Stage de Master 2 (5-6 mois)

Référence : MPC4BI (à rappeler dans toute correspondance)

Lieu : Laboratoire ERIC, Campus Porte des Alpes, Bron. **Tél :** 04 78 77 31 54

Responsables du stage (Emails) :

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

Thématiques : MPC, BI sécurisée

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

Durée : 5-6 mois

Période souhaitée : à partir de février 2024

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

Intitulé : Calcul multipartie sécurisé pour l'amélioration de l'informatique décisionnelle dans le projet BI4people

Sujet : La sécurité des données est un sujet crucial dans la plupart des applications informatiques actuelles. Le projet ANR BI4people (https://eric.univ-lyon2.fr/bi4people/) vise à développer un système de business intelligence (BI) accessible à des utilisateurs novices. Un des enjeux importants de ce projet est de garantir la confidentialité des données utilisateurs. Le sujet du stage proposé s'inscrit dans ce cadre.

Une analyse du problème de la confidentialité des données a été réalisée au cours de la première partie de ce projet. Les cryptosystèmes homomorphes (Homomorphic encryption) permettant d'effectuer des calculs sur des données cryptées sont particulièrement adaptés à cette problématique. Une étude approfondie de ces outils et de leur implémentation a été réalisée [1].

L'objectif de ce stage est de proposer différents scenarii, de les analyser et de les implémenter en utilisant les cryptosystèmes homomorphes les plus adaptés. Plus précisément, vous serez impliqué(e) dans les activités suivantes :

1. Découverte des cryptosystèmes homomorphes et prise en main des bibliothèques analysées au début du projet [1].
2. Étude des protocoles de calcul multipartie sécurisé : Vous explorerez les différents protocoles de MPC, en vous concentrant sur leur applicabilité dans le contexte du projet BI4people [2].
3. Développement de scénarii de BI collaborative et construction de protocoles de calcul multi-parties pour les sécuriser [3].
4. Évaluation des performances et de la sécurité de ces protocoles en termes de temps de calcul, d'utilisation des ressources
5. Analyse de sécurité de ces protocoles pour évaluer les vulnérabilités potentielles et proposer des mesures d'amélioration.
6. Intégration dans le projet BI4people : Vous travaillerez en étroite collaboration avec les autres membres de l'équipe du projet BI4people, en participant aux réunions et en partageant les résultats et les avancées de votre recherche.

Profil du/de la stagiaire : Compétences avancées (niveau M2) en informatique (sécurité informatique, cryptographie fortement souhaitées). Compétences en programmation (par exemple, Python).

- **Merci d'adresser, avant le 31 décembre 2023, 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** mohamed-lamine.messai@univ-lyon2.fr et gerald.gavin@univ-lyon1.fr

Références

[1] T. V. T Doan, M-L. Messai, G. Gavin & J. Darmont. A survey on implementations of homomorphic encryption schemes. *The Journal of Supercomputing*, 2023, p. 1-42.

[2] Y. Wu, X. Wang, W. Susilo, G. Yang, Z. L. Jiang, S. M. Yiu, & H. Wang. Generic server-aided secure multi-party computation in cloud computing. *Computer Standards & Interfaces*, 2022, vol. 79, p. 103552.

[3] Tran, H. Y.. *Privacy-preserving schemes for electricity data analytics in smart grids*. 2023. Thèse de doctorat. UNSW Sydney.