Master Econométrie et Statistiques

Spécialité Data et Sécurité Informatique

Mémoire de fin d'études présenté pour l'obtention du grade de master.

Comment concevoir, intégrer et évaluer efficacement un système de machine learning au sein d'une institution bancaire pour renforcer la lutte contre le blanchiment d'argent et le financement du terrorisme ?

Présenté par

Victor Parcigneau

Maître de stage : Jean-Philippe Vinzant, Directeur Général Département des Risques

Guidant universitaire : Eddy Caron, professeur à l'ISFA (Université Lyon1) et chercheur au LIP (Laboratoire de Calcul Parallèle) situé à l'École Normale Supérieure de Lyon.

Remerciements :

Je tiens à exprimer ma profonde gratitude envers chacun d'entre vous pour votre dévouement et votre soutien tout au long de mon parcours académique. Votre expertise, vos conseils avisés et votre passion pour l'enseignement ont grandement contribué à façonner ma compréhension des concepts complexes de l'économétrie et des statistiques.

À mon maître de stage, Jean-Philippe Vinzant, je vous adresse mes plus sincères remerciements pour m'avoir accueilli au sein de l'équipe de la banque Delubac. Votre mentorat, votre expertise pratique et votre encouragement constant m'ont permis d'acquérir une expérience précieuse dans la mise en pratique des connaissances acquises au sein de l'université.

À mon tuteur universitaire, Eddy Caron, je suis reconnaissant pour votre orientation éclairée, vos conseils bienveillants. Vous avez su être disponible tout au long de l'élaboration de ce mémoire. Votre expertise a été une source d'inspiration et de motivation pour moi, et j'ai apprécié votre étayage tout au long de ce processus.

Enfin, à mes amis et à mes proches, je souhaite exprimer ma profonde gratitude pour votre soutien indéfectible, vos encouragements constants et votre compréhension tout au long de mon cursus. Votre présence a été une source de réconfort et de motivation (surtout toi Suze).

À vous tous, je suis profondément reconnaissant pour votre contribution à mon parcours académique et professionnel. Vos encouragements, votre soutien et votre expertise ont été essentiels à ma réussite, et je vous en suis infiniment reconnaissant.

J’espère que ma production sera à la hauteur de votre investissement et de vos attentes.

Table des matières

INTRODUCTION :

Dans une ère caractérisée par les avancées technologiques et la numérisation, le secteur financier se trouve à l'avant-garde de l'innovation. Cependant, avec les nombreux avantages apportés par les pratiques bancaires modernes, subsiste une menace persistante - la fraude financière. La prolifération des activités frauduleuses pose non seulement des risques financiers importants aux banques, mais elle mine également l'intégrité du système financier. Parmi les multiples formes de malversations financières, le blanchiment d'argent, ainsi que le financement du terrorisme, demeurent une préoccupation pressante, nécessitant des mesures efficientes de détection et de prévention.

Ce mémoire de Master explore le domaine de l'apprentissage automatique, se concentrant spécifiquement sur son application dans la détection de la fraude bancaire. L'objectif global de cette démarche de recherche est de concevoir et de développer un réseau neuronal capable de discerner les activités frauduleuses dans le domaine bancaire. En exploitant la puissance des méthodologies basées sur les données et des techniques analytiques avancées, le réseau neuronal proposé vise à renforcer l'efficacité des mécanismes de détection de fraude, contribuant ainsi à la lutte contre le blanchiment d'argent et le financement du terrorisme.

Le choix du sujet découle de son importance primordiale dans les opérations bancaires contemporaines. En tant qu'étudiant en économétrie et en statistiques, actuellement inscrit dans un Master et engagé en alternance au sein de la banque Delubac, j'ai pu constater la criticité de la lutte contre la fraude financière. Delubac, comme de nombreuses autres entités financières, est confrontée aux défis complexes posés par les activités frauduleuses, nécessitant des mesures proactives pour sécuriser ses opérations et respecter les normes de conformité réglementaire.

La signification de cette recherche est multiforme et s'étend à diverses dimensions dans le domaine bancaire et financier. Tout d'abord, avec la sophistication croissante des tactiques frauduleuses utilisées par les acteurs malveillants, les approches traditionnelles basées sur des règles pour la détection de la fraude sont devenues de plus en plus inadéquates. L'apprentissage automatique, avec sa capacité à discerner des schémas complexes et des anomalies au sein de vastes ensembles de données, offre une voie prometteuse pour améliorer les capacités de détection de la fraude.

Ensuite, les implications de la fraude bancaire dépassent les simples pertes financières, englobant des préoccupations sociétales plus larges telles que le blanchiment d'argent et le financement du terrorisme. En concevant un réseau neuronal destiné à identifier les transactions suspectes et les activités illicites, cette recherche vise à contribuer à l'objectif plus large de lutte contre la criminalité financière et de préserver l'intégrité du système financier mondial.

De plus, d'un point de vue pratique, la mise en œuvre réussie d'un réseau neuronal pour la détection de la fraude détient des implications profondes pour les institutions bancaires, y compris Delubac. En atténuant efficacement les risques associés à la fraude financière, les banques peuvent renforcer la confiance des clients, améliorer l'efficacité opérationnelle et atténuer les pénalités réglementaires, favorisant ainsi une croissance durable et la résilience dans un paysage de plus en plus concurrentiel.

La problématique choisie pour ce mémoire réside dans la conception, l'intégration et l'évaluation d'un système de machine learning au sein d'une institution bancaire en vue de renforcer la lutte contre le blanchiment d'argent et le financement du terrorisme. Cette approche découle d'une reconnaissance croissante de l'ampleur des défis posés par la criminalité financière et de la nécessité d'adopter des stratégies novatrices pour y faire face.

Traditionnellement, la détection de la fraude bancaire reposait largement sur des règles préétablies et des modèles statistiques simples. Cependant, ces approches se sont avérées de plus en plus inefficaces face à la sophistication croissante des stratagèmes frauduleux et à la diversification des techniques utilisées par les criminels financiers. Par conséquent, l'adoption de méthodes basées sur l'apprentissage automatique offre une alternative prometteuse, permettant de détecter les schémas frauduleux complexes et en constante évolution qui échappent souvent aux méthodes traditionnelles.

L'intégration de techniques d'apprentissage automatique, notamment les réseaux neuronaux, les arbres de décision, et les méthodes d'ensemble, au sein d'une institution bancaire permet de développer un système de détection de la fraude à la fois plus flexible et réactif. Ces systèmes peuvent analyser de grandes quantités de données en temps réel, identifier des anomalies subtiles et détecter les tendances émergentes, offrant ainsi une protection accrue contre les activités frauduleuses.

De plus, cette approche présente l'avantage de s'adapter dynamiquement aux changements dans le paysage de la criminalité financière, en permettant une mise à jour continue des modèles de détection en fonction des nouvelles menaces et des tendances observées. En outre, en tirant parti de l'expertise et des données disponibles au sein de l'institution bancaire, ces systèmes peuvent être spécifiquement calibrés pour répondre aux besoins et aux caractéristiques uniques de l'organisation, maximisant ainsi leur efficacité et leur pertinence.

L'objectif principal de cette recherche est de conceptualiser, de développer et d'évaluer un modèle basé sur un réseau neuronal pour la détection de la fraude bancaire. Pour atteindre cet objectif global, les objectifs spécifiques suivants sont définis :

- Acquérir un ensemble de données complet comprenant des transactions bancaires historiques, englobant à la fois des cas légitimes et frauduleux. Prétraiter les données pour garantir la cohérence, l'exactitude et l'adéquation à des fins d'entraînement du modèle.

- Identifier et extraire des caractéristiques pertinentes de l'ensemble de données présentant un pouvoir discriminatoire dans la distinction entre les transactions légitimes et frauduleuses. Explorer des techniques telles que la réduction de dimensionnalité et la sélection de caractéristiques pour améliorer l'efficacité du modèle.

- Concevoir et mettre en œuvre une architecture de réseau neuronal adaptée aux subtilités de la détection de la fraude bancaire. Expérimenter avec diverses architectures de réseaux neuronaux, y compris les cadres d'apprentissage en profondeur tels que les réseaux neuronaux convolutifs et les réseaux neuronaux récurrents, pour déterminer la configuration optimale du modèle.

- Entraîner le modèle de réseau neuronal développé à l'aide de l'ensemble de données prétraité et évaluer sa performance en termes de métriques clés telles que l'exactitude, la précision, le rappel et le score F1. Utiliser des techniques de validation croisée pour garantir la robustesse du modèle.

- Intégrer le modèle de réseau neuronal entraîné dans l'infrastructure existante de détection de fraude de Delubac, facilitant l'intégration transparente avec les flux de travail opérationnels. Développer des mécanismes de surveillance en temps réel et de génération d'alertes pour permettre une intervention rapide en cas d'activités suspectes.

- Valider l'efficacité du modèle déployé à travers des études de cas du monde réel et une validation contre des instances frauduleuses connues, en mettant en lumière son utilité pratique et ses limites.

En poursuivant ces objectifs, cette recherche s'efforce de faire avancer la frontière de la détection de la fraude dans le secteur bancaire et de fournir aux institutions bancaires un outil puissant pour protéger leurs actifs et préserver l'intégrité financière.

Ce mémoire de Master est structuré de la manière suivante, reflétant la progression séquentielle des activités de recherche entreprises pour atteindre les objectifs énoncés. Les chapitres suivants du mémoire sont organisés comme suit :

Chapitre 1 : Revue de la Littérature : État des lieux complet de la littérature et de la recherche concernant la détection de la fraude dans la banque, avec un accent particulier sur les méthodologies d'apprentissage automatique et les réseaux neuronaux.

Chapitre 2 : Dispositifs LCBFT (Lutte contre le blanchiment d'argent et le financement du terrorisme) en place chez Delubac : Vérification des clients (KYC), surveillance des transactions, systèmes d'alerte et de signalement, audits et formations internes. Comparaison avec les approches traditionnelles et intégration des technologies de machine learning pour améliorer la détection des fraudes.

Chapitre 3 : Acquisition et Prétraitement des Données : Présentation des processus de collecte de données, de prétraitement et d'ingénierie des caractéristiques, posant les bases du développement du modèle.

Chapitre 4 : Architecture et Implémentation du Modèle : Présentation de la conception, l'implémentation et l'entraînement du modèle de réseau neuronal pour la détection de la fraude bancaire, en élucidant la justification derrière les choix architecturaux et l'ajustement des hyperparamètres.

Chapitre 5 : Évaluation Expérimentale : Évaluation approfondie du modèle de réseau neuronal développé, analysant sa performance selon diverses métriques d'évaluation et le benchmarking contre les mécanismes de détection de fraude existants.

Chapitre 6 : Intégration et Déploiement : Exploration de l'intégration du modèle développé dans l'infrastructure de détection de fraude existante de Delubac, en élucidant les considérations pratiques et les implications de celle-ci.

In fine nous résumerons les principales conclusions de la recherche, délimiterons les avenues pour le développement futur, et offrirons des remarques conclusives sur l'importance des contributions de la recherche.

En respectant cette structure organisée, ce mémoire de Master s'efforce d'offrir une exploration complète et perspicace de l'application des techniques d'apprentissage automatique, en particulier des réseaux neuronaux, dans le domaine de la détection de la fraude bancaire. À travers une validation empirique et une mise en œuvre pratique, la recherche vise à combler l'écart entre les avancées théoriques et les exigences pratiques, favorisant ainsi l'innovation et la résilience dans la lutte contre la fraude financière.

CHAPITRE 1 : Revue de la littérature

Dans le contexte financier contemporain, la détection et la prévention de la fraude représentent des défis cruciaux pour les institutions bancaires. Face à l'évolution constante des stratégies frauduleuses et à la complexité croissante des transactions financières, les méthodes traditionnelles de lutte contre la fraude se révèlent souvent inefficaces. Toutefois, l'émergence de l'apprentissage automatique ouvre de nouvelles perspectives pour la détection de la fraude, en rendant possible l'analyse de vastes ensembles de données afin d'identifier des schémas et anomalies révélateurs d'activités frauduleuses.

L'apprentissage automatique, ou « machine learning » en anglais, est un domaine de l'intelligence artificielle qui se concentre sur le développement de techniques permettant aux ordinateurs d'apprendre à partir de données et de réaliser des tâches spécifiques sans être explicitement programmés pour les accomplir. Contrairement à la programmation traditionnelle où les instructions sont codées explicitement par un développeur, l'apprentissage automatique permet à un système de s'améliorer progressivement en s'adaptant à des données nouvelles et changeantes. Cette capacité à généraliser à partir de données et à détecter des modèles subtils en fait un outil précieux dans divers domaines, y compris la finance, où la détection de la fraude est d'une importance capitale.

Au sein de l'apprentissage automatique, les réseaux neuronaux constituent une classe de modèles inspirés par le fonctionnement du cerveau humain. Ces modèles, également appelés réseaux de neurones artificiels, sont composés de couches de neurones interconnectés, chaque neurone étant une unité de calcul élémentaire.

À travers des opérations mathématiques sophistiquées, les réseaux neuronaux sont capables d'apprendre des relations complexes entre les données en ajustant les poids des connexions entre les neurones lors du processus d'entraînement. Cette capacité à apprendre des représentations hiérarchiques et abstraites à partir des données en fait un choix privilégié pour des tâches telles que la reconnaissance d'images, le traitement du langage naturel et bien sûr, la détection de la fraude bancaire.

La détection de la fraude dans le domaine financier représente un défi majeur pour les institutions bancaires et les entreprises. Avec l'évolution constante des transactions financières et l'expansion des plateformes numériques, les criminels ont également adapté et sophistiqué leurs méthodes de fraude. Dans ce contexte, l'apprentissage automatique émerge comme un outil puissant pour lutter contre la fraude, offrant des capacités analytiques avancées pour identifier les schémas frauduleux et protéger les actifs financiers.

La revue systématique de la littérature menée par Abdulalem Ali et ses collègues, intitulée "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review", offre une vue d'ensemble détaillée des recherches récentes dans ce domaine crucial. Cette revue met en lumière l'ampleur de la fraude financière, les défis posés par sa détection et l'importance croissante de l'application de méthodes d'apprentissage automatique pour relever ces défis.

