

# Confidentialité et disponibilité des données entreposées dans les nuages

Kawthar Karkouda, Nouria Harbi,  
Jérôme Darmont Gérard Gavin

Laboratoire Eric  
Université Lumière Lyon 2  
*nouria.harbi@univ-lyon2.fr*

31 Janvier 2012

# Plan



- ▶ Contexte
- ▶ Problématique
- ▶ Sécurisation des données par le secret sharing
- ▶ Mise en pratique de la proposition
- ▶ Conclusion
- ▶ Perspectives

# Contexte



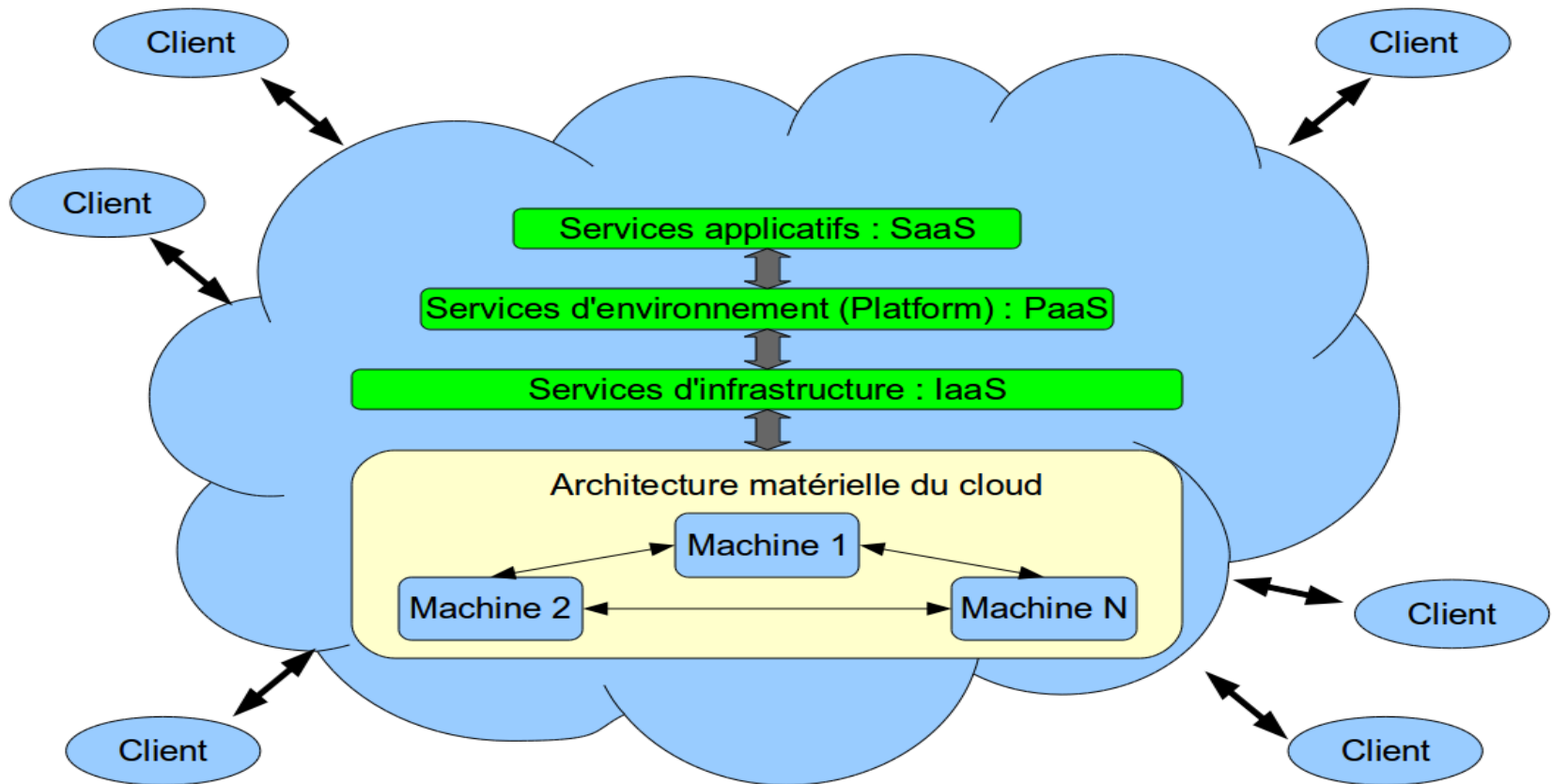
- ▶ Pourquoi passer à l'informatique dans les nuages ?



