Thèse CIFRE : Détection de fraude sur les paiements par carte bancaire

INFORMATIONS CLÉS

Thèse CIFRE dans le cadre de la chaire avec le partenaire industriel LUSIS et CentraleSupélec
Établissement : Université Paris-Saclay et CentraleSupélec
École doctorale : Sciences et Technologies de l'Information et de la Communication
Spécialité : Informatique
Domaine : Intelligence Artificielle - Apprentissage automatique
Unité de recherche : LRI - Laboratoire de Recherche en Informatique, équipe AO/LAHDAK
Directeur de la thèse : Bich-Liên Doan
Co-encadrement : Fabrice Popineau
Contacts pour envoi de candidature : Fabrice Popineau (Fabrice.Popineau@lri.fr) - Bich-Liên Doan (Bich-Lien.Doan@lri.fr) - Arpad Rimmel (Arpad.Rimmel@lri.fr)
Début de la thèse : septembre 2020
Date limite de candidature : <sans limite>

Mots-clés

Détection de fraude, apprentissage automatique, explicabilité

Profil et compétences recherchées

Le candidat devra faire preuve de bonnes compétences en programmation et montrer une connaissance des toolkits dédiés à l'apprentissage automatique comme scikit-learn et tensorflow.

Contexte

Lusis est l'éditeur de TANGO, une plateforme transactionnelle à haute performance pour les systèmes de paiements et la finance de marché. Sur la base de cette plateforme Lusis réalise des systèmes de paiements complets, incluant la détection de fraude, ainsi que des plateformes de trading front to back extrêmement riches et complexes sur lesquelles se traitent aujourd'hui plus de 5 Milliards de dollars par jour, répartis pour moitié sur le Forex et sur les Indices et Matières Premières. Lusis et CentraleSupélec se sont associés en créant une chaire de

recherche pour renforcer leur collaboration dans le domaine de l'intelligence artificielle appliquée au domaine bancaire.

Sujet de thèse

Aujourd'hui, les paiements électroniques par carte bancaire se sont généralisés sur la planète grâce à l'internet. Ces paiements représentent un volume toujours en augmentation de plus de 500 milliards de dollars annuels, et les fraudes constituent moins de 0,5% du nombre de ces transactions. Au niveau mondial, cela représente environ 25 milliards de dollars de pertes estimées par an.

Indépendamment du montant de cette fraude, il faut bien entendu mettre en oeuvre toutes les mesures de détection possibles pour en limiter l'extension. C'est pourquoi de nombreux travaux de recherche ont vu le jour depuis les 20 dernières années sur cette problématique.

Cela représente bien sur un intérêt stratégique pour les particuliers, les banques et les entreprises. En tant qu'éditeur d'une plateforme transactionnelle à haute performance pour les systèmes de paiements, LUSIS est donc intéressée au premier chef par les contre-mesures à la fraude. Dans le cadre de la chaire LUSIS, nous souhaitons étudier la détection de fraude à la fois sous l'angle de la performance des algorithmes, mais également avec une contrainte de réalisme de mise en oeuvre et ce sur des données réelles.

La détection de fraude à la carte bancaire est étudiée depuis de nombreuses années, mais le manque de données réelles étiquetées rend la tâche difficile, à la fois pour l'apprentissage et pour l'évaluation (Parthasarathy et al., 2019).

Opérationnellement, il faut éviter au maximum les faux positifs : les clients n'aiment pas beaucoup voir leurs paiements refusés à tort. Pour des raisons de contrôle du processus, les systèmes déployés aujourd'hui reposent sur des règles. De ce fait, ils sont lourds en traitement et surtout en mise à jour. Les systèmes fondés sur l'apprentissage automatique sont essentiellement à l'étude pour l'instant.

Ces dernières années, les algorithmes de machine learning et deep learning ont montré leur efficacité dans de nombreux domaines. Les principales méthodes d'apprentissage automatique ont toutes été essayées sur ce problème : arbres de décision, random forests, réseaux bayésiens, modèles de Markov cachés, réseaux de neurones et réseaux de neurones profonds (Ryman-Tubb et al., 2018). La difficulté spécifique à la fraude réside dans un très grand déséquilibre entre les classes "fraude" et "non-fraude" (moins de 0,5% de fraude) et au caractère essentiellement en ligne du processus, qui n'est pas pris en compte lors d'études hors-ligne (Carcillo et al., 2018).