Ali et ses collaborateurs commencent par contextualiser l'importance de la détection de la fraude financière dans le paysage actuel des transactions numériques et des activités financières en ligne. Ils soulignent l'impact financier et réputationnel considérable des fraudes, ainsi que les implications légales et réglementaires qui en découlent. Face à cette réalité, les institutions financières sont confrontées à une pression croissante pour renforcer leurs systèmes de détection de la fraude et prévenir les pertes financières et les dommages à la réputation. C’est dans ce contexte qu’ils ont observé une forte augmentation des publications liées à ce sujet, notamment à partir de 2013.

Dans cette période, l'apprentissage automatique émerge comme une solution prometteuse pour améliorer la détection de la fraude financière. Ali et ses collègues explorent un large éventail de techniques d'apprentissage automatique, allant des réseaux neuronaux profonds aux méthodes d'ensemble et aux arbres de décision.

Ils mettent en évidence les avantages de ces approches, notamment leur capacité à détecter des schémas complexes et non linéaires, leur adaptabilité aux données hétérogènes et leur capacité à s'adapter aux évolutions du paysage criminel.

Voici un résumé des conclusions spécifiques concernant chaque méthode :

- Support Vector Machine (SVM) : Les SVM sont des algorithmes d'apprentissage supervisé utilisés pour la classification et la régression. Ils cherchent à trouver l'hyperplan qui maximise la marge entre les classes dans un espace de dimension supérieure, permettant ainsi de séparer efficacement les données. Les SVM se sont avérées être une méthode efficace pour la détection de la fraude, offrant une bonne capacité à séparer les données dans des espaces multidimensionnels. Elles sont particulièrement adaptées aux problèmes de classification avec des données non linéaires et ont démontré des performances solides dans diverses applications de détection de la fraude.

- Fuzzy-Logic-Based Method : Les méthodes basées sur la logique floue permettent de modéliser l'incertitude et la vague dans les données en attribuant des degrés d'appartenance flous aux classes ou aux décisions, permettant ainsi une prise de décision plus flexible et plus tolérante aux erreurs. Les méthodes basées sur la logique floue ont montré leur utilité dans la détection de la fraude en permettant une modélisation plus flexible des données et des décisions incertaines. Elles sont capables de gérer des informations imprécises et ambiguës, ce qui en fait des outils prometteurs pour la détection de la fraude dans des environnements complexes et changeants.

- Hidden Markov Model (HMM) : Les HMM sont des modèles statistiques utilisés pour modéliser des séquences de données, où les états sont cachés et ne peuvent pas être directement observés. Ils sont utilisés pour capturer les dépendances temporelles entre les événements et peuvent être appliqués à la détection de la fraude en modélisant les comportements suspects. Les modèles de Markov cachés se sont révélés efficaces pour modéliser des séquences de données temporelles, ce qui en fait des outils pertinents pour la détection de la fraude dans des processus dynamiques tels que les transactions financières. Ils peuvent capturer les dépendances temporelles entre les événements et détecter les anomalies dans les séquences de données.

- Artificial Neural Network (ANN) : Les réseaux neuronaux artificiels sont des modèles inspirés du cerveau humain, composés de couches de neurones interconnectés. Ils apprennent à partir des données en ajustant les poids des connexions entre les neurones, leur permettant de capturer des relations complexes entre les variables. Les réseaux neuronaux artificiels ont été largement utilisés avec succès dans la détection de la fraude, offrant une capacité à apprendre des représentations complexes à partir des données. Ils sont particulièrement adaptés à la détection de schémas non linéaires et à la modélisation de relations complexes entre les variables, ce qui en fait des outils puissants pour la détection de la fraude.

- KNN Algorithm : L'algorithme des k plus proches voisins attribue une classe à une observation en se basant sur la classe majoritaire parmi ses k voisins les plus proches dans l'espace des caractéristiques. Il est simple et efficace, mais peut être sensible à la dimensionnalité et au choix de la distance. L'algorithme des k plus proches voisins est une méthode simple mais efficace pour la détection de la fraude, en particulier dans les cas où les frontières de décision sont complexes et non linéaires. Il peut être utilisé pour classer les transactions en fonction de leur similarité avec des transactions frauduleuses connues, offrant ainsi une approche intuitive et facile à interpréter.

- Bayesian Method : Les méthodes bayésiennes utilisent le théorème de Bayes pour estimer la probabilité a posteriori d'une classe étant donné les données observées. Elles peuvent intégrer des informations a priori pour améliorer les estimations, offrant ainsi une approche robuste pour la détection de la fraude. Les méthodes bayésiennes offrent un cadre probabiliste pour la détection de la fraude, permettant de prendre en compte à la fois les informations a priori et les données observées pour estimer la probabilité de fraude. Elles sont particulièrement adaptées aux cas où les données sont limitées ou lorsque des informations contextuelles sont disponibles.

- Decision Tree : Les arbres de décision sont des modèles qui partitionnent l'espace des caractéristiques en fonction de règles de décision hiérarchiques, permettant ainsi de diviser les données en sous-groupes homogènes. Ils sont simples à interpréter et peuvent capturer des relations non linéaires entre les variables. Les arbres de décision sont des outils populaires pour la détection de la fraude en raison de leur simplicité et de leur capacité à générer des règles de décision facilement interprétables. Ils peuvent capturer des relations non linéaires entre les variables et sont efficaces pour gérer des ensembles de données hétérogènes.

- Genetic Algorithm : Les algorithmes génétiques utilisent des techniques d'optimisation inspirées de l'évolution biologique pour rechercher des solutions optimales à un problème donné. Ils utilisent des opérateurs génétiques tels que la sélection, le croisement et la mutation pour générer de nouvelles solutions et améliorer progressivement les performances. Les algorithmes génétiques offrent une approche novatrice pour la détection de la fraude en utilisant des techniques d'optimisation inspirées de l'évolution biologique. Ils peuvent être utilisés pour rechercher des ensembles de variables ou des paramètres de modèle optimaux, offrant ainsi une approche flexible et adaptable à divers problèmes de détection de la fraude.

- Ensemble Methods : Les méthodes d'ensemble combinent les prédictions de plusieurs modèles de détection de la fraude pour améliorer les performances globales. Elles peuvent réduire le biais et la variance des modèles individuels, offrant ainsi une meilleure généralisation et une meilleure résistance aux données bruitées ou incorrectes. Elles peuvent réduire le biais et la variance des modèles individuels, offrant ainsi une meilleure généralisation et une meilleure résistance aux données bruitées ou incorrectes.

- Clustering Based Methods : Les méthodes de regroupement identifient des groupes ou des clusters de données similaires, permettant ainsi de détecter des schémas anormaux ou des comportements frauduleux. Elles sont utiles pour l'analyse exploratoire des données et peuvent être utilisées pour identifier des groupes suspects. Les méthodes de regroupement offrent une approche alternative pour la détection de la fraude en identifiant des groupes ou des clusters de transactions similaires. Elles peuvent être utilisées pour détecter des schémas anormaux ou des comportements frauduleux à partir de données non étiquetées, offrant ainsi une approche exploratoire et non supervisée de la détection de la fraude.

- Logistic Regression : La régression logistique est une méthode de régression utilisée pour la classification binaire. Elle modélise la probabilité que la variable dépendante prenne une certaine classe en fonction des variables indépendantes, en utilisant une fonction logistique pour estimer les probabilités. La régression logistique est une méthode classique mais efficace pour la détection de la fraude, offrant une capacité à modéliser des relations linéaires entre les variables et à estimer les probabilités de fraude. Elle est particulièrement adaptée aux problèmes de classification binaire et peut être facilement interprétée.

Dans le cadre de la lutte contre le blanchiment d'argent et le financement du terrorisme, les institutions financières sont tenues de mettre en place des mesures rigoureuses et systématiques pour détecter, prévenir et signaler les activités suspectes. La banque Delubac, au sein de laquelle je réalise mon alternance, ne fait pas exception à cette règle et a déjà mis en œuvre un ensemble de pratiques et de procédures destinées à combattre ces menaces.

La mise en place de ces mesures est cruciale non seulement pour se conformer aux exigences réglementaires, mais aussi pour protéger l'intégrité du système financier global. Dans ce chapitre, nous allons examiner en détail les stratégies et les outils actuellement utilisés par la banque Delubac pour détecter et prévenir les activités frauduleuses et illicites.

Nous allons aborder plusieurs aspects clés, notamment :

- Les processus de vérification des clients (KYC - Know Your Customer) : Les procédures d'identification et de vérification des clients jouent un rôle central dans la prévention du blanchiment d'argent. Nous verrons comment la banque utilise ces procédures pour s'assurer de l'identité de ses clients et de la légitimité de leurs transactions.
- La surveillance des transactions : Une surveillance continue des transactions est essentielle pour détecter les activités suspectes. Nous décrirons les systèmes de surveillance transactionnelle en place et la manière dont ils sont utilisés pour identifier les comportements atypiques qui pourraient indiquer une activité de blanchiment d'argnt ou de financement du terrorisme.
- Les systèmes d'alerte et de signalement : Lorsqu'une transaction suspecte est détectée, il est crucial d'avoir des systèmes d'alerte efficaces pour notifier les autorités compétentes. Nous discuterons des procédures de signalement actuelles et des collaborations avec les organismes de régulation.
- Les audits et les formations internes : La conformité aux réglementations anti-blanchiment et anti-financement du terrorisme exige des efforts continus en termes de formation du personnel et d'audits internes réguliers. Nous explorerons les initiatives de la banque Delubac en matière de formation et d'évaluation pour garantir que les employés sont bien informés et préparés à gérer les risques associés.

En introduisant ces pratiques actuelles, nous pourrons mieux situer l'importance et la pertinence de notre projet de développement d'un réseau neuronal pour la détection des fraudes bancaires. En effet, l'intégration de technologies avancées de machine learning, comme les réseaux de neurones artificiels, vient en complément des méthodes existantes et vise à renforcer l'efficacité de la lutte contre le blanchiment d'argent et le financement du terrorisme.

Ainsi, ce chapitre servira de transition entre les méthodes traditionnelles de lutte contre le blanchiment et le financement du terrorisme (LCBFT) et l'application des technologies de machine learning dans ce domaine.

CHAPITRE 2 : Dispositifs de LCBFT en place chez Delubac

Dans le cadre de la Lutte Contre le Blanchiment d'argent et le Financement du Terrorisme, les institutions financières doivent impérativement instaurer des mesures strictes et systématiques pour détecter, prévenir et signaler toute activité suspecte. La banque Delubac respecte cette obligation en ayant déjà mis en place un ensemble de pratiques et de procédures visant à contrer ces menaces.

La mise en place de ces mesures est cruciale non seulement pour se conformer aux exigences réglementaires, mais aussi pour protéger l'intégrité du système financier global. Dans ce chapitre, nous allons examiner en détail les stratégies et les outils actuellement utilisés par la banque Delubac pour détecter et prévenir les activités frauduleuses et illicites.

2.1 Les processus de vérification des clients (KYC - Know Your Customer)

Les procédures d'identification et de vérification des clients jouent un rôle central dans la prévention du blanchiment d'argent. La banque utilise des procédures de KYC rigoureuses pour s'assurer de l'identité de ses clients et de la légitimité de leurs transactions.

2.1.1 Identification des clients

La première étape du processus KYC consiste à recueillir des informations complètes et précises sur les clients. Cela inclut la collecte de documents d'identité tels que des passeports, des cartes d'identité ou des permis de conduire, ainsi que des preuves de résidence comme des factures de services publics. La banque utilise des technologies avancées pour numériser et vérifier ces documents afin de s'assurer de leur authenticité.

2.1.2 Analyse des risques

Une fois les informations de base collectées, la banque procède à une analyse des risques pour chaque client. Cette analyse comprend l'évaluation de l'historique financier du client, de ses transactions antérieures et de tout lien potentiel avec des activités illicites. La banque utilise des bases de données de sanction et des listes de surveillance pour vérifier les antécédents des clients et détecter tout risque potentiel.

2.1.3 Surveillance continue

Le processus KYC ne s'arrête pas à l'ouverture du compte. La banque Delubac met en place une surveillance continue des clients pour détecter tout changement dans leur profil de risque. Cela prend en compte la mise à jour régulière des informations client et la réévaluation des risques associés à leurs activités.

2.2 La surveillance des transactions

Une surveillance continue des transactions est essentielle pour détecter les activités suspectes. La banque Delubac utilise des systèmes de surveillance transactionnelle sophistiqués pour identifier les comportements atypiques qui pourraient indiquer une activité de blanchiment d'argent ou de financement du terrorisme.

2.2.1 Systèmes de surveillance transactionnelle

La banque Delubac dispose de systèmes automatisés qui surveillent en temps réel toutes les transactions effectuées par ses clients. Ces systèmes utilisent des algorithmes avancés pour analyser les données transactionnelles et détecter les anomalies. Par exemple, des transactions fréquentes et de faible montant peuvent indiquer une tentative de structuration, tandis que des transactions importantes vers des pays à haut risque peuvent signaler un financement terroriste potentiel.

2.2.2 Détection des comportements atypiques

Les systèmes de surveillance transactionnelle sont conçus pour détecter une variété de comportements atypiques. Cela inclut des transactions inhabituelles par rapport à l'historique du client, des transferts fréquents vers des comptes récemment ouverts ou des activités incohérentes avec le profil déclaré du client. Lorsque de telles anomalies sont détectées, une alerte est générée pour une enquête plus approfondie.

2.3 Les systèmes d'alerte et de signalement

Lorsqu'une transaction suspecte est détectée, il est crucial d'avoir des systèmes d'alerte efficaces pour notifier les autorités compétentes. La banque Delubac a mis en place des procédures de signalement robustes pour garantir que les activités suspectes sont signalées de manière appropriée.

2.3.1 Génération d'alertes

Les systèmes de surveillance de la banque génèrent des alertes en cas de détection d'activités suspectes. Ces alertes sont ensuite examinées par une équipe dédiée à la conformité, qui évalue la pertinence des soupçons et décide des actions à entreprendre. Cette équipe utilise des critères stricts pour déterminer si une transaction doit être signalée aux autorités compétentes.

2.3.2 Signalement aux autorités

Lorsque des transactions suspectes sont confirmées, la banque Delubac procède à leur signalement auprès des autorités réglementaires. Ce processus prend en compte la rédaction de rapports détaillés sur les transactions en question, les clients impliqués et les raisons de la suspicion. La banque collabore étroitement avec les organismes de régulation pour s'assurer que toutes les exigences de conformité sont respectées.

