



THEME DU MEMOIRE

**UTILISATION DE L'INTELLIGENCE ARTIFICIELLE POUR LA  
DETECTION DE FRAUDE BANCAIRE : CAS DE LA FRAUDE  
SUR LES TRANSACTIONS EN LIGNE**

Mémoire en vue de l'obtention du diplôme de:  
**Licence en Intelligence Artificielle et Big Data**

Présenté par :

**ESIMINGANA EDOU Robert Franck**

Encadreur Académique:

**M. ABDOURAMAN DALIL**

Encadreur Professionnel:

**M. FOADING Boris**

**Yaoundé, Cameroun**

**Année-académique: 2022-2023**

## RESUME

Avec l'essor du commerce électronique et l'augmentation du nombre de transactions en ligne depuis le début de la pandémie COVID-19, la préoccupation majeure dans le domaine de la fintech <sup>1</sup> concerne la fraude liée aux transactions en ligne. Selon de nombreuses estimations, les pertes mondiales dues à la fraude en ligne devraient atteindre 6 milliards de dollars d'ici 2025, ce qui dénote de l'ampleur du problème auquel font face les institutions financières et les utilisateurs. En effet, les fraudeurs utilisent des mécanismes de plus en plus complexes, tels que l'usurpation d'identité et la création de faux sites web, ce qui rend leur détection de plus en plus ardue pour les systèmes traditionnels de détection.

Dans ce travail de recherche, nous proposons une approche basée sur l'application des techniques d'intelligence artificielle afin de détecter efficacement les cas de fraude. D'une part, nous concevons un modèle d'apprentissage supervisé capable de classer les transactions comme frauduleuses ou non. Les résultats obtenus démontrent que notre modèle parvient à prédire les cas de fraude avec une précision de 99%, après un entraînement sur un jeu de données équilibré.

Étant donné que les cas de fraude représentent moins de 1% du nombre total de transactions, nous adoptons une autre approche basée sur un modèle de détection d'anomalies en utilisant l'algorithme d'apprentissage non supervisé One-Class SVM. Cette approche nous permet d'identifier les différents groupes présentant des comportements suspects.

**Mots clés : apprentissage supervisé, apprentissage non supervisé, anomalie, étiquette, cluster, optimisation et modèle.**

---

<sup>1</sup> (Technologie financière) désigne l'ensemble des nouvelles technologies dont l'objectif est d'améliorer l'accessibilité ou le fonctionnement des activités financières – source Wikipédia

## **ABSTRACT**

With the increase in online transactions since the beginning of the COVID-19 pandemic and the rise of e-commerce, fraud in online transactions has become a major concern in the fintech industry. According to various estimates, global losses due to online fraud are projected to reach \$6 billion by 2025. This demonstrates the magnitude of the problem faced by financial institutions and users, as the mechanisms used by fraudsters, such as identity theft and the creation of fake websites, are becoming increasingly difficult to detect by traditional detection systems.

In this research work, we propose an approach based on the application of AI techniques to effectively detect cases of fraud. Firstly, we design a supervised learning model capable of classifying transactions as fraudulent or non-fraudulent. The obtained results show that our model can predict fraud cases with an accuracy of 99% after training on a balanced dataset.

Since fraud cases represent less than 1% of the total number of transactions, we adopt another approach based on an anomaly detection model using the unsupervised learning algorithm One-Class SVM. This allows us to identify different groups exhibiting suspicious behavior.