# Contexte



## ► L'informatique dans les nuages



# Problématique



Est il raisonnable de confier des données importantes et sensibles aux fournisseurs des nuages ?

Comment peut-on assurer que les fournisseurs des nuages ne disparaissent pas un jour ?

Nos données seront-elles effacées lorsqu'on veut changer le fournisseur ?

Ya t-il un risque de perte de données stockées dans les nuages ?

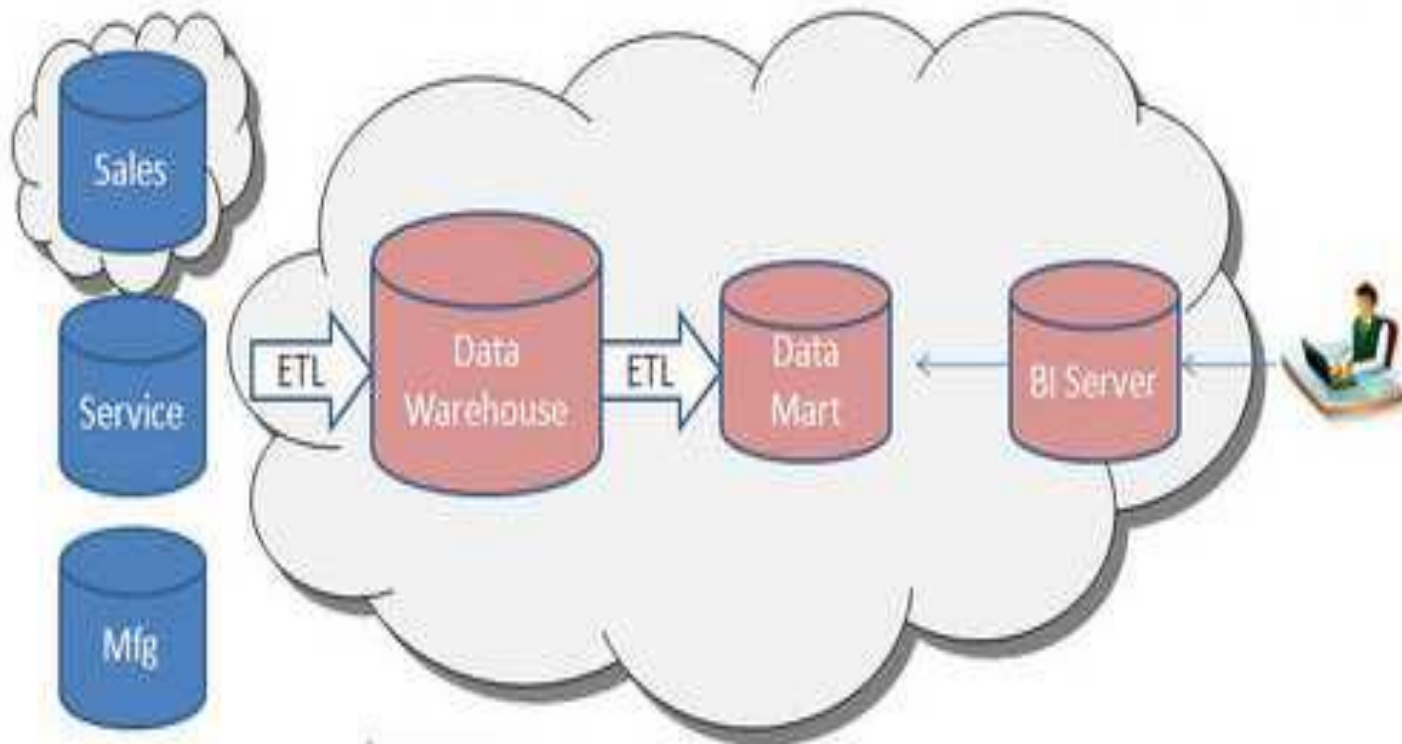
Le service offert par les fournisseurs est-il toujours disponible ?

