Sécuriser les échanges de données dans le Cloud : Microsoft dit avoir résolu l'équation

Des chercheurs de Microsoft travaillent sur un protocole qui permettra aux utilisateurs issus de différentes parties de sécuriser les échanges de données dans le Cloud. L'idée étant de leur éviter d'avoir à choisir entre facilité d'utilisation des données et sécurité. Plus particulièrement, les efforts de l'éditeur de Redmond portent sur un moyen d'effectuer des traitements des données chiffrées sans avoir à les déchiffrer préalablement. Tout en accordant à l'utilisateur le contrôle des informations échangées.

La solution s'appuie sur un «□système de calcul multipartite□» (ou MPC pour Multi-Party Computation) où chaque entité concernée obtient un résultat sans avoir à exposer ses données chiffrées aux autres parties. *« Cette nouvelle recherche de Microsoft vise à libérer la valeur totale des données cryptées en utilisant le Cloud lui-même pour effectuer des transactions sécurisées de données entre de multiples parties consentantes d'une manière qui offre aux utilisateurs un contrôle complet sur la quantité d'informations que l'échange révèle »*, peut-on lire sur le blog de Microsoft Research. *« Ce que nous essayons de faire est de garder les données privées et, en même temps, d'en extraire la valeur »*, résume Ran Gilad-Bachrach, chercheur du groupe Cryptography Research et co-auteur d'un article sur le sujet.

Se comparer sans connaître les données

Pour mieux comprendre le principe de fonctionnement du système de calcul multipartite, les chercheurs de Microsoft font l'analogie avec un groupe de salariés dont chaque individu souhaiterait connaître son niveau de salaire par rapport aux autres membres, mais sans avoir connaissance des rémunérations de chacun et sans avoir à révéler la sienne. Aux yeux des scientifiques de Redmond, il suffirait que chaque employé dévoile ses revenus à un collègue de confiance, lequel calculerait la moyenne de l'ensemble des salaires avant de communiquer le résultat final à tous. Une information qui permettrait ainsi à chacun de vérifier où il se situe par rapport à cette moyenne sans pour autant connaître les rémunérations des autres collaborateurs. Mais encore faudrait-il que le collègue confident oublie tout ce qu'il a appris au cours de sa collecte d'informations. *« Cet échange de données sécurisé émule ce procédé, mais sans imposer la présence d'un collègue de confiance »*, précise Peter Rindal, doctorant à l'Université d'État de l'Oregon et également co-auteur de l'article sur le sujet aux côtés de Kim Laine, Kristin Lauter et Mike Rosulek.

[Dossier : Comment garantir la sécurité du Cloud public]

En transposant ce principe au Cloud, lieu d'échange par excellence de données, l'usage du système de calcul multipartite permettrait d'opérer une fonction sur un ensemble de données sécurisées et de révéler le résultat de cette fonction aux différents propriétaires de l'ensemble des données. Une entreprise pourrait ainsi savoir où elle se situe en cours d'exercice par rapport à ses concurrentes (du moins celles qui accepteraient également de partager leurs données), sans redouter une quelconque forme d'espionnage commercial.

Même le Cloud ignore ce qui est calculé

« Tout le calcul s'effectue dans le Cloud, et le calcul lui-même est chiffré de manière que même le Cloud ignore ce qui est calculé, ce qui protège les données de l'utilisateur, comme un algorithme propriétaire, assure Microsoft sur son blog. *Si tout se passe comme prévu, le Cloud révèle les résultats déchiffrés aux parties intéressées. »* Mais pas les données initiales, donc.

Notons que l'activité Cloud constitue une forte source de revenus pour Microsoft. Le mois dernier, Redmond a déclaré que le chiffre d'affaires généré par son offre Azure avait progressé de 100 % en un an, tout comme l'usage de la plate-forme de Cloud public.

Adaptation d'un article de TechWeekEurope.

Lire également

Sécurité du Cloud : le flou demeure entre l'IT et les métiers
Google dévoile un peu la sécurité de ses datacenters