Université Claude Bernard Lyon 1

DIPLÔME NATIONAL DE DOCTORAT

(Arrêté du 25 mai 2016)

Date de la soutenance :**16 décembre 2024**

Nom de famille et prénom de l'auteur : **Monsieur Farouk DAMOUN**

Titre de la thèse : Amélioration de l'Apprentissage Fédéré pour le Secteur Financier via l'Apprentissage par Graphes et les Modèles de Langage

Résumé

Dans le secteur financier moderne, la nécessité de modèles d'apprentissage automatique robustes devient de plus en plus cruciale, mais les réglementations sur la confidentialité et les préoccupations concurrentielles rendent souvent la centralisation des données impossible. Pour surmonter ces défis, cette thèse propose de nouvelles méthodologies de l'apprentissage fédéré (FL) permettant aux institutions de collaborer pour entraîner des modèles machine learning tout en abordant les compromis critiques entre la confidentialité et l'utilité des données, en intégrant des mécanismes de préservation de la confidentialité conçus pour empêcher la récupération des entrées avec une perte minimale d'utilité des données. Une contribution clé de cette recherche est le développement d'un framework d'apprentissage fédéré pour la détection d'anomalies comportementales et la détection de la fraude dans les transactions financières. En utilisant des réseaux neuronaux de graphes (GNNs) sur des graphes dynamiques ego-centriques, qui permet de capturer et de détecter les schémas transactionnels évolutifs afin de repérer les anomalies, tout en préservant la

confidentialité des individus. Une nouvelle technique d'échantillonnage négatif spécifique au domaine permet l'entraînement du modèle sans la nécessiter de données étiquetées de la part des participants à la fédération, ce qui le rend applicable dans des scénarios industriels. Les résultats montrent que les méthodes basées sur l'apprentissage profond, en particulier les GNNs, surpassent les approches traditionnelles dans la détection d'anomalies et améliorent la détection des fraudes dans les données transactionnelles, en introduisant des mécanismes d'anonymisation et de bruit, même lorsque les gradients des modèles fédéré sont exposés. De plus, nous proposons G-HIN2Vec, une technique basée sur les réseaux neuronaux de graphes pour les réseaux d'information hétérogènes, qui modélise des individus, tels que les détenteurs de cartes, en utilisant des graphes ego-centriques statiques et dynamiques. Cette méthode sert de mécanisme d'anonymisation qui élimine la nécessité d'utiliser un identifiant individuel, tel que les informations personnellement identifiables (PII), dans les modèles fédérés. En intégrant la confidentialité différentielle locale personnalisée (PLDP), nous fournissons une couche de protection supplémentaire, garantissant que même en cas de violation du modèle, les données sensibles restent sécurisées. Enfin, la thèse introduit le tokenizer fédéré basé sur le codage par paires de caractères (BPE) au niveau du byte (Byte-level), une approche de tokenisation respectant la confidentialité des individus mentionnés dans les données textuelles sous forme de PII, conçue pour les ensembles de données textuelles distribuées. Ce tokenizer surpasse les modèles existants en termes de couverture du vocabulaire et d'efficacité, tout en maintenant une stricte confidentialité des données. Notre tokenizer fédéré non seulement concurrentiel par rapport aux modèles centralisés, mais démontre également des améliorations en matière de compression de texte et de préservation de la confidentialité, pour les tokenizers généraux (General domain) et spécifiques au domaine (Domain specific). Les méthodologies présentées dans cette thèse, validées à l'aide de bases de données financières réelles, publiques et privées, transactionnelles et textuelles, mettent en évidence le potentiel de l'apprentissage fédéré pour améliorer la détection de la fraude et les performances des modèles de langage tout en préservant la confidentialité des individus et des institutions grâce

à des mécanismes d'anonymisation et de confidentialité basés sur le bruit.

Mots-clés : Réseaux de neurones,réseaux de neurones de graphe,Apprentissage fédéré,apprentissage automatique