Le transfert des données vers les nuages est-il sécurisé ?



# Contexte

- ▶ Entrepôt de données dans l'informatique dans les nuages



- ✓ Gossman et ses collaborateurs, 2008
- ✓ Doka et ses collaborateurs, 2010

# Problématique



**Sécurité des données**

**Sécurité Logique**

**Sécurité physique**

# Problématique



- ▶ **Sécurité des accès et du stockage des données :**
  - *Jensen et ses collaborateurs*, 2009 (sécurisation navigateur WEB) :  
Utilisation de la cryptographie XML pour adapter le navigateur TLS
  - *Danwei Chen et Yanjun He*, 2010 (accessibilité des données) :  
Algorithme de restauration des données (de partage de clés secrètes de Shamir) extension du théorème de K équations en algèbre

# Problématique



## ▶ Sécurité Logique (Machine virtuelle) :

- *Wei et ses collaborateurs, 2009* (détection d'intrusions) :  
Système de gestion d'images de la MV qui contrôle l'accès et la provenance des ces images à travers des filtres et scanners (fouille de données)
- *Zhou et ses collaborateurs, 2011* (vulnérabilité du moniteur de la machine virtuelle (MMV)) :  
approche pour éliminer la vulnérabilité de l'hyperviseur XEN (Amazon) basée sur la loi de Poison

# Sécurisation des données par le secret sharing



## ► Proposition :

*Ne pas dépendre d'un seul fournisseur de l'informatique dans les nuages .*

## ► Comment ?

► => Algorithme le partage de clés secrètes de Shamir

► Danwei Chen et Yanjun He, 2010

“ Study on Secure Data Storage Strategy in Cloud Computing”

# Sécurisation des données par le secret sharing



Algorithme le partage de clés secrètes de Shamir

- ▶ Définition :

Algorithme de cryptographie proposé par Adi Shamir en 1979

- ▶ Principe :

- Partition des données à travers la construction d'un polynôme
- Restitution des données à travers le polynôme de Lagrange

# Sécurisation des données par le secret sharing



## ► Phase 1: Partage des données

Choix d'un nombre  $k$

Le coefficient  $a_0$  prend la valeur de secret

Choisir au hasard  $k-1$  coefficients  $a_1 \dots a_{k-1}$

Construire un polynôme de degré  $k-1$  :

$$F(x) = a_0 + a_1x + a_2x^2 + \dots + a_{k-1}x^{k-1}$$

Choisir avec au hasard  $n$  points : avec  $i=1 \dots n$

Calcul des couples  $(i, F(i))$

# Sécurisation des données par le secret sharing



## ► Phase 2 : restitution des données

Restitution des images  $F(i)$  calculées dans la première étape.

Calcul des polynômes de base de Lagrange  $l_i(x)$  par la formule suivante :

