Détection de fraude bancaire

Projet de certification – Implémentation d'un modèle de ML pour la néobanque Fluzz

Contexte & Objectifs

Augmentation des transactions frauduleuses dans les néobanques
Les clients sont facturés pour des achats qu'ils n'ont pas réalisés; le coût final est supporté par la banque.

Objectifs du projet

- **Analyser** les transactions historiques pour détecter des **schémas frauduleux**
- **Concevoir** un modèle prédictif **robuste** et **éthique**
- **Déployer** un service de détection avec **tableau de bord**

Cycle de vie des données

- **Acquisition & Stockage** : collecte des données, base interne sécurisé
- **Préparation** : nettoyage, normalisation, gestion valeurs manquante
- **Transformation** : PCA déjà appliquée, feature engineering
- **Entraînement** : orchestration via Airflow pipeline
- **Déploiement** : FastAPI, Docker / Kubernetes
- **Supervision** : Prometheus & Grafana
- **Réentraînement** : intégration de nouveaux jeux de données, amélioration continue

Jeu de données

Jeu de données

- Nombre de lignes: 284807
- Nombre de colonnes: 31

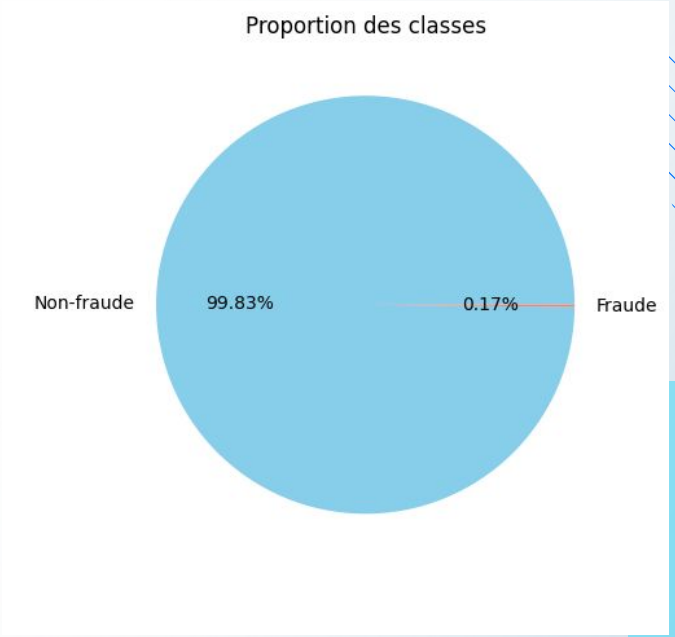
- **Time** contient le montant et l'horodatage de chaque transaction depuis la première du dataset
- **Amount** représente le coût de la transaction
- **V1** à **V28** sont des data pré-process
- **Aucune valeurs null**

Colonne	Null	Type
Time	0	Float
V1 - V28	0	Float
Amount	0	Float
Class	0	Int

Jeu de données

Proportion des classes

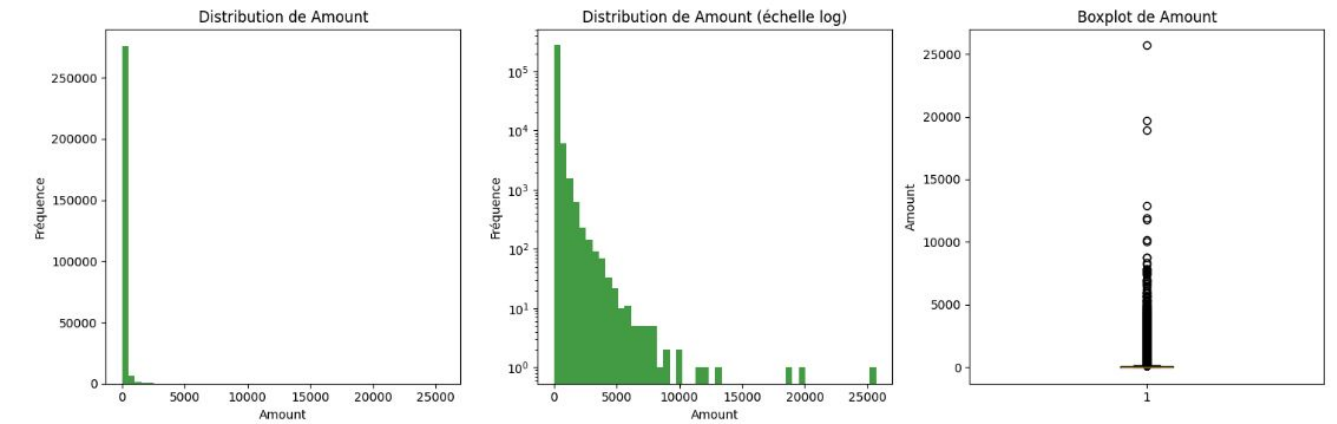
- **284 807 transactions**, **31 variables**, données anonymisées
- Extrêmement déséquilibré : ~**0,17 %** de fraudes