2.4 Les audits et les formations internes

La conformité aux réglementations anti-blanchiment et anti-financement du terrorisme exige des efforts continus en termes de formation du personnel et d'audits internes réguliers. La banque Delubac investit de manière significative dans la formation de ses employés et la réalisation d'audits pour garantir l'efficacité de ses mesures de lutte contre la fraude.

2.4.1 Formation du personnel

Tous les employés de la banque, en particulier ceux impliqués dans les opérations de conformité, reçoivent une formation approfondie sur les réglementations anti-blanchiment et les techniques de détection des fraudes. Cette formation est régulièrement mise à jour pour inclure les dernières tendances et techniques utilisées par les criminels financiers. Les employés sont également formés à l'utilisation des systèmes de surveillance et à la procédure de signalement des transactions suspectes.

2.4.2 Audits internes

La banque Delubac réalise des audits internes réguliers pour évaluer l'efficacité de ses procédures de conformité. Ces audits incluent des examens détaillés des processus KYC, de la surveillance des transactions et des systèmes d'alerte. Les résultats des audits sont utilisés pour identifier les domaines nécessitant des améliorations et pour renforcer les mesures de lutte contre la fraude.

2.5 Intégration des technologies de machine learning

En introduisant ces pratiques actuelles, nous pouvons mieux situer l'importance et la pertinence de notre projet de développement d'un réseau neuronal pour la détection des fraudes bancaires. L'intégration de technologies avancées de machine learning, comme les réseaux de neurones artificiels, vient en complément des méthodes existantes et vise à renforcer l'efficacité de la lutte contre le blanchiment d'argent et le financement du terrorisme.

L'utilisation de réseaux de neurones artificiels permet d'analyser de grandes quantités de données transactionnelles et de détecter des schémas de fraude complexes qui pourraient échapper aux systèmes traditionnels. Ces technologies offrent également une capacité d'apprentissage continu, permettant au modèle de s'adapter aux nouvelles tactiques de fraude.

En conclusion, la banque Delubac a mis en place un ensemble complet de mesures pour lutter contre le blanchiment d'argent et le financement du terrorisme. Ces mesures incluent des procédures rigoureuses de vérification des clients, une surveillance continue des transactions, des systèmes d'alerte efficaces et des initiatives de formation et d'audit interne. L'intégration de technologies de machine learning, comme les réseaux de neurones artificiels, représente une avancée supplémentaire pour renforcer ces efforts et améliorer la détection des fraudes bancaires.

Afin de mettre en place ces outils, je voulais me baser sur les données transactionnelles des clients de la banque et entraîner mon IA dessus. Malheureusement, celles-ci étaient trop confidentielles et je n’ai pas pu y accéder. Afin de pallier à cela, j’ai dû utiliser des données en open source provenant de Kaggle, en l'occurrence ici « Credit Card Transactions Fraud Detection Dataset ». En utilisant ces données alternatives, nous pouvons néanmoins explorer et développer des modèles efficaces de détection de fraude.

CHAPITRE 3 : Acquisition et Prétraitement des Données

Ce chapitre se concentre sur les étapes cruciales de l'acquisition, du prétraitement et de la présentation des données utilisées pour développer notre modèle de détection de fraude. Les données que nous utilisons proviennent du dataset open source « Credit Card Transactions Fraud Detection Dataset » disponible sur Kaggle.

3.1 Acquisition des Données

Le dataset comprend des transactions par carte de crédit, avec une étiquette indiquant si chaque transaction est frauduleuse ou non. Chaque ligne du dataset représente une transaction individuelle avec des informations détaillées sur la transaction, le client et le commerçant.

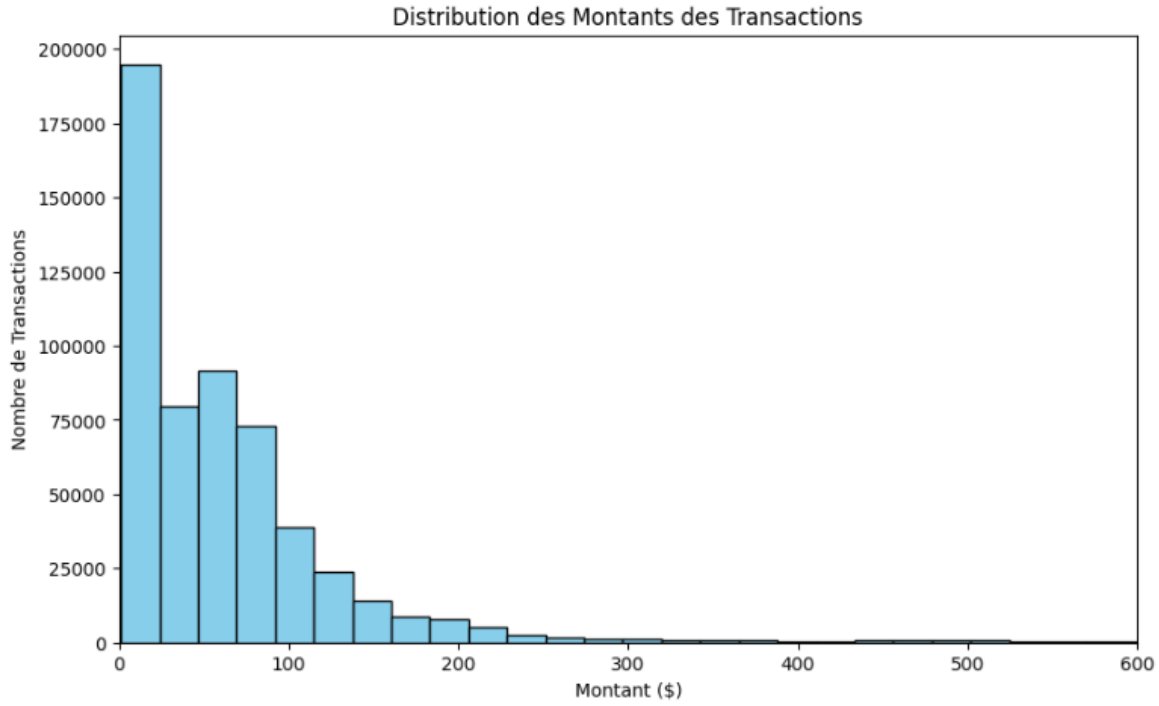
3.2 Description des Données

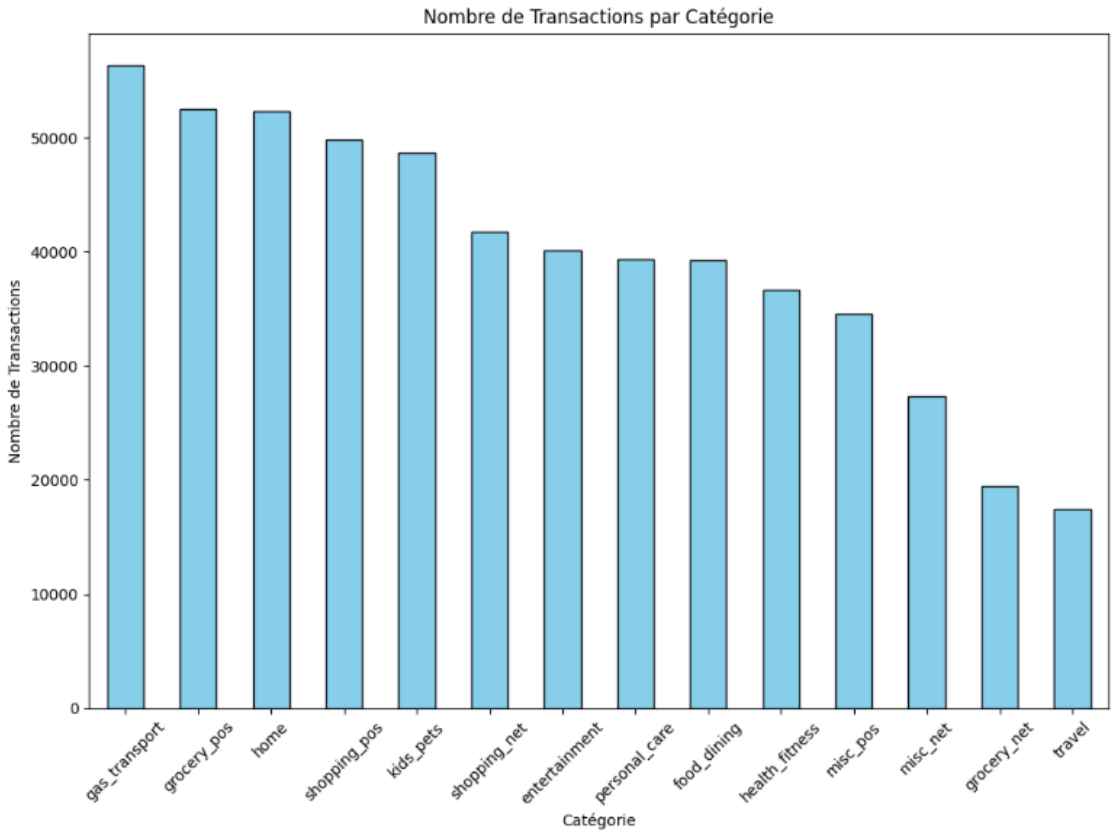
Voici un aperçu des colonnes présentes dans le dataset :

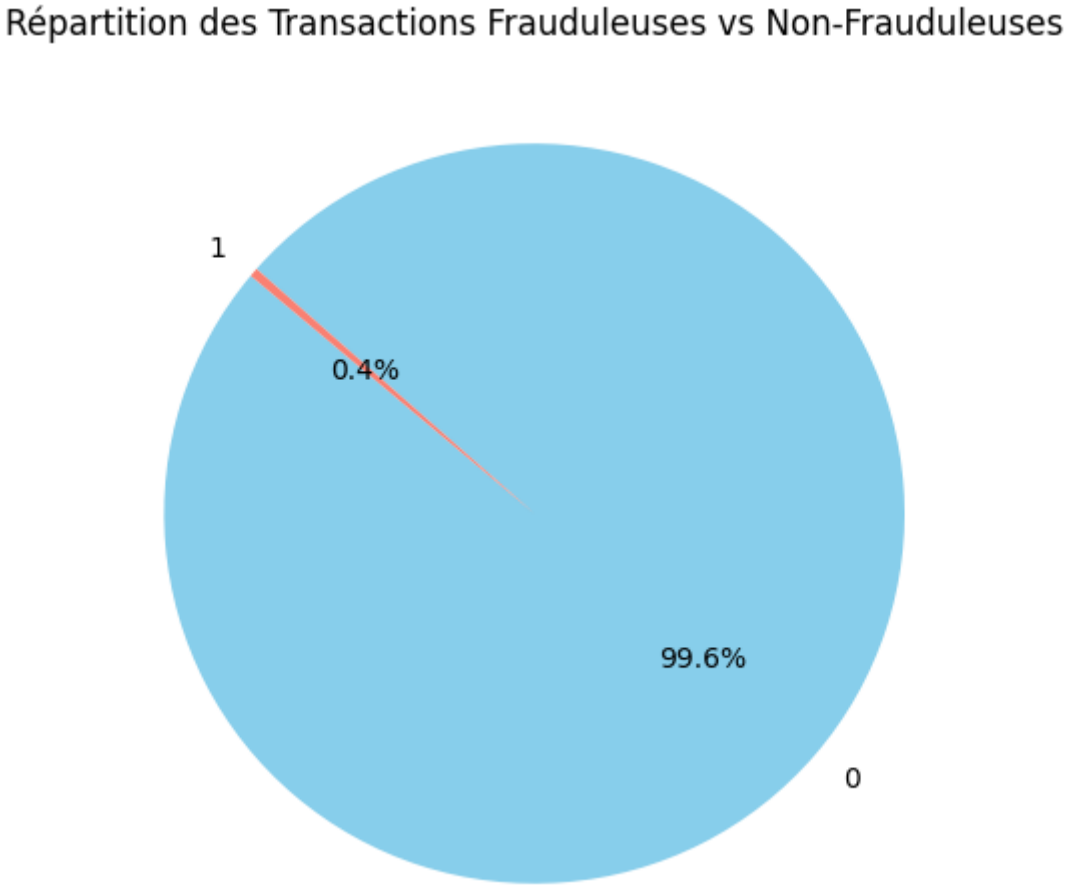
- **trans_date_trans_time** : Date et heure de la transaction.
- **cc_num** : Numéro de la carte de crédit.
- **merchant** : Nom du commerçant.
- **category** : Catégorie du commerçant.
- **amt** : Montant de la transaction.
- **first** : Prénom du client.
- **last** : Nom de famille du client.
- **gender** : Sexe du client.
- **street** : Adresse du client.
- **city** : Ville du client.
- **state** : État du client.
- **zip** : Code postal du client.
- **lat** : Latitude de la résidence du client.

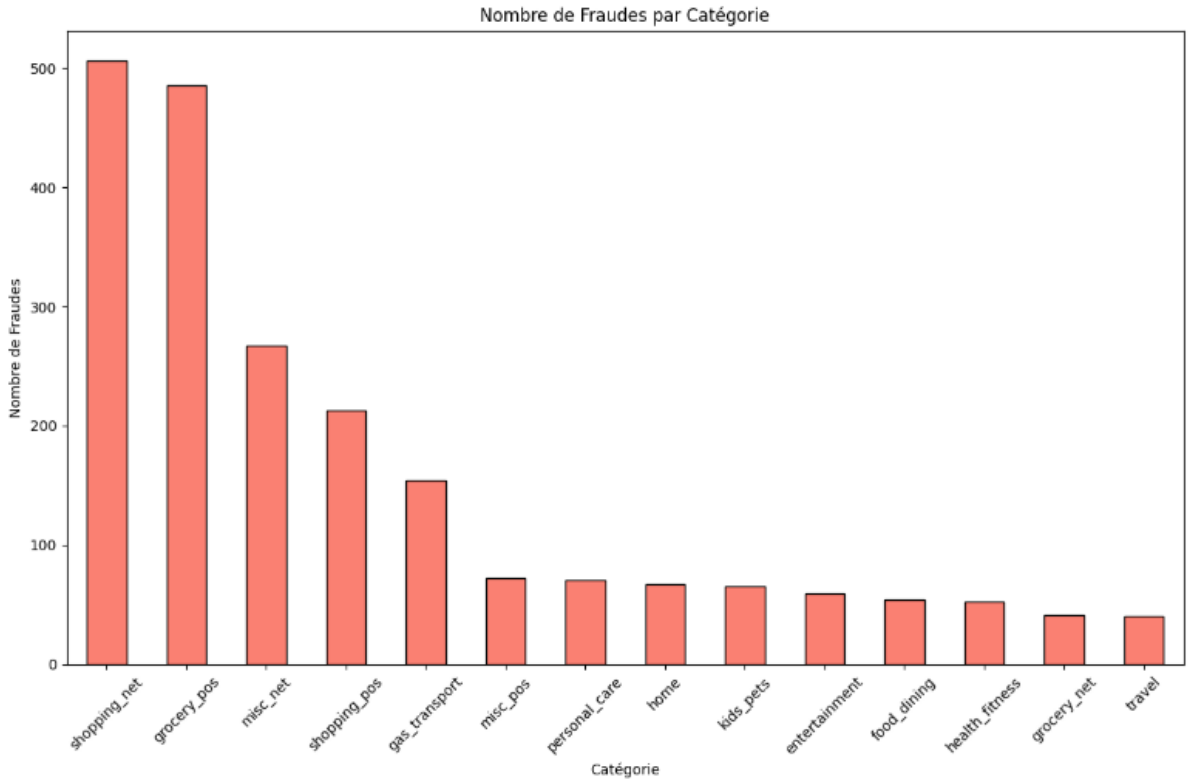
- **long** : Longitude de la résidence du client.
- **city_pop** : Population de la ville du client.
- **job** : Profession du client.
- **dob** : Date de naissance du client.
- **trans_num** : Identifiant unique de la transaction.
- **unix_time** : Temps de la transaction en format UNIX.
- **merch_lat** : Latitude du commerçant.
- **merch_long** : Longitude du commerçant.
- **is_fraud** : Indicateur de fraude (0 pour non-frauduleux, 1 pour frauduleux).