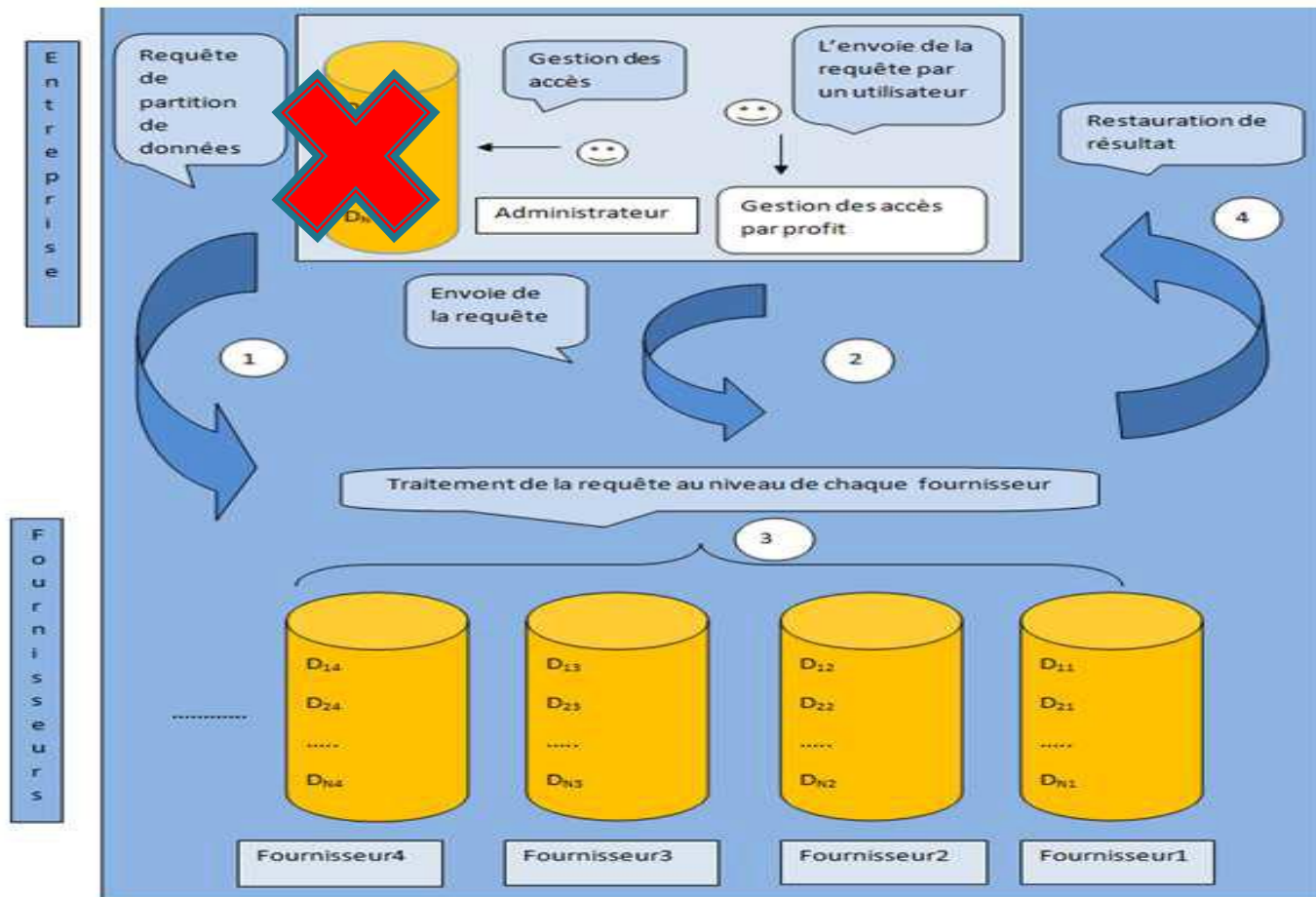
$$l_i(x) = \prod_{j=0, j \neq i}^n \frac{x - x_j}{x_i - x_j}$$

Construction du polynôme  $F(x)$  à travers les images  $F(i)$  et les polynômes de base  $l_i(x)$

# Sécurisation des données par le secret sharing



- Scénarios d'un entrepôt de données partagé dans le nuage



# Sécurisation des données par le secret sharing



- ▶ Niveaux de sécurité attendu :

Capacité de  
restauration des  
données

Sécurité des  
transactions

Confidentialité des  
données

# Sécurisation des données par le secret sharing



- ▶ Choix des coefficients :

$$F(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + \dots + a_{K-1}x^{K-1}$$

- ▶ Complexité Temporelle :