Jeu de données

Analyse sur Amount

- Présente d'outlier (box écraser vers le bas)
- La plupart des valeurs sont petite
- Potentiel utilisation d'un RobustScaler pour atténuer les données aberrantes



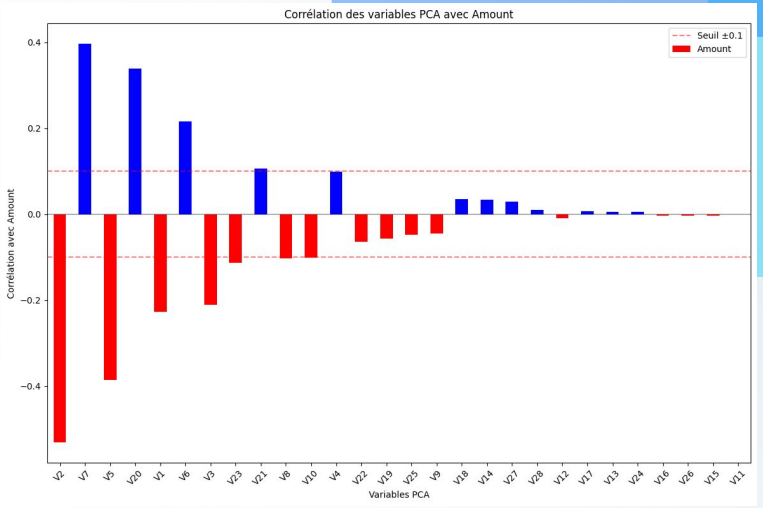
Jeu de données

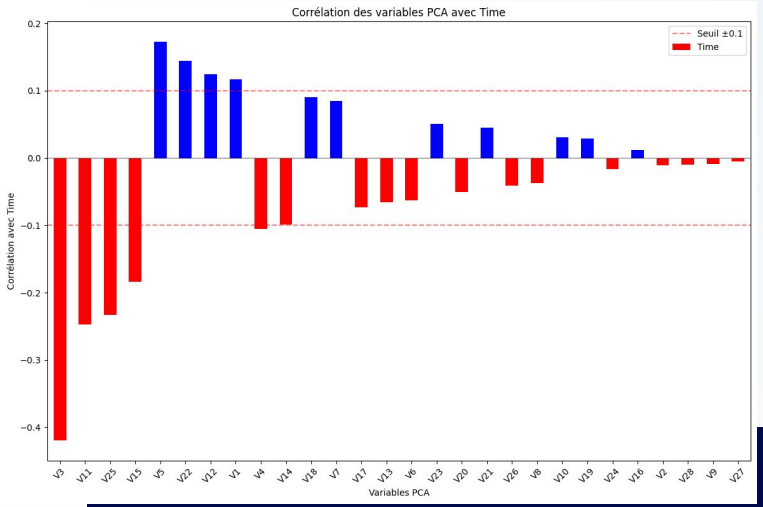
Corrélation avec les valeurs V1 à V28

- Les valeurs **V1** à **V28** n'ont aucune corrélation entre-elle ce qui découle d'une bonne transformation préalable
- Les variables **Amount** et **Time** on une forte corrélation avec certaines variables