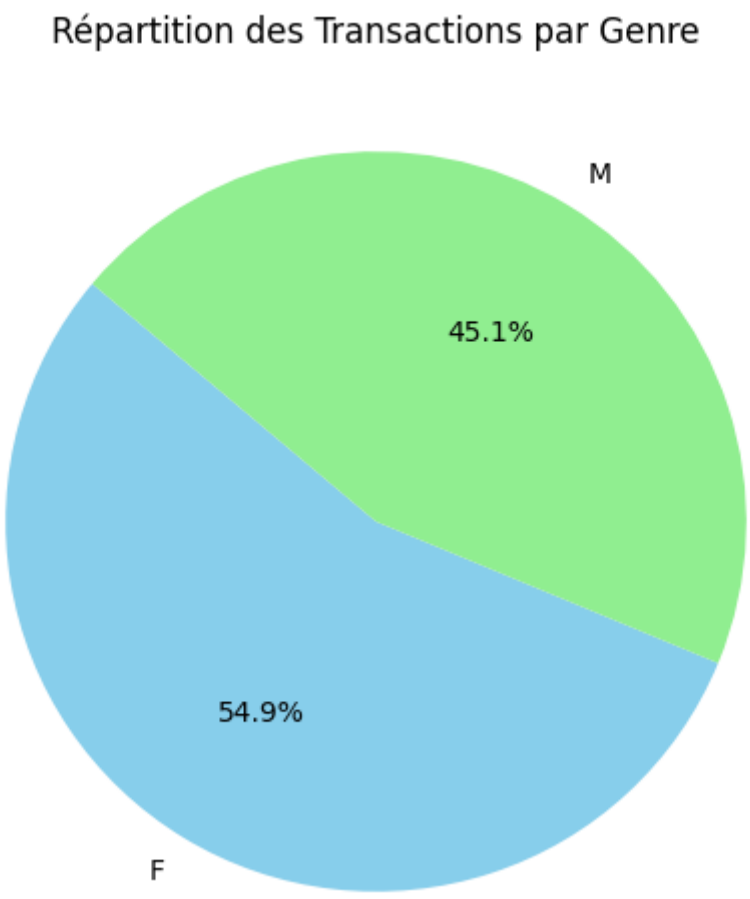
Les données sont réparties comme suit :




Nombre de Transactions par Catégorie
Nombre de Transactions
0
10000
20000
30000
40000
50000
gas_transport
grocery_pos
home
shopping_pos
kids_pets
shopping_net
entertainment
personal_care
food_dining
health_fitness
misc_pos
misc_net
grocery_net
travel
Catégorie


Répartition des Transactions Frauduleuses vs Non-Frauduleuses
1
0.4%
99.6%
0


Nombre de Fraudes par Catégorie
Nombre de Fraudes
0
100
200
300
400
500
shopping_net
grocery_pos
misc_net
shopping_pos
gas_transport
misc_pos
personal_care
home
kids_pets
entertainment
food_dining
health_fitness
grocery_net
travel
Catégorie

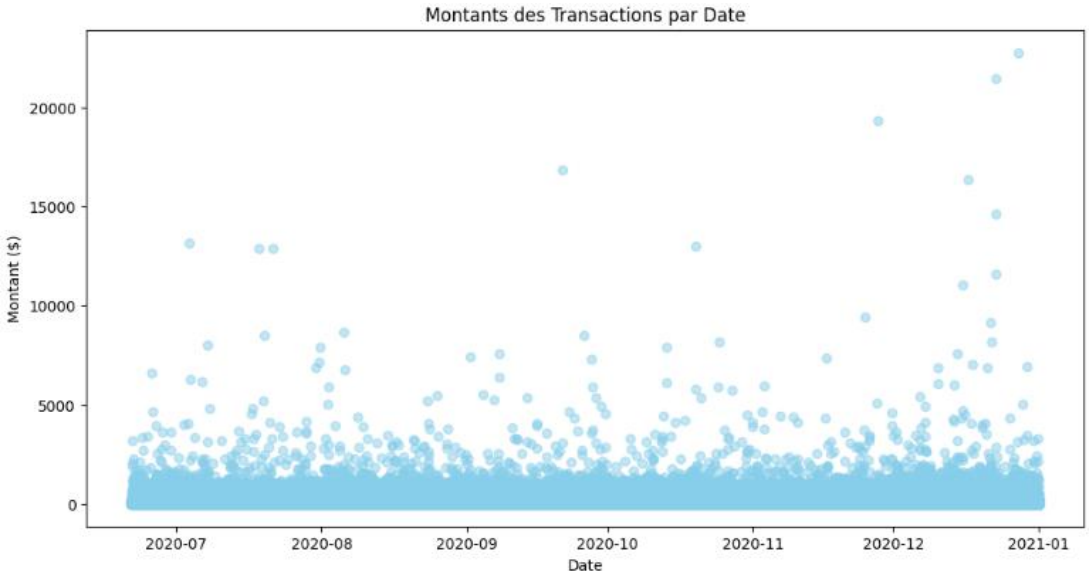

Répartition des Transactions par Genre
M
45.1%
54.9%
F

Nous observons que la majorité des transactions sont inférieures à 200 $. Les principales catégories de dépenses sont les transports, la nourriture et le logement. Seulement 0,4 % des transactions sont frauduleuses, avec une concentration notable dans les achats de vêtements en ligne, les courses alimentaires et les dépenses diverses sur Internet. La répartition par genre est de 55 % de femmes et 45 % d'hommes, avec une tranche d'âge allant de 20 à 100 ans et une distribution d'âge presque gaussienne, la moyenne étant d'environ 50 ans. Ces caractéristiques semblent refléter fidèlement la réalité.

3.3 Prétraitement des Données

Le prétraitement des données est une étape essentielle pour garantir la qualité et la fiabilité des modèles prédictifs. Les étapes suivantes ont été suivies :

- **Nettoyage des Données** : Suppression des doublons et correction des incohérences.
- **Gestion des Valeurs Manquantes** : Imputation ou suppression des valeurs manquantes en fonction de leur proportion et de leur impact potentiel sur le modèle.
- **Transformation des Variables** : Conversion des variables catégorielles en variables numériques à l'aide de techniques comme l'encodage one-hot.



Les transactions sont réparties de manière uniforme entre juin 2020 et janvier 2021. On observe toutefois une nette augmentation en décembre, probablement en raison des achats de Noël.

3.4 Analyse Exploratoire des Données (EDA)

Une analyse exploratoire des données a été réalisée pour identifier les tendances et les relations dans les données. Les principales étapes de l'EDA comprennent :

- **Visualisation des Données** : Utilisation de graphiques tels que les histogrammes, les boxplots et les heatmaps pour visualiser la distribution des variables et les corrélations entre elles.
- **Statistiques Descriptives** : Calcul des mesures statistiques telles que les moyennes, les médianes et les écarts-types pour résumer les caractéristiques des données. Vous pouvez retrouvez tout cela dans le code python en annexe.

Cette analyse permet de détecter les relations entre les variables numériques, offrant des insights sur les facteurs qui pourraient influencer les montants des transactions ou leur nature (frauduleuses ou non). Les résultats montrent comment les différentes caractéristiques des transactions, telles que les montants et les catégories, sont interconnectées et fournissent des indications utiles pour l'élaboration de modèles prédictifs et la détection de comportements anormaux.

La heatmap des corrélations montre les coefficients de corrélation entre différentes variables du jeu de données de fraudes bancaires, révélant des insights importants. Les latitudes et longitudes (lat, long, merch_lat, merch_long) montrent des corrélations très fortes entre elles. Par exemple, lat et merch_lat ont une corrélation positive de 0.99, indiquant qu'ils représentent des coordonnées géographiques similaires ou liées. De même, long et merch_long ont une corrélation positive parfaite de 1. En revanche, zip et long présentent une forte corrélation négative (-0.91), suggérant une relation inverse entre le code postal et la longitude dans cette base de données.

En ce qui concerne la variable is_fraud, elle montre une corrélation positive modérée avec amt (0.18). Cela suggère que des montants plus élevés sont plus souvent associés à des transactions frauduleuses. Cependant, les autres corrélations avec is_fraud sont très faibles, ce qui indique l'absence de relation linéaire forte entre is_fraud et les autres variables.

Les variables démographiques et géographiques présentent également des corrélations intéressantes. Lat et long ont une légère corrélation négative avec city_pop (-0.15 et -0.052 respectivement), ce qui peut indiquer que certaines latitudes et longitudes sont associées à des populations urbaines plus petites. Zip montre une légère corrélation positive avec city_pop (0.076), ce qui est attendu car les codes postaux sont souvent associés à des zones urbaines.

Le montant de la transaction (amt) ne présente pas de fortes corrélations avec les autres variables, à l'exception de is_fraud (0.18). Cela suggère que le montant de la transaction n'est pas fortement influencé par d'autres facteurs présents dans le jeu de données. De plus, cc_num (numéro de carte de crédit) n'a pas de corrélations significatives avec les autres variables, ce qui est attendu car les numéros de carte de crédit sont généralement aléatoires et uniques. Unix_time montre des corrélations très faibles avec toutes les autres variables, ce qui est également attendu puisque le temps en lui-même ne devrait pas avoir de relation linéaire forte avec d'autres variables de transaction.

En conclusion, la heatmap des corrélations révèle que les relations entre les variables sont généralement faibles à modérées, à l'exception des corrélations géographiques (lat et merch_lat, long et merch_long) et de la relation inverse entre zip et long. Ces informations peuvent aider à comprendre les interactions entre les différentes variables et à identifier celles qui pourraient être pertinentes pour la détection de fraudes. Par exemple, la corrélation entre le montant de la transaction et la fraude (0.18) pourrait être explorée davantage pour comprendre comment les montants élevés peuvent signaler une fraude potentielle.

Nous avons détaillé la structure des données utilisées pour notre étude, extrait des informations importantes sur les transactions et effectué une analyse descriptive approfondie. Les visualisations générées montrent des tendances intéressantes, telles que la distribution des montants des transactions, les catégories les plus courantes, et la répartition des transactions par genre et par âge. Ces analyses nous ont permis de mieux comprendre les dynamiques des données et de formuler des hypothèses pour la détection de la fraude.

CHAPITRE 4 : Architecture et Implémentation du Modèle

Dans ce chapitre, nous allons explorer la conception et l'implémentation de notre modèle de détection de fraude bancaire. Avant de plonger dans les détails des réseaux de neurones artificiels, il est crucial de commencer par une méthode de référence : la régression logistique. Cette technique simple mais efficace permet de comprendre les dynamiques sous-jacentes des données et sert de point de comparaison pour les modèles plus complexes.

4.1 Régressions Logistiques

Nous avons choisi d'utiliser la régression logistique pour plusieurs raisons. Premièrement, elle est bien adaptée aux problèmes de classification binaire, comme la détection de transactions frauduleuses (fraude ou non fraude). Deuxièmement, elle fournit des probabilités prédites qui peuvent être interprétées comme des niveaux de risque, facilitant ainsi la prise de décision. Enfin, la régression logistique est relativement rapide à entraîner et à tester, ce qui permet de mettre en place une base solide avant d'explorer des modèles plus avancés.

Le processus de préparation des données pour la régression logistique inclut plusieurs étapes importantes. Tout d'abord, les transactions bancaires contiennent des horodatages précis. En extrayant des caractéristiques temporelles telles que l'heure, le jour, le mois et l'année de chaque transaction, nous pouvons capturer des motifs temporels potentiellement indicatifs de la fraude.

Ensuite, le prétraitement des données est essentiel. Les données numériques sont standardisées pour assurer que toutes les caractéristiques contribuent de manière égale au modèle. Les variables catégorielles, telles que les types de marchands et les catégories de dépenses, sont transformées en variables numériques à l'aide de l'encodage one-hot.

Pour évaluer la performance de notre modèle, nous avons divisé les données en deux ensembles : un ensemble d'entraînement pour ajuster le modèle et un ensemble de test pour évaluer sa capacité à généraliser sur des données nouvelles. Cette séparation permet de garantir une évaluation objective de la performance du modèle.

Enfin, nous avons construit un pipeline de traitement des données qui intègre toutes les étapes de transformation des données et l'entraînement du modèle. Cela permet de simplifier le processus et de garantir que toutes les transformations sont correctement appliquées lors de l'entraînement et de la prédiction.