Danwei Chen et Yanjun He, 2010

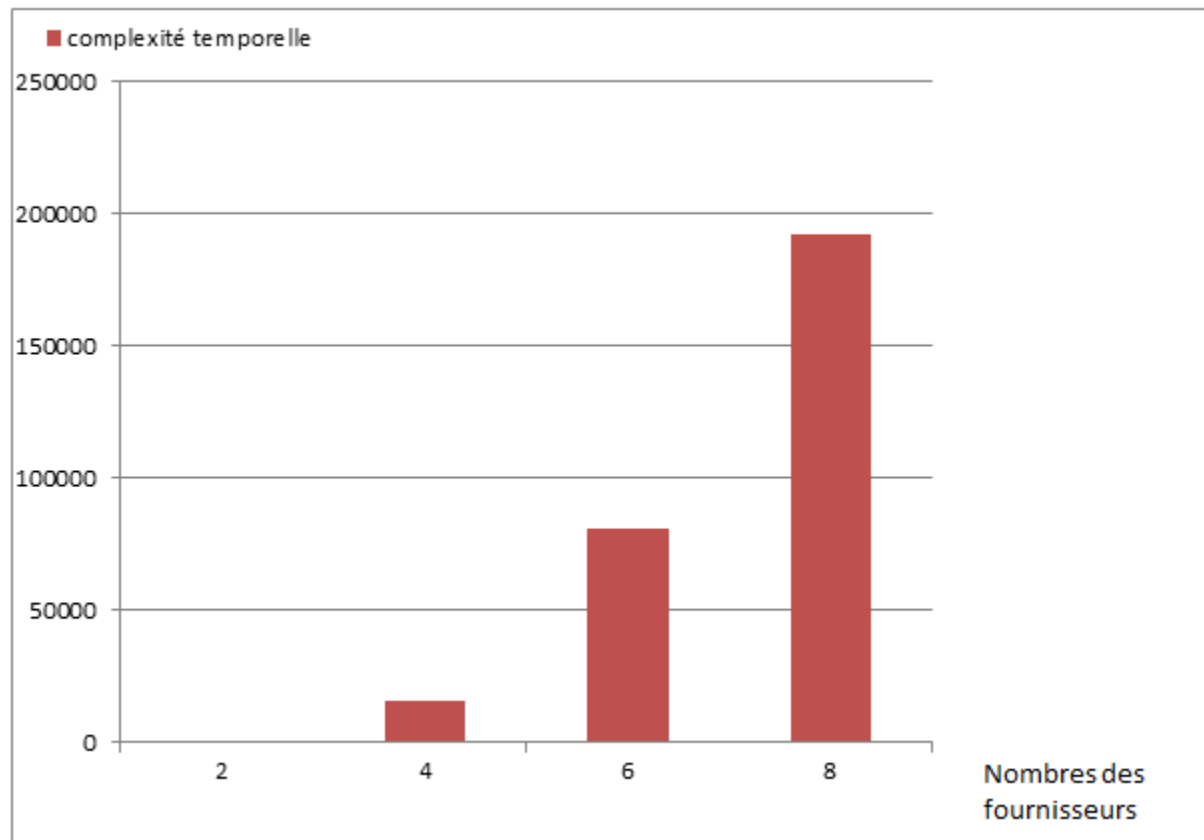
“Study on Secure Data Storage Strategy in Cloud Computing”

