendu

Développer un programme C2QL optimal

Choix à faire

Structure des preuves

Erreurs corrigées

Critère de complétude

Exemple

Tableau des effets de chaque loi

Conclusion