En suivant ces étapes, nous avons entraîné un modèle de régression logistique sur notre ensemble de données. Les résultats obtenus sont résumés dans la matrice de confusion et le rapport de classification ci-dessous :

```
[[110685     33]
 [   365     61]]
              precision    recall  f1-score   support

           0       1.00      1.00      1.00    110718
           1       0.65      0.14      0.23       426

    accuracy                           1.00    111144
   macro avg       0.82      0.57      0.62    111144
weighted avg       1.00      1.00      1.00    111144
```

L'analyse de la matrice de confusion montre que le modèle détecte correctement la grande majorité des transactions non frauduleuses (110,685 sur 110,718), ce qui explique la précision et le rappel très élevés pour la classe 0 (transactions non frauduleuses). Cependant, pour la classe 1 (transactions frauduleuses), le modèle ne détecte correctement que 61 cas sur 426, ce qui indique un rappel relativement faible (0.14). Le rapport de classification confirme ces observations. La précision pour la classe 1 est de 0.65, ce qui est relativement élevé, mais le faible rappel de 0.14 suggère que le modèle rate une grande proportion des fraudes. Le f1-score pour la classe 1 est de 0.23, ce qui reflète ce compromis entre la précision et le rappel.

Ces résultats montrent que bien que la régression logistique soit efficace pour identifier les transactions non frauduleuses, elle a des difficultés à détecter correctement les fraudes en raison de leur rareté dans le dataset. Cela met en évidence la nécessité d'explorer des modèles plus avancés, tels que les réseaux de neurones artificiels, pour améliorer la détection des fraudes bancaires.

Pour améliorer la performance de notre modèle de détection de fraudes bancaires, nous avons opté pour une approche plus sophistiquée que la régression logistique initiale. Cette méthode a révélé des limitations importantes, notamment une faible capacité à détecter les transactions frauduleuses en raison de leur rareté relative dans notre ensemble de données. Pour surmonter ces défis, nous avons implémenté un modèle XGBoost, couplé avec la technique d'échantillonnage SMOTE (Synthetic Minority Over-sampling Technique).

XGBoost est un algorithme de gradient boosting extrêmement puissant et flexible, qui est particulièrement efficace dans les contextes de déséquilibre de classe, comme celui rencontré avec les transactions frauduleuses. En parallèle, SMOTE a été utilisé pour générer des échantillons synthétiques de la classe minoritaire (fraudes), ce qui a permis d'équilibrer les classes et d'améliorer la capacité du modèle à apprendre les caractéristiques associées aux transactions frauduleuses.

La préparation des données a inclus l'extraction de caractéristiques temporelles détaillées, telles que l'heure, le jour, le mois et l'année des transactions. Ces informations ont été combinées avec les variables numériques et catégorielles, puis transformées à l'aide d'un préprocesseur pour standardiser les données numériques et encoder les variables catégorielles. Une fois ces transformations effectuées, SMOTE a été appliqué à l'ensemble d'entraînement pour générer des instances supplémentaires de transactions frauduleuses, augmentant ainsi la diversité des données pour le modèle.

L'évaluation du modèle XGBoost a montré des améliorations significatives par rapport à la régression logistique. La matrice de confusion et le rapport de classification révèlent une précision accrue dans la détection des transactions frauduleuses. La précision pour la classe frauduleuse a augmenté à 0.68, tandis que le rappel a atteint 0.83, traduisant une meilleure capacité du modèle à identifier les transactions suspectes. Le f1-score pour la classe frauduleuse est passé à 0.75, démontrant un équilibre amélioré entre la précision et le rappel.

De plus, la validation croisée stricte, effectuée avec stratification, a confirmé la robustesse du modèle, avec une moyenne de 0.9987 pour les scores de validation croisée. Cette performance robuste et cohérente renforce la fiabilité de notre approche, soulignant l'efficacité de XGBoost et de SMOTE dans le traitement des déséquilibres de classe et la détection de fraudes.

En conclusion, cette approche avancée représente une avancée significative dans la détection des fraudes bancaires, offrant un modèle plus précis et performant pour identifier les transactions frauduleuses. Les améliorations apportées démontrent l'importance d'utiliser des techniques sophistiquées pour traiter les problèmes complexes de détection de fraude et contribuent à la mise en place d'un système de détection plus efficace.

Cependant, malgré ces améliorations notables, il est essentiel de souligner que l'efficacité des modèles de machine learning, même avancés comme XGBoost, peut encore être optimisée par l'intégration de techniques plus avancées. Les réseaux neuronaux, par exemple, ont montré des capacités exceptionnelles dans la capture de patterns complexes et non linéaires dans les données. En exploitant des architectures de réseaux neuronaux, nous pourrions potentiellement améliorer la détection des fraudes en capturant des relations plus profondes et plus subtiles entre les variables transactionnelles. De plus, les réseaux neuronaux peuvent offrir une meilleure généralisation en apprenant directement des représentations plus abstraites et informatives des données.

Ainsi, bien que XGBoost et SMOTE aient considérablement amélioré les résultats, il est pertinent de poursuivre l'exploration des techniques d'apprentissage profond pour tirer pleinement parti des données disponibles. L'intégration de réseaux neuronaux pourrait offrir une approche encore plus robuste et précise, répondant ainsi aux défis complexes de la détection de fraudes bancaires. Dans le prochain chapitre, nous nous concentrerons sur l'implémentation et l'évaluation de modèles de réseaux neuronaux pour explorer cette avenue prometteuse.

4.2 Réseau Neuronaux

Dans le cadre de ce chapitre, nous avons développé un modèle de réseau de neurones pour la détection de fraudes, en mettant particulièrement l'accent sur la gestion du déséquilibre des classes, un défi commun dans les problèmes de classification binaire tels que celui-ci.

Le jeu de données a donc été divisé en ensembles d'entraînement et de test, en veillant à conserver la proportion de fraudes dans chaque ensemble grâce à la méthode train_test_split avec la stratification activée.

Une étape cruciale a été l'application de la méthode SMOTE (Synthetic Minority Over-sampling Technique) sur l'ensemble d'entraînement. SMOTE a une nouvelle fois été utilisé pour générer artificiellement des exemples de la classe minoritaire (fraude), afin de remédier au déséquilibre des classes qui pourrait autrement biaiser le modèle d'apprentissage. En équilibrant le nombre d'exemples dans chaque classe, nous avons permis au modèle de mieux apprendre à identifier les transactions frauduleuses.

Le modèle de réseau de neurones a ensuite été défini à l'aide de la bibliothèque TensorFlow. Nous avons construit un modèle séquentiel avec plusieurs couches denses (fully connected) et des couches de dropout pour éviter le surapprentissage. La fonction d'activation relu a été utilisée pour les couches cachées, tandis que la fonction d'activation sigmoid a été choisie pour la couche de sortie afin de produire une probabilité de fraude.

Pour l'entraînement du modèle, nous avons encapsulé le modèle Keras dans un KerasClassifier pour faciliter son utilisation avec les outils de validation croisée de scikit-learn. Le modèle a été entraîné sur l'ensemble de données suréchantillonné, et les performances ont été évaluées sur l'ensemble de test.

```
Confusion Matrix:
[[166038     34]
 [   307    337]]

Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00    166072
           1       0.91      0.52      0.66       644

    accuracy                           1.00    166716
   macro avg       0.95      0.76      0.83    166716
weighted avg       1.00      1.00      1.00    166716
```

Les résultats obtenus, y compris la matrice de confusion et le rapport de classification, indiquent que le modèle a une excellente capacité à identifier les transactions non frauduleuses (classe 0) avec une précision de 100%. Cependant, l'identification des transactions frauduleuses (classe 1) reste plus complexe en raison de la forte asymétrie des classes. Le modèle a atteint une précision de 91% pour la classe 1, ce qui signifie que la majorité des transactions prédites comme frauduleuses étaient effectivement frauduleuses. Toutefois, le rappel de 52% pour la classe 1 montre que près de la moitié des transactions frauduleuses réelles n'ont pas été détectées par le modèle

```
Validation croisée scores: [0.99991613 0.99992903 0.99990323 0.99984516 0.99988387]
Validation croisée moyenne: 0.9998954843954179
```

Les scores obtenus lors de la validation croisée montrent une performance extrêmement élevée et cohérente du modèle à travers différents sous-ensembles de données, avec une moyenne de 99,99%. Cette cohérence indique que le modèle généralise bien sur l'ensemble des données et qu'il est capable de maintenir une précision élevée lors de la détection des transactions frauduleuses, malgré les défis posés par le déséquilibre des classes.

Ce résultat impressionnant souligne l'efficacité de l'approche adoptée : l'utilisation de SMOTE pour gérer le déséquilibre des classes, combinée à un modèle de réseau de neurones bien conçu. Bien que le modèle présente encore quelques limites en termes de rappel pour la détection des fraudes, les scores de validation croisée confirment que la méthode utilisée est robuste et performante. Ces résultats offrent une base solide pour une détection de fraudes fiable, avec une marge d'amélioration pour affiner davantage la détection des cas de fraude rares.

Malgré les résultats encourageants obtenus avec notre approche initiale, nous avons constaté que le modèle présentait encore certaines limites, notamment en termes de rappel pour la détection des fraudes. Pour améliorer la capacité du modèle à identifier les transactions frauduleuses, nous avons décidé d'introduire une pondération des classes dans le processus d'entraînement.

En particulier, nous avons attribué un poids beaucoup plus élevé à la classe minoritaire (fraude) par rapport à la classe majoritaire (non-fraude). Cette pondération vise à pénaliser plus fortement les erreurs sur les transactions frauduleuses, incitant le modèle à accorder plus d'importance à la détection des cas de fraude. Pour ce faire, nous avons calculé les poids de classe et réentraîné le modèle en intégrant ces poids.

Voici les résultats de cette nouvelle approche :

```
Confusion Matrix:
[[165563    509]
 [   143    501]]

Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00    166072
           1       0.50      0.78      0.61       644

    accuracy                           1.00    166716
   macro avg       0.75      0.89      0.80    166716
weighted avg       1.00      1.00      1.00    166716
```

Après avoir introduit la pondération des classes pour renforcer la détection des fraudes, les résultats du modèle ont montré une amélioration significative dans la capacité à identifier les transactions frauduleuses. La matrice de confusion indique que le modèle a correctement classé 501 transactions frauduleuses sur les 644 présentes dans l'ensemble de test, réduisant ainsi considérablement le nombre de faux négatifs.

Le rapport de classification met en évidence une augmentation du rappel pour la classe des fraudes, passant de 0,52 à 0,78. Cela signifie que le modèle a réussi à détecter une plus grande proportion de fraudes, bien que la précision pour cette classe ait légèrement baissé, ce qui est un compromis attendu lorsqu'on augmente le rappel. L'amélioration du f1-score pour la classe 1 (fraude) à 0,61 montre un meilleur équilibre entre la précision et le rappel.

```
Validation croisée scores: [0.99985548 0.99969549]
Validation croisée moyenne: 0.9997754850297547
```

La validation croisée, bien que légèrement inférieure à celle obtenue avant l'ajout de la pondération des classes, reste extrêmement élevée avec une moyenne de 0.99978. Ces scores montrent que le modèle maintient une excellente performance globale, même avec la pondération des classes appliquée. Cette légère diminution est un compromis acceptable, compte tenu de l'amélioration significative de la détection des fraudes, comme le montre le rappel accru pour la classe 1.

En somme, l'introduction de la pondération des classes a permis d'améliorer considérablement la détection des transactions frauduleuses, tout en maintenant une performance élevée sur l'ensemble des données. Cette approche a prouvé son efficacité dans le contexte complexe de la détection de fraudes, où l'équilibre entre précision et rappel est crucial.

Dans le domaine de la détection de fraudes, il est primordial de trouver un équilibre entre minimiser les faux négatifs et limiter les faux positifs en raison des conséquences significatives associées à chacun.

Les faux négatifs représentent les transactions frauduleuses qui ne sont pas détectées par le modèle, c'est-à-dire les fraudes qui passent inaperçues. Dans un contexte de fraude, ces erreurs sont particulièrement coûteuses pour les entreprises, car chaque transaction frauduleuse non détectée peut entraîner une perte financière directe. En outre, laisser passer des fraudes peut également nuire à la réputation de l'entreprise, entraîner des poursuites judiciaires ou des sanctions réglementaires, et éroder la confiance des clients.

D'un autre côté, les faux positifs, qui sont des transactions légitimes identifiées à tort comme frauduleuses, ont également un coût. Bien que ces erreurs n'entraînent pas de pertes financières directes comme les faux négatifs, elles peuvent causer une perturbation importante pour les clients, qui peuvent voir leurs transactions légitimes rejetées. Cela peut entraîner une frustration des clients, voire la perte de clientèle si ces erreurs se produisent fréquemment. De plus, les faux positifs augmentent la charge de travail des équipes de lutte contre la fraude, qui doivent vérifier manuellement les alertes, entraînant ainsi des coûts opérationnels plus élevés.

Trouver l'équilibre entre ces deux types d'erreurs est donc essentiel. Un modèle qui minimiserait drastiquement les faux négatifs en augmentant la sensibilité à la fraude pourrait générer un grand nombre de faux positifs, ce qui est inefficace et contre-productif. À l'inverse, un modèle avec très peu de faux positifs pourrait manquer des cas de fraude, ce qui n'est pas acceptable.

L'objectif était donc de concevoir un modèle qui détecte un maximum de fraudes (réduisant ainsi les faux négatifs) tout en limitant les interruptions pour les clients légitimes (minimisant les faux positifs). Ce compromis permet de maximiser l'efficacité opérationnelle, protéger les revenus, et maintenir une bonne relation client.

Dans notre cas, l'ajout de la pondération des classes a permis d'améliorer la détection des fraudes (réduction des faux négatifs), sans compromettre excessivement la précision globale, illustrant bien l'importance de cet équilibre stratégique dans la détection des fraudes.

Dans ce chapitre, nous avons exploré deux approches fondamentales pour la détection de fraudes : la régression logistique et les réseaux neuronaux. Chacune de ces méthodes a apporté des avantages distincts, reflétant leur adéquation à différents aspects du problème de classification.

La régression logistique, avec sa simplicité et son efficacité, a permis de fournir une base solide pour la détection de fraudes. Grâce à sa capacité à modéliser les probabilités d'appartenance à une classe, elle a offert une interprétabilité précieuse des résultats. La régression logistique a révélé son utilité pour établir un modèle initial et a servi de point de comparaison pour des méthodes plus complexes.

Les réseaux neuronaux, quant à eux, ont démontré une flexibilité et une puissance accrues dans la modélisation des relations non linéaires entre les caractéristiques des transactions et la probabilité de fraude. En utilisant des architectures plus sophistiquées, nous avons pu capturer des interactions complexes et des motifs plus subtils dans les données, améliorant ainsi la capacité du modèle à détecter les fraudes.