$$[ P^{K-1} / (K-1) ! ]$$

# Sécurisation des données par le secret sharing



## ► Complexité Temporelle :



# Sécurisation des données par le secret sharing



- ▶ Résultats théoriques : Rapport coût/risque

$$D * C_S + T * C_T + T_{rq} * C_{Tr} = C_{tot}$$

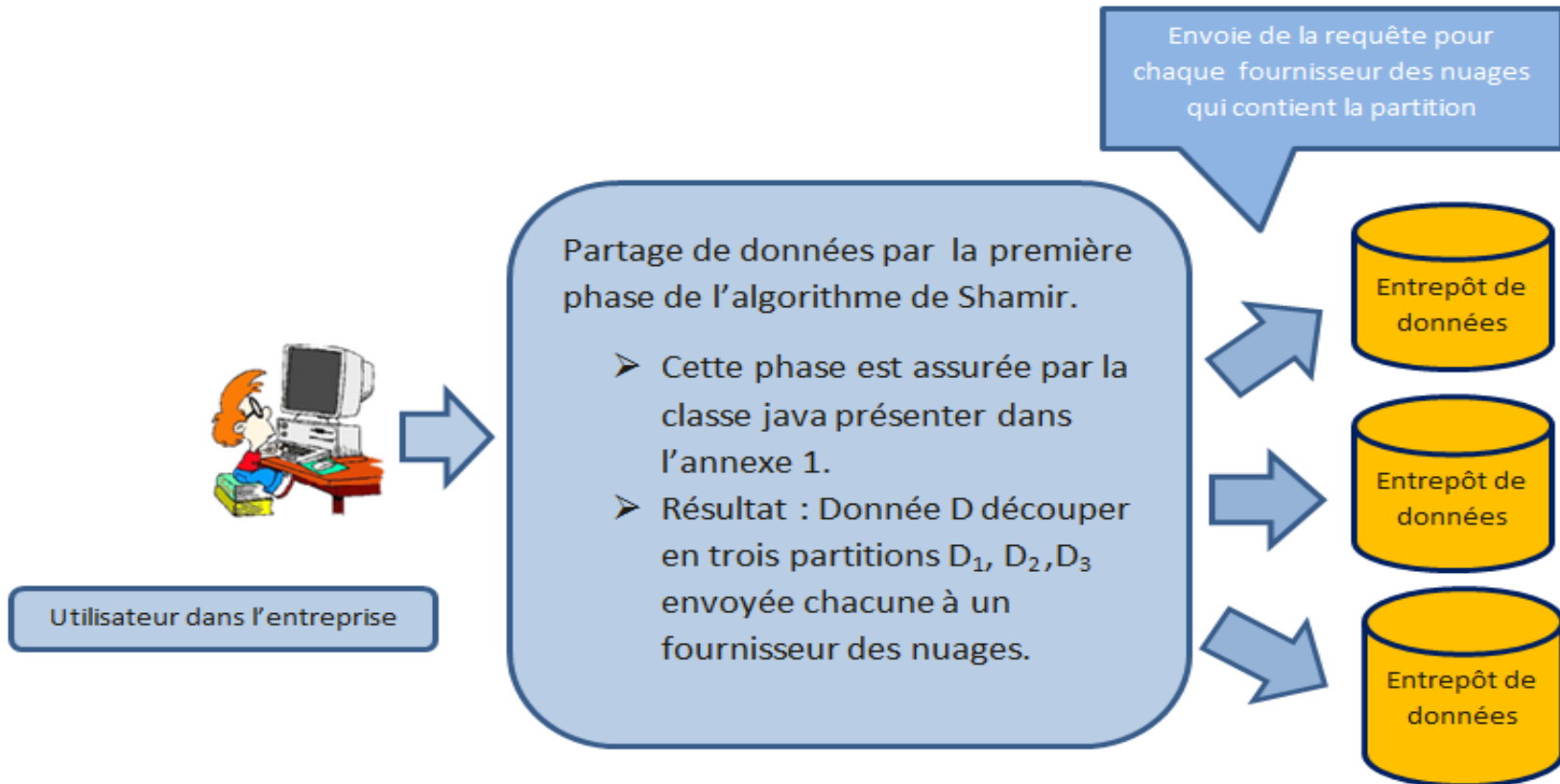
$$\sum_{i=1}^n (D_i * C_{Si} + T_i * C_{Ti} + T_{rqi} * C_{Tri}) = C_{tot}$$