**Keywords: supervised learning, unsupervised learning, anomaly, label, cluster, optimization, and model."**

# SOMMAIRE

|  |     |
|--|-----|
| RESUME .....   | i   |
| ABSTRACT.....  | ii  |
| SOMMAIRE .....   | iii |
| TABLES DES FIGURES .....   | iv  |
| LISTES DES ABREVIATIONS .....  | v   |
| INTRODUCTION GENERALE .....  | 1   |
| 1.Contexte générale de l'étude .....                                   | 1   |
| 2.Problématique de l'étude .....                                       | 2   |
| 3.Hypothèse de l'étude .....   | 3   |
| 4.Objectif de l'étude .....  | 4   |
| 5.justification de l'étude .....                                       | 5   |
| 6.Délimitation de l'étude .....  | 5   |
| 7.Plan du mémoire.....   | 6   |
| CHAPITRE I : CADRE CONCEPTUEL ET THÉORIQUE .....                       | 7   |
| 1.1. Cadre théorique.....  | 7   |
| 1.2. Historique.....   | 9   |
| 1.3. Cadre réglementaire .....   | 10  |
| CHAPITRE II : MÉTHODOLOGIE DE RECHERCHE .....                          | 13  |
| 1.Nature de la recherche .....   | 13  |
| 2.Variables de recherche.....  | 13  |
| 3.Outils de recherche .....  | 18  |
| CHAPITRE III : PRÉSENTATION DU SITE ET DES DONNEES COLLECTEES .....    | 21  |
| 1.Présentation de l'entreprise.....                                    | 21  |
| 2.Données collectées .....   | 25  |
| CHAPITRE IV : ANALYSE & DIAGNOSTIC ET PROPOSITION D'INTERVENTION ..... | 28  |
| 1.présentation et analyse de la situation .....                        | 28  |
| 2.intervention proposée et justification.....                          | 30  |
| 3.Objectif de l'intervention – projet envisagé .....                   | 30  |
| 4.composante de l'intervention.....                                    | 30  |
| 5.stratégie d'action et contenu .....                                  | 31  |
| 6.Conception de l'application.....                                     | 42  |
| 7.Faisabilité .....  | 43  |
| CONCLUSION GENERALE.....   | 45  |

## TABLES DES FIGURES

|  |    |
|--|----|
| Figure 1: l'IA et ses sous-sections .....                      | 14 |
| Figure 2: Types d'apprentissage automatique .....              | 15 |
| Figure 3: Cycle d'un projet de Machine Learning .....          | 17 |
| Figure 4: Structure hiérarchique de Gohze .....                | 24 |
| Figure 5: Dataset de classification .....                      | 26 |
| Figure 6: Dataset pour la Detection D'anomalie .....           | 26 |
| Figure 7: Taux de fraude par type de paiement .....            | 29 |
| Figure 8: preprocessing des données .....                      | 31 |
| Figure 9: processus d'un arbre de décision .....               | 33 |
| Figure 10: Modèle DecionTreeClassifier.....                    | 33 |
| Figure 11: Rapport de classification .....                     | 35 |
| Figure 12: GridSearchCV .....                                  | 35 |
| Figure 13: OverSampling & UnderSampling .....                  | 36 |
| Figure 14:Matrice de confusion du modèle .....                 | 37 |
| Figure 15: Code de la courbe d'apprentissage .....             | 38 |
| Figure 16:Learning Curve.....                                  | 38 |
| Figure 17:Principe du OCSVM .....                              | 39 |
| Figure 18: Code du Setup de PyCaret.....                       | 39 |
| Figure 19: Modèle de détection d'anomalie et prédictions ..... | 39 |
| Figure 20: Umap Plot.....                                      | 40 |
| Figure 21: t-SNE 3D Plot.....                                  | 41 |
| Figure 22: Interface de l'application .....                    | 43 |

## **LISTES DES ABREVIATIONS**

- **CV** : Validation croisée
- **IA** : Intelligence Artificielle
- **ML** : Machine Learning
- **OCSVM** : One-class Support Vector Machine
- **PCA** : Analyse en Composante Principale
- **QML** : Apprentissage Automatique Quantique
- **TIC** : technologie de l'information et de la communication
- **T-SNE** : t-Distributed Stochastic Neighbor Embedding
- **UMAP** : Uniform Manifold Approximation and Projection