Feature Engineering

- Vérifier que la suppression des variables **Amount** et **Time** sur les différents modèles à analyser
- La **création de variables temporel difficile** car nous n'avons pas d'info sur la **date et l'heure du début** du dataset (**potentiel biais**)





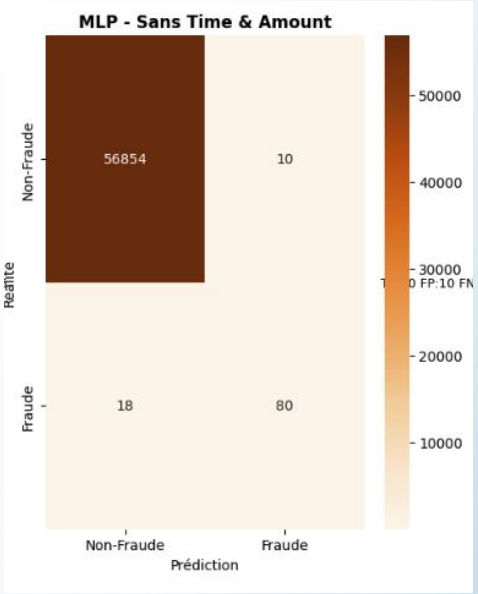
Évaluation préalable

Models

- Régression logistique
- Random Forest
- MLP

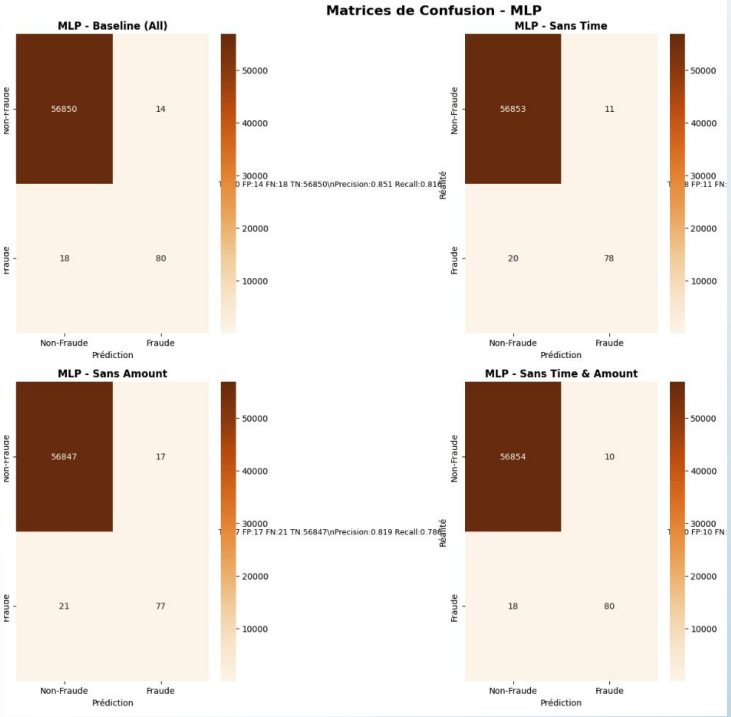
Scoring

- Dataset désiquilibrer, donc grande importance au **Recall (ne pas laisser passer une fraude)**, **Précision (ne pas accuser à tort une transaction normale.)** et **F1 (équilibre entre Recall et Précision)**
- Utilisation de la **matrice de confusion** pour évaluer le compromis entre **faux positifs (FP)** et **faux négatifs (FN)**.