$$C_{tot} / \text{coût des risques} < 1$$

# Mise en pratique de la proposition



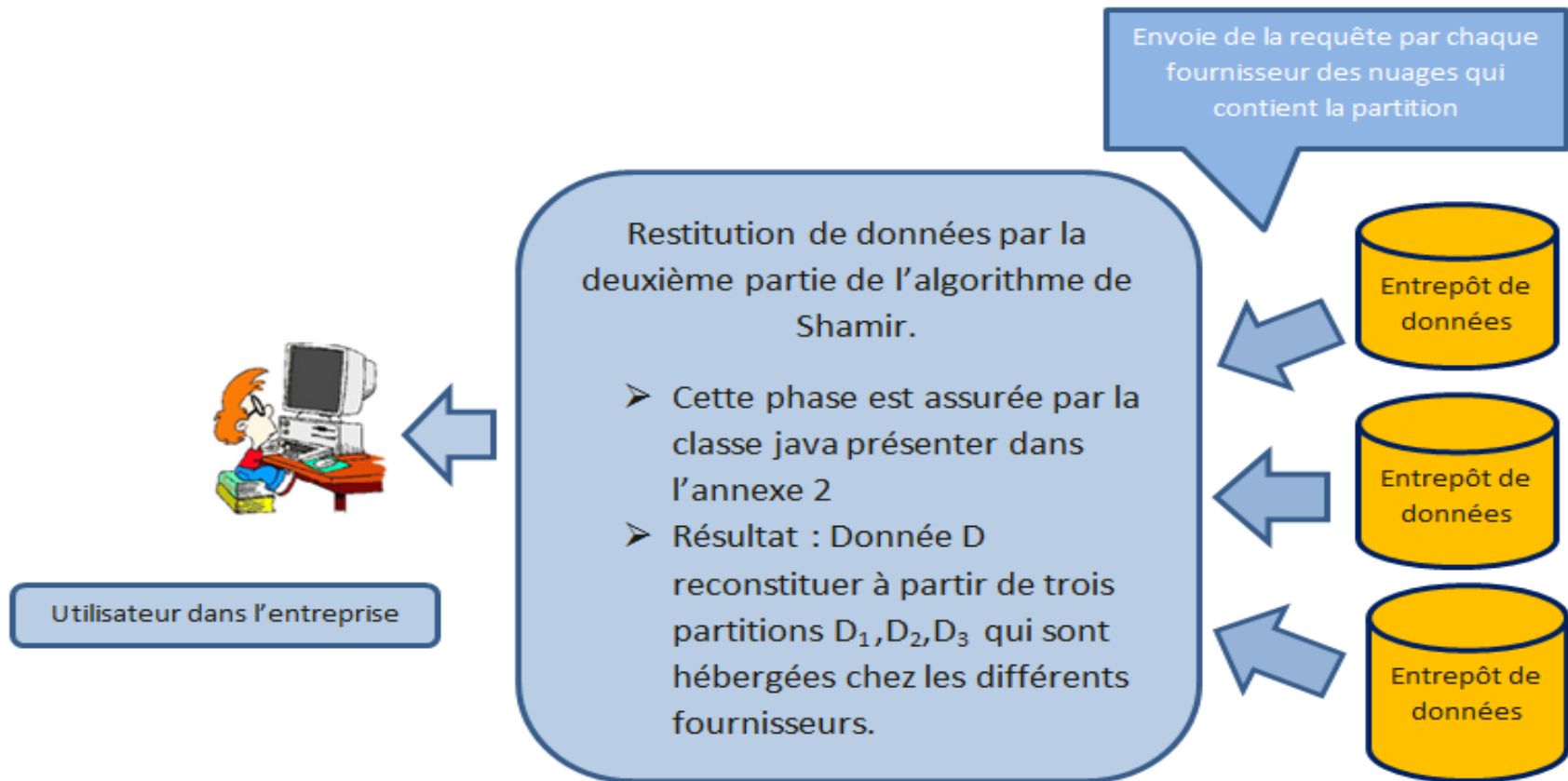
## ► *Etape 1* : Partage des données :





# Mise en pratique de la proposition

- ▶ *Etape 2* : Restitution des données :