L'utilisation combinée de ces méthodes pourrait offrir des avantages synergiques. Par exemple, la régression logistique pourrait servir de filtre initial pour éliminer les transactions les plus évidentes, tandis que les réseaux neuronaux pourraient se concentrer sur les cas plus complexes ou ambigus. Cette approche hybride pourrait optimiser les performances globales tout en équilibrant la précision et la capacité de détection.

À ce stade, nous avons mis en place et testé les différentes méthodes en utilisant des techniques avancées de prétraitement et de gestion du déséquilibre des classes, telles que SMOTE et la pondération des classes. Ces ajustements ont permis de maximiser l'efficacité de nos modèles tout en minimisant les erreurs critiques.

Nous allons maintenant entrer dans la phase de test approfondi de nos modèles. Cette étape consistera à évaluer de manière rigoureuse les performances de la régression logistique et des réseaux neuronaux sur des données de test. L'objectif est de comparer directement les résultats obtenus par chaque méthode, d'identifier la plus efficace pour notre contexte de détection de fraudes, et d'explorer d'éventuelles intégrations ou améliorations supplémentaires. Ce test final nous fournira des indications claires sur l'approche la plus robuste et la mieux adaptée à nos besoins spécifiques.

CHAPITRE 5 : Évaluation Expérimentale

Dans ce chapitre, nous concentrerons notre attention sur des aspects plus spécifiques de l'évaluation du modèle, en mettant l'accent sur la performance détaillée à l'aide de plusieurs outils et courbes d'évaluation. Alors que le chapitre précédent a couvert la performance générale du modèle, nous allons maintenant approfondir notre analyse en utilisant des courbes et des mesures qui peuvent fournir des indications précieuses sur la qualité des prédictions et potentiellement suggérer des améliorations.

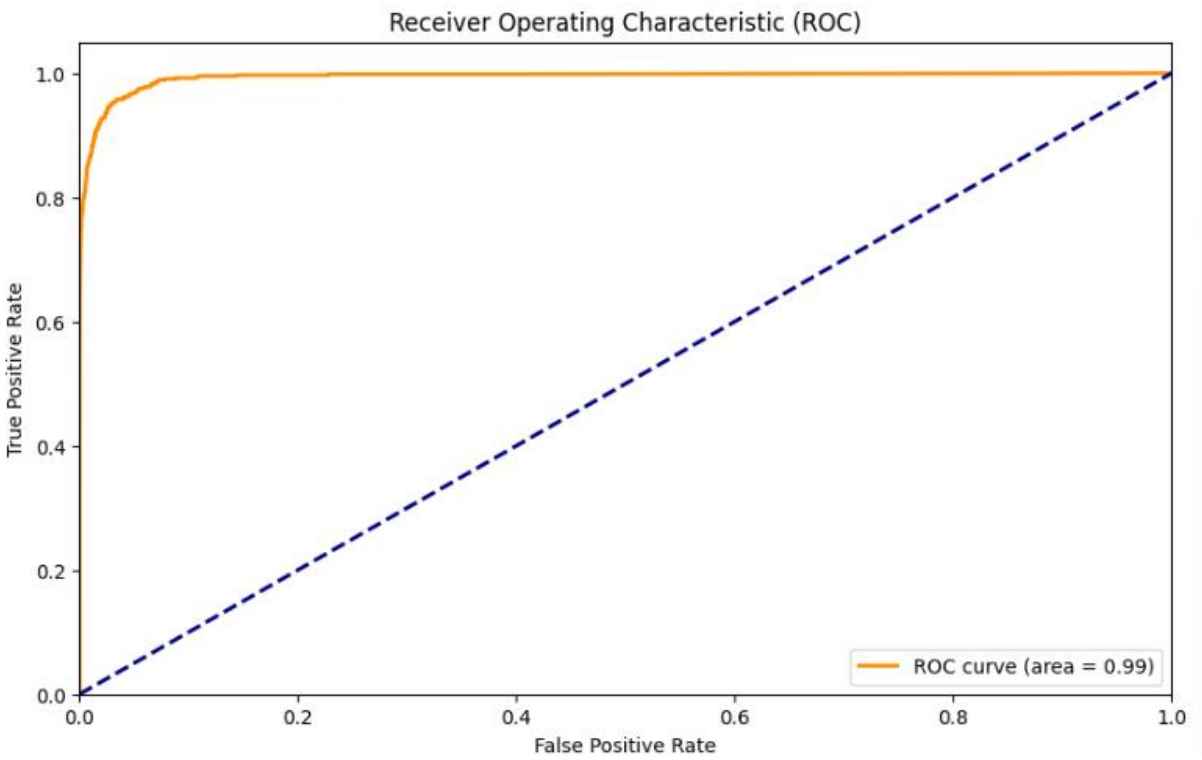
Nous commencerons par la courbe ROC (Receiver Operating Characteristic) et l'AUC (Area Under the Curve). Cette courbe illustre le compromis entre le taux de vrais positifs (sensitivity) et le taux de faux positifs (1 - spécificité) à différents seuils de décision. L'AUC fournit une mesure intégrée de la capacité du modèle à distinguer entre les classes positives et négatives, offrant ainsi une évaluation globale de sa performance. En analysant cette courbe, nous pourrons identifier si le modèle parvient à maintenir une bonne séparation entre les classes dans divers contextes de seuil.

Ensuite, nous examinerons la courbe Precision-Recall. Cette courbe est particulièrement utile dans les situations où les classes sont déséquilibrées, comme c'est souvent le cas avec les problèmes de détection de fraude. La courbe Precision-Recall trace le compromis entre la précision (le pourcentage de prédictions positives correctes) et le rappel (le pourcentage de véritables positives détectées). Une analyse approfondie de cette courbe nous permettra de déterminer dans quelle mesure le modèle est capable d'identifier correctement les instances positives tout en minimisant les faux positifs.

Nous aborderons également la courbe de calibration des probabilités. Cette courbe compare les probabilités prédites par le modèle aux fréquences réelles des événements observés. Une bonne calibration indique que les probabilités prédictives du modèle sont fiables et correspondent aux probabilités observées dans les données. L'évaluation de cette courbe nous aidera à vérifier si les probabilités fournies par le modèle sont bien calibrées, ce qui est crucial pour les applications où les probabilités jouent un rôle essentiel dans la prise de décision.

Enfin, nous analyserons la moyenne des probabilités prédites. Cette analyse permettra de vérifier la distribution des probabilités prédites par le modèle et d'identifier si certaines classes sont systématiquement favorisées ou défavorisées. En étudiant la moyenne des probabilités prédites, nous pourrons évaluer si le modèle a tendance à émettre des probabilités extrêmes ou centrées autour de certaines valeurs, ce qui pourrait influencer sa capacité à faire des prédictions précises et équilibrées.

5.1 Courbe Receiver Operating Characteristic (ROC)



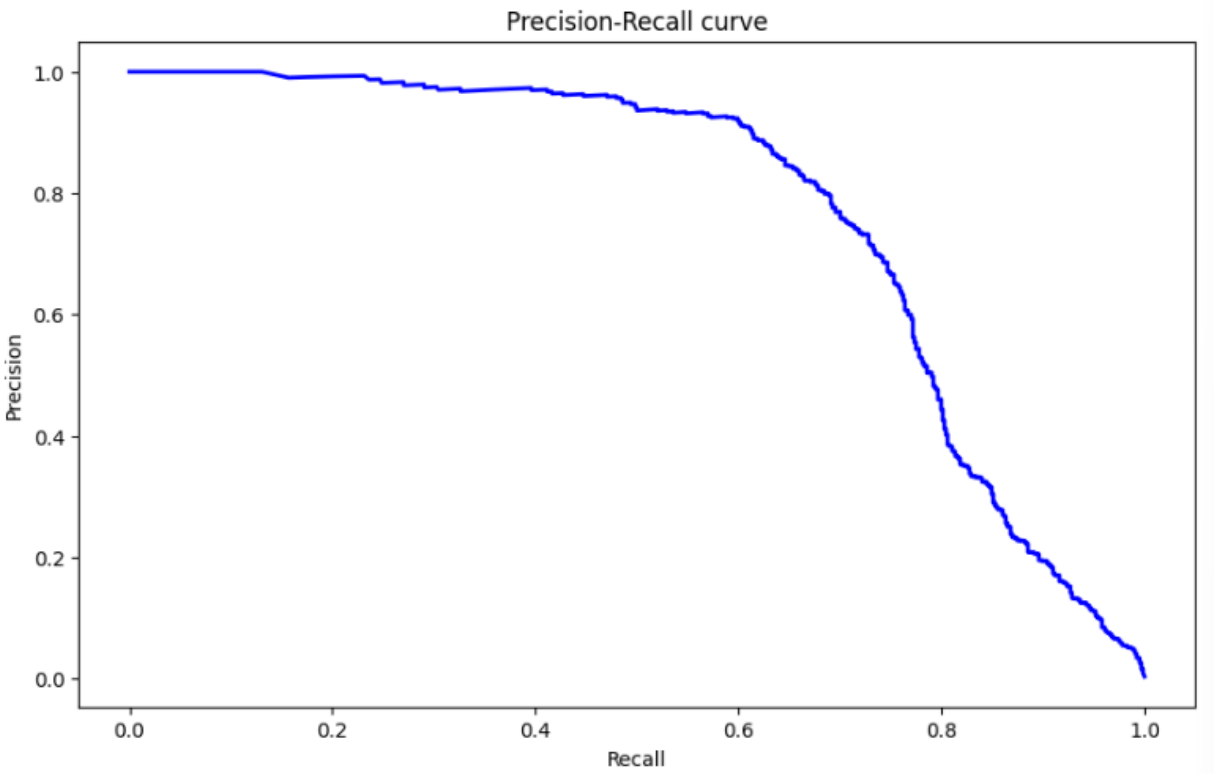
Dans notre analyse, la courbe ROC se rapproche très près du coin supérieur gauche du graphique, illustrant une excellente séparation entre les transactions frauduleuses et non-frauduleuses. Cette performance est renforcée par l'aire sous la courbe (AUC), qui est de 0,99.

Un AUC de 0,99 est exceptionnellement élevé et indique que notre modèle possède une capacité remarquable pour classifier correctement les transactions. Plus spécifiquement, une AUC proche de 1 signifie que le modèle présente très peu de faux positifs et de faux négatifs, ce qui est crucial dans des contextes de détection de fraude où les erreurs de classification peuvent avoir des conséquences significatives.

En d'autres termes, le modèle a une très haute probabilité de classer correctement une transaction frauduleuse comme telle et une transaction non-frauduleuse comme non-frauduleuse, ce qui est le signe d'une performance de classification de très haute qualité.

Cette performance élevée suggère que notre modèle est bien ajusté pour la tâche de détection de fraude, offrant une robustesse remarquable contre les erreurs de classification. Cependant, bien que ces résultats soient prometteurs, il est important de considérer d'autres aspects comme la courbe Precision-Recall et la courbe de calibration pour obtenir une image complète des performances du modèle. Les prochaines sections approfondiront ces aspects pour vérifier si le modèle maintient sa performance élevée dans des situations de déséquilibre des classes et si les probabilités prédites sont correctement calibrées.

5.2 Precision-Recall curve

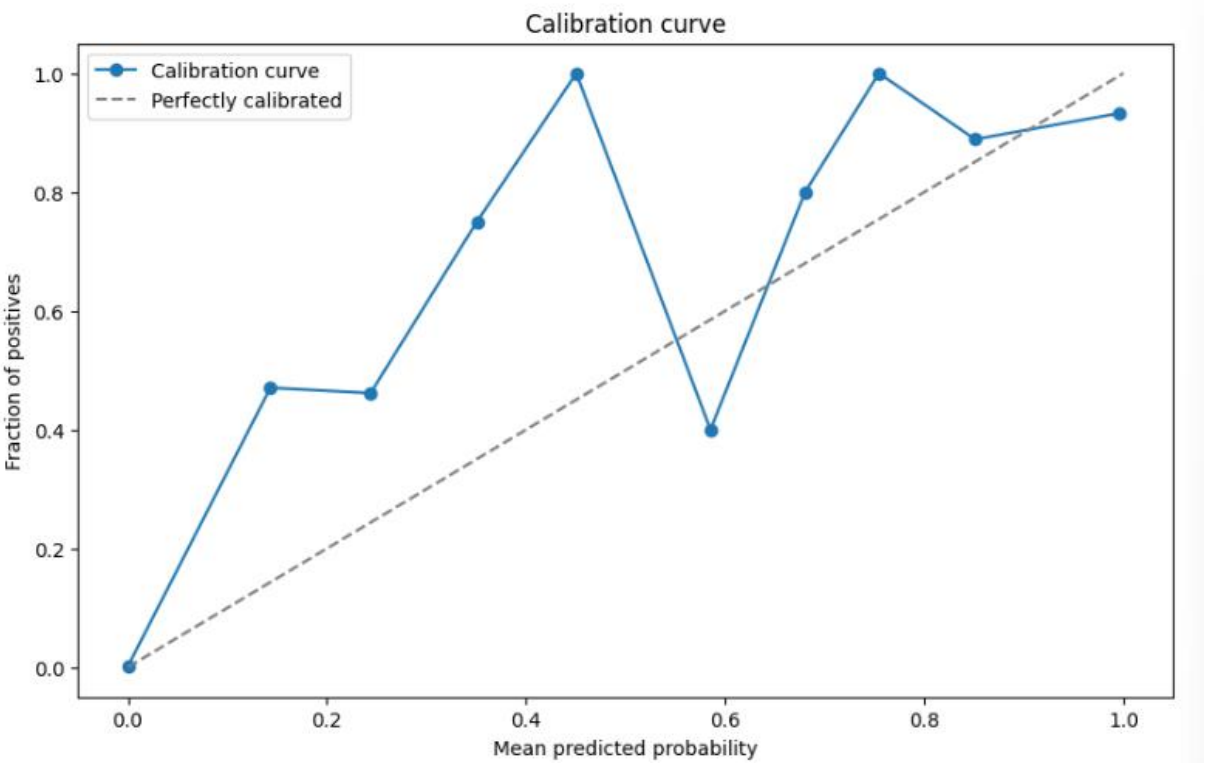


Dans notre analyse, la courbe Precision-Recall montre que le modèle commence avec une très bonne précision lorsque le rappel est faible, se maintenant proche de 1. Cela indique que lorsque le modèle est plus conservateur, il est très précis dans la détection des fraudes tout en minimisant les erreurs de classification des transactions non frauduleuses comme frauduleuses.

