Stage de Master 2 (6 mois)

Sécurisation des analyses en ligne d'entrepôts de données partagés.

Référence. SSBi4 (à rappeler dans toute correspondance)

Lieu : laboratoire Eric - Campus Porte des Alpes, Bron **Tél :** 04 78 77 31 54

Responsable(s) du stage (Email) :

- Gérald Gavin (gerald.gavin@univ-lyon1.fr)
- Jérome Darmont (jerome.darmont@univ-lyon2.fr)
- Fahad Muhammad (mhd.fahad@gmail.com)

Thématique(s). Business Intelligence et sécurité

Type de stage. Fin d'études bac+5, Master 2

Durée : 6 mois

Période souhaitée. Printemps 2021

Intitulé. Sécurisation des d'analyses en ligne d'entrepôts de données partagés.

Sujet. Ce stage se fera dans le cadre du projet ANR BI4people (http://eric.univ-lyon2.fr/bi4people/). L'utilisation des technologies de la *Business Intelligence* (BI) telles que les entrepôts de données et les techniques d'analyses en ligne (OLAP) restent complexes et restent réservées à des spécialistes. L'objet de ce projet est de simplifier ces outils afin de les rendre accessible au plus grand nombre, par exemple des petites entreprises, des associations, etc.

Dans ce contexte, il est important de permettre aux utilisateurs de pouvoir partager leurs données et leurs analyses. Ces aspects collaboratifs induisent des problèmes de confidentialité de données. Plus généralement, on peut considérer des scenarios où la confidentialité des données et/ou des requêtes doivent être garanties. On pourrait également imaginer que des utilisateurs agissent de manière malveillante afin d'altérer les calculs afin de compromettre le résultat des requêtes.

Quelques solutions sont proposées dans la littérature [1, 2]. Les plus abouties en termes de sécurité sont basées sur des primitives cryptographiques récentes,

appelées FHE (*Fully Homomorphic Encryption*). Ces solutions n'ont à ce jour qu'un intérêt théorique puisque les FHE existants ne sont pas encore suffisamment performants [3]. Pour obtenir des solutions utilisables en pratique, il est donc nécessaire de rogner sur la sécurité et/ou sur le type de requêtes pris en charge. Des hypothèses sur les utilisateurs peuvent aussi être introduites, comme par exemple la proportion d'utilisateurs malveillants, le fait qu'ils soient coalisés ou non, etc.

L'objectif de ce stage est d'explorer, d'évaluer et de comparer les solutions existantes. Suite à cette analyse de l'état de l'art, il s'agira de proposer des solutions dédiées à la problématique et aux contraintes spécifiques du projet BI4people.

[1] *Raluca A. Popa*, Catherine M. S. Redfield, Nickolai Zeldovich, Hari Balakrishnan: CryptDB: protecting confidentiality with encrypted query processing. SOSP 2011: 85-100

[2] Dan Boneh, *Craig Gentry*, Shai Halevi, Frank Wang, David J. Wu: Private Database Queries Using Somewhat Homomorphic Encryption. ACNS 2013: 102-118

[3] Ilaria Chillotti, *Nicolas Gama*, Mariya Georgieva, Malika Izabachène:
TFHE: Fast Fully Homomorphic Encryption Over the Torus. J. Cryptol. 33(1): 34-91 (2020)

Profil du stagiaire. Compétences avancées (niveau M2) en informatique. Notions de cryptographie et/ou de sécurité informatique fortement souhaitées.

Merci d'adresser, avant le 15 décembre 2020, votre candidature avec un CV, une lettre de motivation ainsi que vos notes de l'année universitaire en cours et de l'année dernière à gerald.gavin@univ-lyon1.fr et jerome.darmont@univ-lyon2.fr