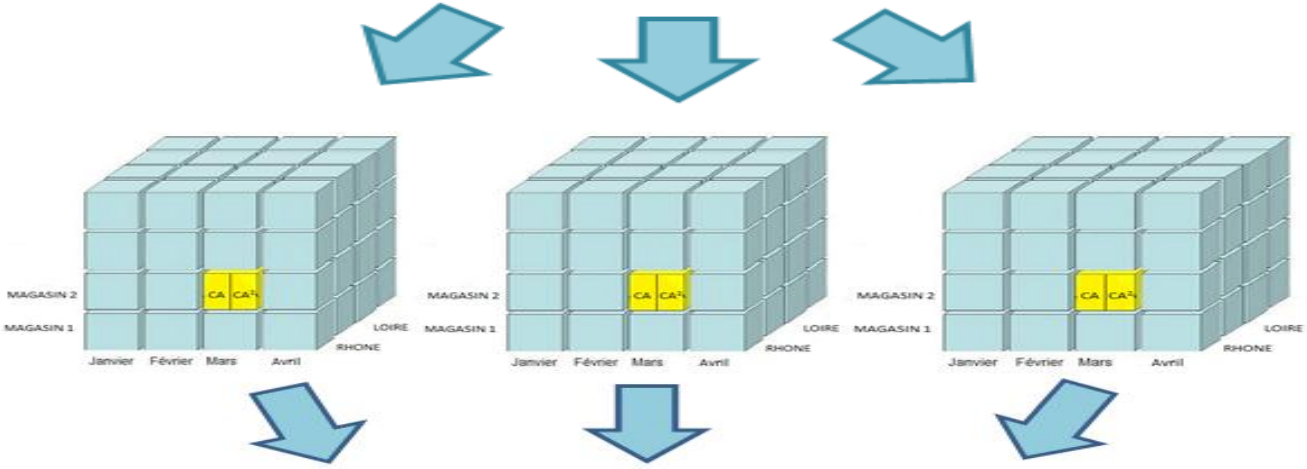




# Mise en pratique de la proposition

► Variance :

Multiplier les différentes valeurs de chiffre d'affaire :  $CA^2$



Restitution :

- $\sum CA$
- $\sum CA^2$
- Nombre d'enregistrement
- =>calcul de la variance



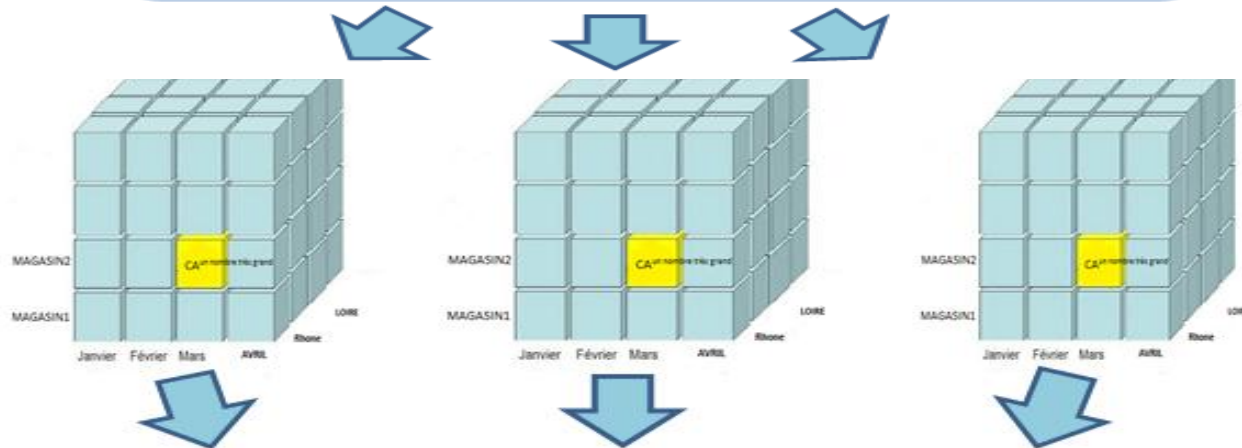
# Mise en pratique de la proposition

## ► Maximum :

Calculer :

$$-CA^{nbr}$$

Où nbr est un nombre très grand



Restituer:

$$- \sum CA^{nbr}$$

=> Application de la deuxième phase de l'algorithme de secret Sharing sur la somme.

=> Calcul de  $R^{1/nbr}$

# Conclusion



## Sécurité des données dans les nuages (Cloud Computing)

### ➤ Proposition :

#### ▶ Plusieurs fournisseurs

#### ▶ Création d'un prototype assurant :

- *partage et restitution des données* basé sur l'algorithme 'partage de clés secrètes de Shamir'
- *opérateurs d'agrégation* (Max, Count, variance, moyenne) pour l'analyse OLAP.

### ➤ Avantages

- Restauration en cas de non disponibilité de service
- Sécurité de transfert des données
- Confidentialité des données

# Perspectives



- ▶ Implémenter d'autres opérateurs nécessaires pour les analyses OLAP exemple Min
- ▶ Appliquer une méthode de gestion des risques pour déterminer le coût du risque de l'indisponibilités des données.
- ▶ Renforcer la sécurité en intégrant la gestion des accès à l'entrepôt basée sur le profil .
- ▶ Etudier la possibilité d'intégrer la cryptographie traditionnelle .

▶ **MERCI POUR VOTRE ATTENTION**

