Stratégie d'intégration de l'apprentissage automatique

1. Objectif

L'objectif de cette stratégie est de décrire comment les modèles d'apprentissage automatique sont intégrés dans l'architecture de données afin de détecter les transactions frauduleuses.

Le modèle de machine learning complète les systèmes OLTP, OLAP et NoSQL en apportant une capacité d'analyse automatique basée sur les données historiques et en temps réel.

2. Sources de données et extraction des caractéristiques

Les modèles d'apprentissage automatique utilisent des données provenant de plusieurs systèmes :

- **OLTP** : données transactionnelles (transactions, clients, marchands, appareils, localisations).
- **OLAP** : données historiques et agrégées (revenus, historique de fraude, activité client).
- **NoSQL** : données non structurées (logs, interactions utilisateurs, résultats de scoring précédents).

Les pipelines de données sont orchestrés par **Airflow**.
Les données sont nettoyées et préparées afin de créer des caractéristiques (features) exploitables par le modèle.

Les données préparées sont stockées :

- dans le système OLAP pour l'entraînement des modèles,
- dans le système NoSQL pour le scoring en quasi temps réel.

3. Entraînement du modèle

L'entraînement du modèle est réalisé de manière périodique à partir des données historiques.

Processus général :

- extraction des données depuis le système OLAP,
- création d'un jeu de données d'entraînement avec des transactions labellisées (fraude / non fraude),
- entraînement du modèle sur ces données.

Les paramètres du modèle et les résultats des entraînements (métriques principales) sont enregistrés afin d'assurer la traçabilité et le suivi des performances.

4. Déploiement du modèle

Le modèle entraîné est déployé sous la forme d'un service de scoring.

Lorsqu'une nouvelle transaction est traitée :

- les données de la transaction sont envoyées au modèle,
- le modèle retourne un score de risque de fraude,
- une décision (acceptée, à vérifier, rejetée) est associée à la transaction.

Les résultats du scoring sont stockés dans la collection **fraud_analysis** du système NoSQL afin d'être consultables par les équipes et exploitables pour l'analyse.

5. Surveillance et réentraînement du modèle

Les performances du modèle sont surveillées afin de s'assurer de sa fiabilité dans le temps.

Les éléments surveillés incluent :

- le taux de détection de la fraude,
- le taux d'erreurs,
- la stabilité des données d'entrée.

Lorsque les performances diminuent ou que le comportement des données évolue, un réentraînement du modèle est déclenché à partir de nouvelles données historiques.

Cette approche permet d'adapter le modèle à l'évolution des comportements de fraude.

6. Sécurité et conformité du modèle

L'intégration du machine learning respecte les règles de sécurité et de conformité définies dans l'architecture globale :

- chiffrement des données utilisées par le modèle,
- accès restreint aux jeux de données et aux modèles,
- journalisation des prédictions et des versions du modèle.

Les données personnelles utilisées pour l'entraînement sont anonymisées ou pseudonymisées conformément au RGPD.

7. Conclusion

Cette stratégie permet d'intégrer un modèle d'apprentissage automatique de manière simple et cohérente dans l'architecture de données.
Le modèle s'appuie sur les données historiques et en temps réel pour détecter la fraude tout en respectant les contraintes de sécurité, de traçabilité et de conformité.