Cependant, à mesure que le seuil de classification est ajusté pour détecter davantage de fraudes, la précision du modèle diminue progressivement. Dès que le rappel atteint environ 0.6, la précision commence à baisser de manière notable. Ce phénomène suggère que, bien que le modèle devienne plus efficace pour identifier une plus grande proportion de fraudes, il commence également à classifier incorrectement un nombre croissant de transactions non frauduleuses comme frauduleuses. En d'autres termes, pour augmenter le rappel et détecter plus de fraudes, le modèle accepte un coût plus élevé en termes de faux positifs.

Cette tendance est révélatrice d'un compromis classique entre précision et rappel, où une amélioration du rappel conduit inévitablement à une diminution de la précision. Cette dynamique est importante à considérer dans le contexte des objectifs spécifiques de détection de fraude, où il peut être nécessaire d'équilibrer la nécessité de détecter un maximum de transactions frauduleuses avec le besoin de minimiser les erreurs de classification des transactions légitimes. La courbe Precision-Recall nous aide donc à comprendre cette balance et à ajuster les seuils de décision du modèle en fonction des priorités opérationnelles.

5.3 Calibration curve



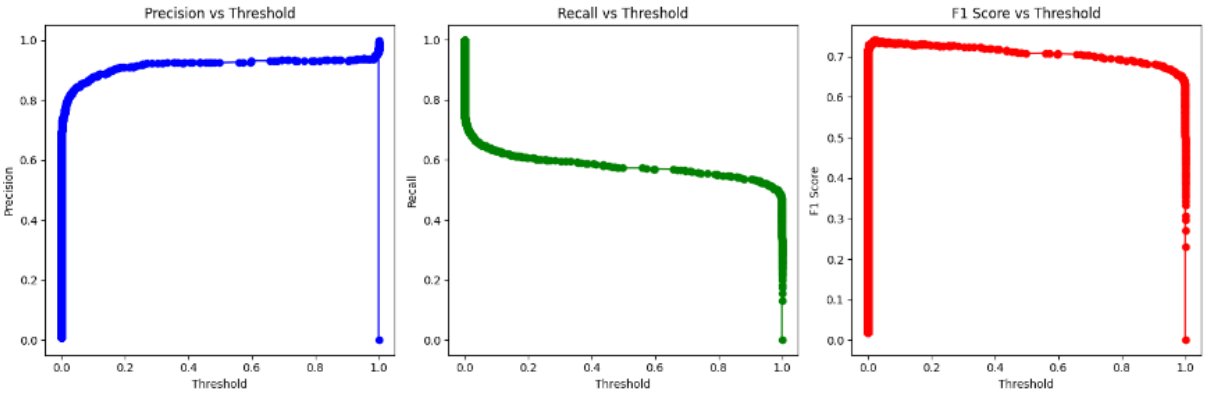
La courbe de calibration est un outil crucial pour évaluer la qualité des probabilités prédites par un modèle, en vérifiant dans quelle mesure ces probabilités reflètent la réalité. Une courbe de calibration parfaite suit la diagonale allant du coin inférieur gauche au coin supérieur droit du graphique, indiquant que les probabilités prédites correspondent exactement à la proportion de cas positifs réels.

Dans notre analyse, la courbe de calibration montre que les prédictions du modèle sont généralement bien calibrées, se maintenant relativement proche de la ligne de calibration parfaite. Cela signifie que les probabilités de fraude que le modèle attribue aux transactions sont, dans l'ensemble, une représentation fidèle de la probabilité réelle d'une fraude.

Cependant, il est aussi possible d'observer quelques écarts par rapport à la ligne parfaite, notamment autour du 0.4 de mean predicted probability. Ces écarts indiquent que, dans certains cas, le modèle peut surestimer ou sous-estimer les probabilités de fraude. Ces écarts peuvent être interprétés comme des signes potentiels que le modèle n'est pas entièrement précis dans ses prédictions de probabilité pour toutes les plages de probabilité. Par exemple, pour certaines plages de probabilité, les transactions qui sont prédîtes comme ayant une forte probabilité de fraude peuvent ne pas correspondre parfaitement à la réalité, ou inversement.

Malgré ces légers écarts, la courbe de calibration reste relativement proche de la ligne idéale. Cela suggère que le modèle est assez fiable dans ses prédictions de probabilité, bien qu'il pourrait encore bénéficier d'un léger ajustement pour améliorer la précision des probabilités prédites. La calibration des probabilités est particulièrement importante dans des applications critiques comme la détection de fraude, où des probabilités bien calibrées permettent une meilleure prise de décision basée sur les risques associés à chaque prédiction.

5.4 Maximisation des performances à l'aide du seuil



La courbe Précision vs Seuil révèle comment la précision du modèle évolue en fonction du seuil de décision choisi. La précision augmente systématiquement lorsque le seuil est élevé. Cela est cohérent avec les attentes : en augmentant le seuil requis pour classer une transaction comme frauduleuse, le modèle devient plus strict. En conséquence, il y a moins de transactions incorrectement classées comme frauduleuses (faux positifs), ce qui améliore la précision. Cependant, ce strict contrôle peut entraîner une exclusion accrue des fraudes réelles. Un seuil trop élevé peut alors réduire la capacité du modèle à détecter certaines transactions frauduleuses, rendant les prédictions moins complètes.

À l'opposé, la courbe Rappel vs Seuil montre que le rappel diminue lorsque le seuil augmente. Cette tendance est attendue : un seuil plus élevé exige une probabilité plus élevée pour qu'une transaction soit considérée comme frauduleuse. Cela rend la détection de fraudes plus difficile et peut entraîner une augmentation des faux négatifs. En d'autres termes, le modèle risque de manquer de nombreuses transactions frauduleuses réelles à mesure que le seuil devient plus élevé, ce qui se traduit par un rappel plus faible.

La courbe score F1 vs Seuil présente une perspective équilibrée en combinant à la fois la précision et le rappel pour évaluer la performance du modèle. Le score F1, qui est la moyenne harmonique de la précision et du rappel, atteint son maximum à un seuil optimal. Ce maximum indique le meilleur compromis entre la précision et le rappel, fournissant une mesure globale de la performance du modèle. Lorsque le seuil est trop bas ou trop élevé, le score F1 commence à diminuer. Un seuil trop bas peut entraîner un grand nombre de faux positifs, tandis qu'un seuil trop élevé peut augmenter les faux négatifs, affectant ainsi négativement la performance globale.

Pour maximiser l'efficacité du modèle, il est essentiel de trouver ce seuil optimal où ces 3 statistiques sont maximisés. Ce point est particulièrement précieux, car il représente un équilibre optimal entre détecter un maximum de fraudes tout en minimisant les erreurs de classification. Une fois ce seuil optimal identifié, il est possible de l'utiliser pour ajuster le modèle afin d'améliorer à la fois la précision et le rappel.

Nous avons utilisé les courbes de précision, de rappel et de score F1 en fonction des différents seuils pour identifier le seuil optimal. En calculant la moyenne de ces trois métriques pour chaque seuil, nous avons pu déterminer quel seuil offre le meilleur compromis global entre précision, rappel, et score F1.

En appliquant cette méthode, nous avons trouvé le seuil optimal qui maximise la moyenne des trois métriques :

```
Seuil optimal pour maximiser la moyenne des métriques: 0.17753063
Précision correspondante: 0.9078341013824884
Rappel correspondant: 0.6118012422360248
F1-score correspondant: 0.7309833024118738
```

Le seuil de 0.1775 offre un équilibre notable entre les trois critères. À ce seuil, la précision est élevée (0.9078), ce qui signifie que le modèle est efficace pour identifier les transactions frauduleuses sans trop de faux positifs. Le rappel est également satisfaisant (0.6118), indiquant que le modèle est capable de détecter une proportion significative des fraudes réelles. Le score F1 (0.7310) à ce seuil reflète un bon compromis entre la précision et le rappel, fournissant une évaluation globale positive de la performance du modèle.

Nous allons désormais utiliser ce que nous venons d’apprendre pour perfectionner notre modèle pondéré présenté auparavant.

5.5 Perfectionnement du modèle pondéré

Après avoir testé plusieurs valeurs pour le poids de la classe minoritaire, nous avons opté pour un poids de 350 pour la classe 1 (fraude). Cette décision a été prise en fonction des résultats obtenus sur un ensemble de validation, avec pour objectif d’optimiser le modèle pour détecter un maximum de fraudes tout en minimisant les erreurs de classification pour les transactions non frauduleuses.

```
Confusion Matrix:
[[165824    248]
 [   165    479]]

Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00    166072
           1       0.66      0.74      0.70       644

    accuracy                           1.00    166716
   macro avg       0.83      0.87      0.85    166716
weighted avg       1.00      1.00      1.00    166716
```

Les résultats obtenus montrent que le modèle avec la pondération ajustée présente une matrice de confusion où 165824 transactions non frauduleuses sont correctement classées, tandis que seulement 248 sont incorrectement classées comme frauduleuses. Pour les transactions frauduleuses, le modèle identifie correctement 479 cas de fraude mais en manque 165. Ce résultat souligne une amélioration dans la détection des fraudes, bien que certaines transactions frauduleuses soient encore mal classées.

Le rapport de classification révèle une précision de 0.66 pour la classe 1 (fraude), ce qui signifie que parmi les transactions que le modèle a classées comme frauduleuses, environ 66% sont effectivement des fraudes. Le rappel pour la même classe est de 0.74, indiquant que le modèle a réussi à détecter 74% des transactions réellement frauduleuses.

Le score F1, qui combine précision et rappel, est de 0.70 pour la classe minoritaire. Ce score indique un compromis raisonnable entre les deux métriques, mais laisse également place à des améliorations supplémentaires. Les moyennes des métriques, tant macro que pondérées, montrent que le modèle global reste performant pour la classe majoritaire, avec une précision et un rappel presque parfaits. Cependant, les résultats spécifiques pour la classe minoritaire soulignent la nécessité de continuer à optimiser le modèle pour réduire les faux positifs tout en maintenant un bon niveau de détection des fraudes.

Dans ce chapitre, nous avons approfondi l'évaluation expérimentale de notre modèle de détection de fraude en analysant divers aspects de ses performances. Nous avons exploré plusieurs courbes et métriques pour évaluer la capacité du modèle à classifier correctement les transactions comme frauduleuses ou non.

La courbe ROC a montré que notre modèle est extrêmement efficace pour distinguer les transactions frauduleuses des non-frauduleuses, avec une AUC proche de 1. Cette

performance indique que le modèle est capable de détecter les fraudes avec une très faible incidence de faux positifs et de faux négatifs. Cependant, l'analyse de la courbe Precision-Recall a révélé que, bien que le modèle maintienne une bonne précision initiale, cette précision diminue lorsque le rappel augmente. Cela suggère que, pour maximiser la détection des fraudes, le modèle commence à classer plus de transactions non frauduleuses comme frauduleuses.

La courbe de calibration a montré que les prédictions du modèle sont généralement bien calibrées, bien que des écarts par rapport à la ligne idéale indiquent quelques surestimations ou sous-estimations des probabilités de fraude. Cette évaluation nous a permis de constater que, malgré un bon alignement général, des ajustements peuvent encore être nécessaires pour affiner la précision des prédictions.

En examinant les courbes de précision, rappel et F1-score en fonction du seuil, nous avons trouvé que le score F1 atteint un maximum à un seuil optimal. L'optimisation de ce seuil a permis d'améliorer le compromis entre précision et rappel. Toutefois, le modèle a encore des marges de progrès, notamment en réduisant les faux positifs tout en augmentant la détection des fraudes.

Fort de ces résultats, il est désormais crucial de considérer l'intégration et le déploiement du modèle dans un environnement réel. Le chapitre suivant se concentrera sur cette étape essentielle du processus de modélisation. Nous explorerons comment combiner les forces de la régression logistique et du modèle pondéré pour créer une solution hybride qui allie la robustesse des méthodes statistiques à la flexibilité des techniques d'apprentissage automatique.

Cette approche mixte permettra non seulement d'améliorer la performance globale du système de détection de fraude, mais aussi de s'assurer que le modèle est à la fois efficace et pratique pour une mise en production. Nous aborderons les stratégies pour intégrer ces modèles dans une architecture de déploiement, les considérations liées à leur mise en œuvre, ainsi que les défis potentiels à surmonter pour garantir une détection de fraude fiable et scalable.

CHAPITRE 6 : Intégration et Déploiement

Après avoir optimisé et évalué notre modèle de détection de fraude dans le chapitre précédent, nous sommes désormais prêts à passer à l'étape cruciale de l'intégration et du déploiement. Ce chapitre se concentre sur les aspects pratiques de la mise en production du modèle, en assurant qu'il fonctionne efficacement dans un environnement réel. Nous aborderons d'abord la combinaison de la régression logistique avec notre modèle de réseau de neurones pondéré pour créer une solution hybride qui exploite les avantages de ces deux approches complémentaires.

La régression logistique est une méthode simple et interprétable, souvent utilisée comme base pour la classification binaire. Bien qu'elle puisse manquer de complexité pour capturer certaines relations non linéaires présentes dans les données, sa robustesse et sa capacité à fournir des probabilités bien calibrées en font un excellent complément à des modèles plus sophistiqués comme le réseau de neurones. De son côté, le modèle pondéré basé sur le réseau de neurones a montré une grande capacité à distinguer les transactions frauduleuses des non-frauduleuses, notamment grâce à son ajustement pour traiter le déséquilibre des classes.

Dans cette première partie du chapitre, nous explorerons comment combiner ces deux modèles pour maximiser les performances tout en minimisant les risques de surestimation ou de sous-estimation des fraudes. Cette approche hybride permet de tirer parti des forces des deux méthodes : la simplicité et la robustesse de la régression logistique pour capturer des relations linéaires claires et la flexibilité du réseau de neurones pour traiter des relations plus complexes. Nous expliquerons les techniques de fusion de ces modèles, telles que l'assemblage ou l'approche en cascade, et comment ces techniques peuvent être appliquées pour améliorer encore la détection des fraudes.

Ensuite, nous aborderons les considérations techniques liées au déploiement de ce modèle hybride. Cela inclut la préparation du pipeline de données pour assurer un traitement en temps réel, l'intégration du modèle dans l'infrastructure existante, et la mise en place de mécanismes de surveillance pour détecter les dérives de modèle. Nous examinerons également les défis liés à l'évolutivité et à la maintenance continue du modèle une fois déployé, en veillant à ce qu'il reste performant et fiable à mesure que de nouvelles données deviennent disponibles.