Analyse

- **Meilleurs résultat** sans **Amount** et **Time** dans le cas d'utilisation de MLP (F1 : 0,82)
- **Random forest** est équilibré mais en dessous de **MLP**
- **Régression logistique** à un score **F1** très loins derrière les deux autres models
- Les scores **F1**, **Précision** et **Recal** sont supérieurs avec **MLP**
- L'**utilisation de SDV** sur le dataset génère du **bruit** avec un modèle **GaussianCopula**
    - **CopulaGAN** : résultats corrects mais **temps de traitement long**



Détection de drift

- **Métriques surveillées** : Précision, Recall et F1
- **Déclencheurs** : baisse des performances sous un seuil défini
- **Action** : alerte Grafana → réentraînement via pipeline Airflow
- **Traçabilité** : versioning du modèle (MLflow ou équivalent)

Biais identifiés

- **Dataset très limité** : seulement deux jours de données, ce qui réduit fortement la représentativité.
- **Mauvaise utilisation des techniques d'amplification** : risque lié à l'emploi de méthodes comme SMOTE ou SDV, qui peuvent générer des données artificielles peu fiables.
- **Données déjà traitées en amont** : application préalable de la PCA, ce qui peut entraîner une sur-utilisation ou une redondance de variables déjà exploitées.
- **Données personnelles** : si le dataset contient des informations sensibles, cela pose des enjeux de confidentialité et de conformité réglementaire.

Sécurité

- Dataset déjà **anonymisé** (*PCA*) ; seules les variables **"Amount"** et **"Time"** restent exploitables
- **Datacenter interne** à l'entreprise, couvrant l'intégralité des **demandes en matière de sécurité**
- **Consentement client** déjà en place lors de l'ouverture du compte chez **Fluzz**
- Application du **principe du moindre privilège** pour la gestion des accès et droits utilisateurs
- Conformité **RGPD** :
    - Conservation des données limitée au strict nécessaire (**minimisation des données**)
    - Droit d'accès, de rectification et de suppression garanti aux clients
    - Traçabilité et auditabilité des traitements mis en place

Pipeline API

Step 1
FastAPI

Step 2
Prometheus

Step 3
Grafana

FastAPI – API de vérification

- **Vérification de la transaction entrante** : chaque transaction est analysée par le modèle avant validation.
- **Blocage en cas de fraude** : si une anomalie est détectée, la transaction est automatiquement refusée.

Prometheus & Grafana – Alertes clés

- **Volumétrie des requêtes** : suivi du nombre de requêtes traitées par le système.
- **Temps de traitement du modèle** : détection de latences ou ralentissements anormaux.
  Nombre de fraudes par heure : surveillance en temps réel pour identifier des pics inhabituels.

Pipeline Airflow

Step 1
AIRFLOW

Step 2
Prometheus

Step 3
Grafana

Airflow – Pipeline proposé

1. **Préparation des données d'entrée** : nettoyage, transformation et mise en forme des données brutes.
2. **Entraînement du modèle** : lancement du training selon les configurations définies.
3. **Sauvegarde et versioning** : stockage du modèle entraîné avec gestion des versions.
4. **Mise à jour du lien symbolique** : changement du *symlink* vers la dernière version validée du modèle.

Grafana – Indicateurs de suivi

- **Taux d'échec des tâches** : proportion de jobs qui n'aboutissent pas.
- **Durée des tâches** : temps moyen/maximum d'exécution des jobs.
- **Échecs de validation des données** : par exemple en cas de détection de *drift* ou d'anomalies.

Industrialisation et déploiement

2 pipelines distincts :

- **Airflow** → training, scoring, monitoring (**Prometheus + Grafana**)
- **FastAPI** → service de prédiction temps réel + monitoring (**Prometheus + Grafana**)
- **Conteneurisation Docker** → isolation, portabilité, reproductibilité
- **CI/CD avec GitHub Actions** → build & push des images Docker, déploiement automatisé sur Kubernetes
- **Déploiement interne sur Kubernetes** :
  - **Rolling updates** pour assurer le **zéro downtime**
  - **Scalabilité** (adapter la charge automatiquement)
  - **Haute disponibilité** (réplicas, tolérance aux pannes)

Supervision intégrée avec Prometheus & Grafana pour les deux pipelines

Conclusion & Perspectives

- **Solution complète** : pipeline + monitoring + conformité RGPD
- **Prochain modèle candidat** : **XGBoost**
  a. Très performant sur données déséquilibrées
  b. Robuste, avec un fort potentiel d'optimisation
- **Objectif** : tester XGBoost en production et comparer aux modèles actuels