Confidentialité et disponibilté des données entreposées dans les nuages

Kawthar Karkouda, Nouria Harbi, Jérôme Darmont, Gérald Gavin

Confidentialité et disponibilté des données entreposées dans les nuages

Kawthar Karkouda*, Nouria Harbi**,
Jérôme Darmont **, Gérald Gavin ***

Laboratoire Eric, Université Lumière Lyon 2, 5 avenue Mendès France, Bât K, 69767 Bron Cedex
* kawthar.karkouda@gmail.com ** nouria.harbi,jerome.darmont@univ-lyon2.fr
*** gerald.gavin@univ-lyon1.fr

Résumé. Avec l'avènement de l'informatique dans les nuages (Cloud Computing) comme un nouveau modèle de déploiement des systèmes informatiques, les entrepôts de données profitent de ce nouveau paradigme. Dans ce contexte, il devient nécessaire de bien protéger ces entrepôts de données des différents risques et dangers qui sont nés avec l'informatique dans les nuages. En conséquence nous proposons dans ce travail une façon de limiter ces risques à travers l'algorithme le partage de clés secret de Shamir et nous mettons cette contribution en pratique.

1 Motivation

L'utilisation de l'informatique dans les nuages est basée sur la confiance qu'on peut accorder aux fournisseurs de ce type de service. Une telle situation est difficile et renforcée avec l'architecture traditionnelle du Cloud qui repose sur un seul fournisseur. Cette dépendance menace la confidentialité des données des clients puisque ces dernières sont hébergées chez un seul prestataire externe qui risque de les exploiter.

2 Proposition

Notre proposition consiste à partager chaque donnée à stocker chez plusieurs fournisseurs des nuages à travers l'algorithme de secret Sharing. inspirée de l'idée proposée par Danwei Chen et Yanjun He dans leur article intitulé 'A Study on Secure Data Storage Strategy in Cloud Computing'. Il s'agit d'une solution basée sur l'algorithme de secret sharing qui partage les données en n-uplet et les stocke chez un seul fournisseur. Dans la solution que nous suggérons, notre apport consiste à stoker le n-uplet chez plusieurs fournisseurs. Cette façon de répartir les données permet d'une part de stocker au niveau de chaque fournisseur une partie de l'information, celles-ci sont alors non compréhensibles et non exploitables par un utilisateur malveillant en cas d'intrusion et d'autre part de ne pas dépendre d'un seul fournisseur, ce qui minimise le risque de non disponibilité des données. Les étapes de la démarche sont :
-Chaque fournisseur des nuages possède une copie de l'architecture de l'entrepôt du client.

-Chaque donnée de l'entreprise est partagée et stockée chez les différents fournisseurs de manière à la rendre inexploitable par chaque fournisseur car non significative.
-Le nombre de fragments dépend du nombre de fournisseurs choisis par le client.
-Pour la restauration d'une donnée, le client doit récupérer les fragments stockés chez les différents fournisseurs pour reconstituer la donnée initiale (figure 1).

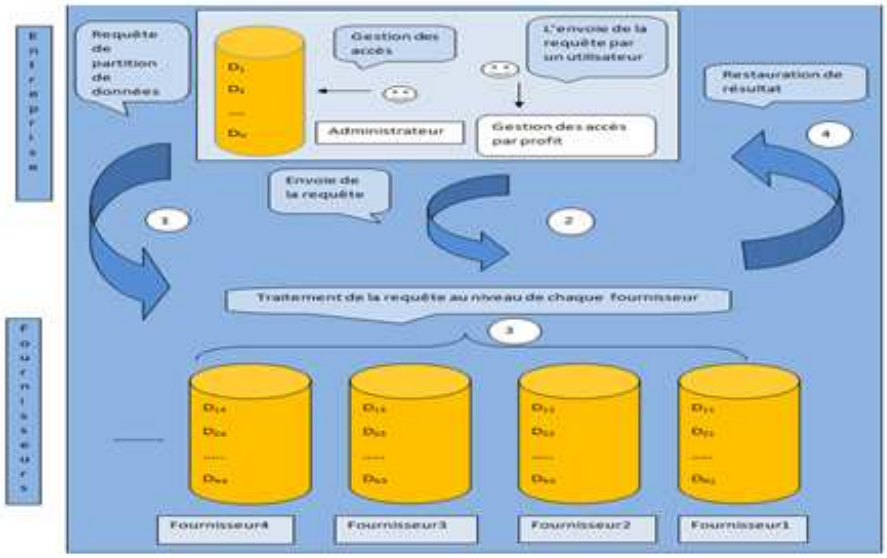

FIG. 1 – *Scénario d'un entrepôt de données partagé dans les nuages*

Notre solution assure trois niveaux de sécurité :
- Capacité de restauration des données en cas de non disponibilité du service ou de la disparition d'un fournisseur puisque l'idée est basée sur l'algorithme de secret sharing qui est capable de reconstituer la donnée initiale à partir d'un nombre prédéfini de fragments qui peut être inférieur au nombre de fragments stockés chez les différents fournisseurs.
- Sécurité des transactions entre le client et les fournisseurs puisque les données qui transitent sur le réseau sont partielles et inexploitables.
- Sécurité des données stockées chez les différents fournisseurs puisque chacun d'eux n'a qu'une partie d'une donnée non significative.

Summary

With the rise of cloud computing as a new model for deploying computer systems, data warehouses benefit from this new paradigm. In this context, it becomes necessary to adequately protect these data warehouses of various risks and dangers that are born with cloud computing .Therefore, we propose in this work a way to limit these risks through the algorithm Shamir's secret Sharing and we make this contribution in practice .