(Zojaji et al., 2016) établit une classification des techniques en deux approches principales de détection de la fraude, à savoir les abus (supervisés) et la détection des anomalies (non

supervisées) : une classification des techniques est proposée en fonction de la capacité à traiter les ensembles de données numériques et catégorielles. (Kamaruddin & Ravi, 2016) ont utilisé une approche de classification à classe unique en développant une architecture hybride composée d'un algorithme d'optimisation d'un essaim de particule et de réseau neuronal auto-associatif. Les approches par graphes telles que décrites par (Zhang et al., 2019) ou (Belle et al., 2019) sont très récentes et prometteuses.

Face au problème de l'apparition de nouvelles stratégies de fraude, le paradigme de détection d'anomalie (*anomaly detection*) dans les habitudes de paiement des consommateurs prend tout son sens. Dans ce cadre, il faut tenir compte du fait que ces habitudes évoluent dans le temps : c'est ce que l'on nomme *concept drift* ou dérive conceptuelle pour un consommateur. Le modèle FraudMemory développé par (Yang & Xu, 2019) permet de saisir les schémas séquentiels associés à chaque transaction et exploite les réseaux de mémoire (*memory networks*) pour améliorer à la fois la performance et l'interprétabilité tout en prenant en compte la dérive conceptuelle.

Enfin, un dernier point demeure relativement peu exploré dans les travaux relatifs à la détection de fraude au paiement : celui de l'explicabilité. Ce point devient crucial avec la loi RGPD, puisque chaque consommateur qui se verra refuser un paiement valide pourra demander une explication au prestataire.

En conclusion, malgré les très bons résultats obtenus par les techniques comme les *random forests* sur des jeux données collectés, la problématique de la détection de fraude n'est pas résolue et de nombreuses pistes restent à explorer pour atteindre un système robuste dans le temps et explicable.

Grâce à notre partenariat avec l'entreprise LUSIS, nous disposons de jeux de données réelles et d'un champ d'expérimentation de qualité avec des experts métier. Le sujet de thèse que nous proposons portera sur quatre orientations de recherche :

1. les réseaux attribués (« attributed networks »),
2. la détection d'anomalie,
3. la dérive conceptuelle,
4. l'explicabilité.

Dans une première phase d'étude bibliographique, l'étudiant devra synthétiser l'état de l'art sur les méthodes existantes et leurs avantages et inconvénients du point de vue métier. Ensuite, il s'agira de proposer une architecture, éventuellement hybride, répondant aux critères de performance, robustesse et explicabilité.

Références bibliographiques

Belle, R. V., Mitrovic, S., & Weerdt, J. D. (2019). *Graph Representation Learning for Fraud Prediction : A Nearest Neighbour Approach*. 6.

Carcillo, F., Le Borgne, Y.-A., Caelen, O., & Bontempi, G. (2018). Streaming active learning strategies for real-life credit card fraud detection : Assessment and visualization. *International Journal of Data Science and Analytics*, *5*(4), 285‑300. https://doi.org/10.1007/s41060-018-0116-z

Kamaruddin, Sk., & Ravi, V. (2016). Credit Card Fraud Detection using Big Data Analytics : Use of PSOAANN based One-Class Classification. *Proceedings of the International Conference on Informatics and Analytics - ICIA-16*, 1‑8. https://doi.org/10.1145/2980258.2980319

Parthasarathy, G., Ramanathan, L., JustinDhas, Y., Saravanakumar, J., & Darwin, J. (2019). Comparative Case Study of Machine Learning Classification Techniques Using Imbalanced Credit Card Fraud Datasets. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3351584

Ryman-Tubb, N. F., Krause, P., & Garn, W. (2018). How Artificial Intelligence and machine learning research impacts payment card fraud detection : A survey and industry benchmark. *Engineering Applications of Artificial Intelligence*, *76*, 130‑157. https://doi.org/10.1016/j.engappai.2018.07.008

Yang, K., & Xu, W. (2019, janvier 8). *FraudMemory : Explainable Memory-Enhanced Sequential Neural Networks for Financial Fraud Detection*. https://doi.org/10.24251/HICSS.2019.126

Zhang, Z., Cui, P., & Zhu, W. (2019). Deep Learning on Graphs : A Survey. *arXiv:1812.04202 [cs, stat]*. http://arxiv.org/abs/1812.04202

Zojaji, Z., Atani, R. E., & Monadjemi, A. H. (2016). *A Survey of Credit Card Fraud Detection Techniques : Data and Technique Oriented Perspective*. 26.