L'homomorphie est-elle l'avenir du Cloud ?

L'organisme qui confie son information à un Cloud mutualisé, semi-public ou public perd la gouvernance d'une partie de son système d'information. Cette appréhension ajoutée à la crainte que le Cloud pourrait ne pas être un endroit suffisamment sécurisé, surtout pour traiter l'information sensible, sont les principaux freins perçus avant de sauter dans le nuage.

Ce qui importe aujourd'hui, avec la disponibilité et la gouvernance de son système d'information, c'est la confidentialité et aussi l'intégrité des informations confiées au Cloud qui sont rendues possibles par les mécanismes de chiffrement.

Le problème est que si les données, confiées à un Cloud, sont chiffrées, comment les utiliser pour leur faire subir un traitement ? Une solution simple consiste bien entendu à rapatrier les données à traiter, les déchiffrer puis effectuer, chez soi, le traitement sur ces données en clair. Mais cela fait perdre le principal bénéfice du Cloud qui, au delà d'être un seul espace de stockage, peut être aussi, et surtout, un espace de traitement. D'autant plus que c'est là que résideront les puissances de calcul de demain.

Alors faut-il se résigner à ne pas chiffrer ? Non, car ce problème pourra être résolu avec élégance par le **chiffrement homomorphique**. Essayons d'expliquer, de manière très simple, en quoi ce chiffrement consiste.

Prenons comme données à traiter la valeur "1" et la valeur "2". Nous voulons additionner ces valeurs entre elles, soit calculer 1+2 (ça fait 3 :-)).

Mais vous avez confié ces données "1" et "2", après les avoir chiffrées, à un Cloud. Le résultat du chiffrement de "1" a donné, mettons les valeurs "103" et "43". Pourquoi deux valeurs et pas une ? Pour rester plus près de la réalité du chiffrement homomorphique, et parce que ça n'entraine pas vraiment de complication dans ce papier qui se veut très simple. De même le résultat du chiffrement de "2" a donné les valeurs "51" et "95".

Si vous demandez au Cloud d'additionner les deux valeurs confiées (les valeurs chiffrées de "1" et de "2") tout ce qu'il pourra calculer est "103 + 51 = 154" et "43 + 95 = 138".

So what ? Que faire avec ce résultat "154, 138" que vous rapatriez chez vous ?

Et bien si vous avez utilisé le chiffrement homomorphique depuis le début, le déchiffrement de "154, 138" donnera la valeur ... "3".

Miraculeux non !!! ?

Bon le chiffrement homomorphique fait appel à la théorie des groupes qui est une partie complexe des mathématiques et hors sujet dans ce travail de simplification extrême.

Dans le Cloud, les données confiées sont et restent chiffrées, le résultat du calcul aussi. En rapatriant ce résultat chez vous, comme vous seul connaissez la ou les clés pour déchiffrer, vous seul pouvez obtenir, en clair, le résultat du traitement.

Mais pas de précipitation, le chiffrement homomorphique à l'usage du Cloud, pour tout traitement pouvant y être effectué : recherches dans des bases de données, statistiques, calculs..., n'est pas disponible dans le commerce aujourd'hui, et ne le sera sans doute pas dans un futur très proche. Mais il a tout de même déjà un nom dont on parlera de plus en plus : le "**fully homomorphic encryption scheme**".

Et ne nous endormons pas en pensant que quelque chose est impossible, car nous serions réveillés par le bruit fait par notre voisin en train d'achever de la réaliser.

Gérard Peliks
Expert sécurité
CyberSecurity Centre
CASSIDIAN