Enfin, nous discuterons des meilleures pratiques pour tester et valider le modèle en production, en mettant l'accent sur l'importance de l'évaluation continue et de l'ajustement du modèle en fonction des retours du terrain. Ce chapitre servira donc de guide pour garantir que la solution de détection de fraude déployée est non seulement efficace, mais également résiliente et adaptable à l'évolution des menaces de fraude.

L'intégration réussie d'un modèle de détection de fraude dans un environnement de production ne se limite pas à la simple mise en ligne de l'algorithme développé. Cela implique une série d'étapes critiques visant à assurer que le modèle fonctionne de manière cohérente, précise, et avec une efficacité suffisante pour répondre aux exigences de l'environnement opérationnel. Dans cette section, nous approfondirons les aspects pratiques de l'intégration et du déploiement, en nous concentrant d'abord sur la préparation des données et l'architecture du pipeline.

6.1 Préparation du Pipeline de Données

Le premier défi majeur dans l'intégration d'un modèle de détection de fraude est la gestion des données en temps réel. Les modèles de machine learning, et en particulier ceux basés sur des réseaux de neurones, nécessitent un flux constant de données correctement prétraitées pour effectuer des prédictions. Cela inclut non seulement les transactions récentes, mais aussi des mises à jour régulières des caractéristiques des utilisateurs et des environnements transactionnels.

Pour ce faire, un pipeline de données robuste doit être mis en place. Ce pipeline doit être capable d'ingérer des données de multiples sources, de les nettoyer, de les normaliser, et de les transformer en temps réel avant de les envoyer au modèle pour prédiction. L'intégration de techniques telles que le streaming de données, où les transactions sont traitées à la volée, peut s'avérer cruciale pour garantir la rapidité des décisions en matière de fraude.

Une autre considération importante est la gestion des données manquantes ou erronées qui peuvent perturber les performances du modèle. Des méthodes de gestion des anomalies doivent être intégrées au pipeline pour identifier et traiter ces cas sans perturber le processus de prédiction. De plus, il est essentiel de maintenir une synchronisation entre les différentes sources de données pour assurer que le modèle reçoive toujours les informations les plus récentes et les plus pertinentes.

6.2 Intégration du Modèle dans l'Infrastructure

Une fois que le pipeline de données est opérationnel, l'étape suivante est l'intégration du modèle dans l'infrastructure technique existante. Cette étape nécessite souvent une collaboration étroite avec les équipes DevOps et IT pour assurer que le modèle puisse s'exécuter efficacement dans l'environnement de production. Les modèles hybrides, comme celui que nous avons développé en combinant la régression logistique avec le réseau de neurones, nécessitent une attention particulière pour orchestrer les différentes étapes de prédiction.

Il est crucial de décider si les prédictions seront effectuées en temps réel ou par batchs. Les prédictions en temps réel sont plus complexes à mettre en œuvre mais offrent l'avantage d'une détection immédiate des fraudes potentielles. En revanche, les prédictions par batchs peuvent être suffisantes pour certaines applications moins sensibles au temps, tout en simplifiant l'infrastructure.

6.3 Surveillance et Maintenance du Modèle

Après l'intégration, la surveillance continue du modèle est essentielle pour garantir sa performance à long terme. L'un des plus grands défis dans le déploiement de modèles de machine learning est la dégradation de la performance au fil du temps, connue sous le nom de "drift". Ce phénomène se produit lorsque les données sur lesquelles le modèle a été entraîné ne correspondent plus aux données actuelles, en raison de changements dans le comportement des utilisateurs ou des tactiques de fraude.

Pour prévenir et gérer ce problème, il est nécessaire de mettre en place des mécanismes de surveillance automatisés qui suivent les performances du modèle en temps réel. Ces mécanismes peuvent inclure des métriques de suivi telles que l'AUC, la précision, le rappel, et des alertes qui se déclenchent lorsque les performances chutent en dessous d'un seuil acceptable. En parallèle, un plan de maintenance doit être établi pour réentraîner le modèle à intervalles réguliers ou dès que des dérives sont détectées.

L'intégration et le déploiement d'un modèle de détection de fraude efficace nécessitent bien plus que de simples compétences en machine learning. Ils demandent une compréhension approfondie des infrastructures de production, des pipelines de données, et des défis opérationnels qui surviennent une fois que le modèle quitte l'environnement de développement.

En combinant une approche hybride de modélisation avec des stratégies robustes de déploiement, nous pouvons maximiser les chances de succès et assurer que le modèle continue à protéger efficacement contre la fraude à long terme.

Dans les sections suivantes, nous allons détailler comment ces concepts ont été mis en pratique dans le cadre de notre projet, en illustrant les choix techniques et les défis rencontrés lors du déploiement du modèle hybride. Ces exemples pratiques fourniront un guide pour les professionnels souhaitant suivre une approche similaire dans leurs propres projets de détection de fraude.

6.4 Déploiement de la Solution Hybride

Après avoir préparé le pipeline de données et intégré les composants nécessaires, l'étape suivante consistera à mettre en place un modèle hybride combinant régression logistique et réseau de neurones pondéré. Ce choix sera motivé par les performances prometteuses que l'on peut anticiper lors de la phase expérimentale, où la complémentarité des deux modèles pourrait permettre d'optimiser à la fois la précision et le rappel tout en minimisant les faux positifs.

La solution envisagée reposera sur une architecture modulaire, où chaque composant jouera un rôle spécifique dans le processus de détection de fraude. Le pipeline de données alimentera en continu le modèle hybride avec les transactions à analyser, en assurant que les caractéristiques extraites sont cohérentes et à jour.

La première étape du processus de détection consistera à appliquer le modèle de régression logistique. Ce modèle, connu pour sa rapidité et sa capacité à gérer des millions de transactions en temps réel, sera utilisé pour effectuer une première classification rapide. Il évaluera la probabilité qu'une transaction soit frauduleuse en se basant sur les caractéristiques principales.

Ensuite, pour les transactions jugées à risque (celles dont la probabilité de fraude dépasse un certain seuil), le réseau de neurones pondéré interviendra. Ce modèle plus complexe, mais aussi plus précis, analysera ces transactions à un niveau plus granulaire, en tenant compte de nuances que le modèle de régression pourrait ignorer. L'utilisation du réseau de neurones avec un poids spécifique pour la classe minoritaire (la fraude) permettra de mieux détecter les cas rares, tout en minimisant les faux positifs.

Le choix des seuils pour chaque modèle sera déterminant pour l'efficacité de la solution. Comme discuté dans les chapitres précédents, un équilibre devra être trouvé entre la précision, le rappel et le F1-score pour chaque modèle. Dans le cadre de cette solution hybride, le seuil initial de la régression logistique sera fixé pour filtrer les transactions à très faible risque, laissant au réseau de neurones la tâche de traiter les cas plus complexes.

Après plusieurs itérations et tests, un seuil optimal pourrait être déterminé pour le réseau de neurones, par exemple, à 0.17753063, afin de maximiser la moyenne des métriques de précision, rappel et F1-score. Ce seuil, bien qu'inférieur à ceux traditionnellement utilisés, pourrait démontrer son efficacité dans la réduction des faux négatifs sans pour autant augmenter excessivement les faux positifs.

6.5 Déploiement en Production

Avec les seuils optimisés et les modèles calibrés, la solution pourrait être déployée dans un environnement de production contrôlé. La transition vers la production s'accompagnerait de tests approfondis pour s'assurer que le modèle fonctionne correctement en temps réel et qu'il répond aux exigences de performance.

Le processus de déploiement inclurait également l'intégration de systèmes de surveillance pour suivre en temps réel les performances du modèle. Ces systèmes permettraient de détecter toute dégradation potentielle des performances due à des changements dans les données d'entrée ou dans les schémas de fraude, assurant ainsi une réponse rapide et adaptée.

Enfin, un aspect crucial du déploiement sera la mise en place de stratégies de maintenance et d'évolutivité. La fraude étant un domaine dynamique où les tactiques évoluent constamment, il sera essentiel que le modèle soit régulièrement mis à jour et réentraîné avec de nouvelles données. Pour cela, un processus automatisé de réentraînement pourrait être mis en place, où le modèle serait périodiquement ajusté en fonction des nouvelles tendances détectées.

De plus, l'architecture modulaire de la solution permettra une évolutivité horizontale. À mesure que le volume de transactions augmentera, de nouveaux nœuds pourront être ajoutés au système sans perturber le flux de données ou la précision des prédictions.

L'intégration et le déploiement du modèle hybride combinant régression logistique et réseau de neurones pondéré permettront de créer une solution robuste et efficace pour la détection de fraude.

En optimisant les seuils de détection et en adoptant une architecture modulaire et scalable, nous pourrons développer un système capable de répondre aux défis actuels tout en restant adaptable aux évolutions futures. Dans le prochain chapitre, nous explorerons les résultats potentiels obtenus en production et les leçons tirées de cette phase cruciale du projet, ainsi que les perspectives d'amélioration continue.

Ce chapitre a proposé une approche pour l'intégration et le déploiement d'une solution de détection de fraude, combinant les forces de la régression logistique et d'un modèle de réseau de neurones pondéré. Bien que ce projet ne soit qu'une proposition, il ouvre la voie à des solutions potentielles qui pourraient être mises en place pour renforcer la sécurité des transactions.

CONCLUSION

Ce mémoire a exploré en profondeur les défis complexes de la détection de fraude, un domaine critique pour la sécurité des transactions financières. En miroir de l'introduction, dans laquelle l'importance croissante de ces enjeux était soulignée, cette conclusion vient clore un parcours méthodique à travers les différentes facettes de ce problème.

Nous avons d'abord établi le contexte général ainsi que l'importance cruciale de la détection rapide et précise des transactions frauduleuses. Face à la menace persistante que représente la fraude financière, il est essentiel d'adopter des solutions innovantes, capables non seulement d'identifier les fraudes mais aussi de minimiser les faux positifs, limitant ainsi les perturbations pour les utilisateurs légitimes

À travers ce travail, nous avons présenté une approche hybride, intégrant la robustesse d'un modèle de régression logistique avec la puissance d'un réseau de neurones pondéré. Ce cadre théorique, bien que basé sur des modèles classiques et avancés, démontre qu'une combinaison de ces techniques peut potentiellement offrir une solution plus équilibrée face à la complexité des comportements frauduleux.

La partie expérimentale a permis de valider certaines hypothèses initiales, montrant que l'ajustement des seuils et des pondérations peut conduire à une amélioration significative des performances des modèles. Bien que les résultats obtenus restent dans le cadre d'une proposition, ils fournissent une base solide pour des travaux futurs qui pourraient transformer ces concepts en solutions pratiques et opérationnelles.

Enfin, le dernier chapitre a proposé un cadre pour l'intégration et le déploiement de ces modèles dans un environnement réel. Ce travail ouvre des perspectives prometteuses pour le développement de systèmes de détection de fraude plus efficaces, capables de s'adapter aux évolutions constantes du comportement des fraudeurs.

En conclusion, ce mémoire ne se contente pas de présenter des modèles, mais propose également une réflexion sur leur implémentation et leur adaptation dans le monde réel.

Si les défis sont nombreux, les pistes explorées offrent des solutions viables pour renforcer la sécurité des transactions financières, dans un contexte où la fraude continue d'évoluer et de se sophistiquer. Le chemin parcouru dans ce mémoire pose les jalons d'une lutte plus efficace contre la fraude, soulignant l'importance d'une approche à la fois rigoureuse et adaptable.

En poursuivant cette réflexion, il est essentiel de souligner que la lutte contre la fraude ne peut jamais être totalement statique. Le paysage de la fraude évolue rapidement, avec des fraudeurs qui adaptent continuellement leurs techniques pour contourner les systèmes de sécurité. C'est pourquoi, dans ce mémoire, l'accent a été mis non seulement sur le développement de modèles performants, mais aussi sur leur capacité à évoluer et à s'adapter aux nouvelles menaces.

Le cadre théorique et pratique proposé dans ce mémoire pourrait servir de base à des implémentations futures qui nécessiteront non seulement des ajustements technologiques, mais aussi une réflexion stratégique constante. L'intégration d'approches hybrides, telles que la combinaison de la régression logistique et des modèles pondérés, apparaît comme une voie prometteuse pour répondre aux défis actuels tout en laissant la porte ouverte à des améliorations futures.

Ainsi, ce travail se veut une invitation à continuer d'explorer et de tester ces modèles dans des contextes réels, en les affinant au fil du temps pour qu'ils restent à la pointe de la détection de fraude. De plus, il met en lumière l'importance de la collaboration entre les chercheurs, les ingénieurs, et les praticiens du secteur pour traduire les avancées académiques en solutions pratiques et efficaces sur le terrain.

En somme, ce mémoire propose une fondation solide sur laquelle d'autres travaux pourraient s'appuyer pour renforcer encore davantage les défenses contre le blanchiment d'argent et le financement du terrorisme. Les conclusions tirées ici ne sont pas une fin en soi, mais un point de départ pour des recherches et des développements futurs, qui devront être menés avec la même rigueur et le même souci d'innovation.

C'est dans cet esprit de continuité et d'amélioration continue que se clôture ce mémoire, avec l'espoir que les idées et les méthodes présentées ici puissent contribuer, à terme, à une meilleure protection des systèmes financiers contre les différentes menaces. J'espère que ce travail contribuera à enrichir les discussions et les recherches futures dans ce domaine.

Bibliographie:

Kaggle. (2024). *Credit Card Fraud Detection*. Kaggle Dataset. Retrieved from https://www.kaggle.com/mlg-ulb/creditcardfraud

Ali, A., Razak, S. A., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., Elhassan, T., Elshafie, H., & Saif, A. (2022). Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review. Journal of Risk and Financial Management, 15(2), 81. doi:10.3390/jrfm15020081

Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2015). Credit Card Fraud Detection and Concept-Drift Adaptation with Hierarchical Ensemble Learning. *2015 IEEE Symposium Series on Computational Intelligence*, 2015, 255–262. doi:10.1109/SSCI.2015.48

Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. Springer.

Schmidhuber, J. (2015). Deep Learning in Neural Networks: An Overview. *Neural Networks*, 61, 85-117. doi:10.1016/j.neunet.2014.09.003