Stage de Master 2 (6 mois)

Cryptographie

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

Responsables du stage (Email) :

- Gérald Gavin (gerald.gavin@univ-lyon1.fr)
- Mohamed-Lamine Messai (mohamed-lamine.messai@univ-lyon2.fr)
- Jérome Darmont (jerome.darmont@univ-lyon2.fr)

Thématiques : Business Intelligence, sécurité, cryptographie

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

Durée : 5-6 mois

Période souhaitée : à partir de février 2022

Rémunération : Indemnités de stage légales (environ 550 € par mois)

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

Sujet : Ce stage se déroulera dans le cadre de l'ANR BI4people (https://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 réservées à des spécialistes. L'objet de cette ANR est de simplifier ces outils afin de les rendre accessible au plus grand nombre (petites entreprises, 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 ou des requêtes doit être garantie. On pourrait également

imaginer que des utilisateurs agissent de manière malveillante afin d'altérer les calculs et 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 existantes ne sont pas encore suffisamment performantes [3]. Pour obtenir des solutions utilisables en pratique, il est donc nécessaire de dégrader la sécurité ou le type de requêtes prises en charge. Des hypothèses sur les utilisateur·trices 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 BI4 people.

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

Merci d'adresser, avant le 1er décembre 2021, 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, mohamed.messai@univ-lyon2.fr et jerome.darmont@univ-lyon2.fr.

Références

[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)