## INTRODUCTION GENERALE

L'essor des TIC a considérablement facilité les transactions bancaires en ligne notamment à travers le développement du commerce électronique. Cependant, cela a également ouvert la porte à de nouvelles formes de fraudes, notamment la fraude en ligne. Celle-ci englobe un large éventail de techniques utilisées par les fraudeurs pour accéder aux informations sensibles, usurper l'identité des utilisateurs et effectuer des transactions frauduleuses. Cette menace représente un défi de taille pour les institutions financières et nécessite des mécanismes de détection et de prévention efficaces. C'est dans ce contexte que l'utilisation de l'intelligence artificielle (IA) a émergé comme une solution prometteuse pour détecter et prévenir la fraude bancaire en ligne. En exploitant la puissance de l'apprentissage automatique et de l'analyse de grandes quantités de données en temps réel, l'IA permet d'identifier les activités suspectes et de prendre des mesures préventives pour protéger les utilisateurs et les institutions financières.

L'objectif de ce mémoire est d'explorer en profondeur l'utilisation de l'IA dans la détection de la fraude bancaire en ligne. Nous nous concentrerons en particulier sur des approches basées sur le ML afin de concevoir des modèles prédictifs capables de lutter efficacement contre ce fléau.

### 1.Contexte générale de l'étude

La fraude est une activité illégale et trompeuse dans laquelle une personne ou une entité fait usage de vice ou de manipulation dans le but d'obtenir un gain financier, des biens ou des services d'une manière injuste ou illégale.

On distingue plusieurs types de fraudes parmi lesquelles on peut citer : la fraude à l'assurance, la fraude à l'identité, la fraude fiscale, le schéma de ponzi et la fraude bancaire... Dans ce devoir de recherche nous nous intéressons à la fraude bancaire qui fait référence à un ensemble d'activités illicites visant les institutions financières, les clients ou encore les systèmes financiers. Elle implique très souvent l'usurpation d'identité et d'autres nombreuses techniques de manipulation.

Depuis les années 1980, où les premières escroqueries par cartes de crédit ont vu le jour, jusqu'à nos jours, la fraude bancaire a connu des changements et des avancements technologiques considérables. En effet, dans le cadre actuel de digitalisation<sup>2</sup> croissante des services bancaires, les institutions financières sont confrontées à de nouveaux défis en matière de sécurité et de prévention de fraude. Les avancées technologiques ont non seulement ouvert de nouvelles possibilités pour les consommateurs, mais ont également fourni de nouvelles opportunités aux fraudeurs, qui exploitent les vulnérabilités des systèmes bancaires pour commettre des actes frauduleux, mettant ainsi en péril la stabilité financière et la confiance des clients.

Selon les statistiques, les pertes dues aux fraudes bancaires ont augmenté de façon exponentielle, passant de 9,84 milliards de dollars en 2011 à environ 31,16 milliards de dollars en 2020 (LexisNexis Risk solutions, 2020).

Les méthodes classiques de détection de fraude, telles que les règles prédéfinies et les analyses statistiques, étant presque obsolètes dans la détection des techniques de fraude avancées et le nombre croissant de fraudes en temps réel. Les institutions financières sont donc confrontées au défi de trouver des solutions plus efficaces pour anticiper, détecter et prévenir la fraude.

Ce projet sera implémenté sous forme d'application et intégrera deux principales fonctionnalités :

- ✓ La classification des transactions en frauduleuses ou non à l'aide du ML supervisé
- ✓ La détection d'anomalies en fin d'identifier des groupes de comportements suspects à utilisant le ML non supervisé

## **2.Problématique de l'étude**

### ***2.1. Présentation du problème***

Les institutions financières font face à des défis constants liés à la détection et à la prévention des fraudes dont les techniques et canaux sont en perpétuels évolution. L'IA offre un potentiel prometteur pour relever ces défis en permettant l'analyse et la prédiction des fraudes.

---

<sup>2</sup> Conversion des informations d'un support ou d'un signal électrique en données numériques.

Cependant, plusieurs questions et problèmes subsistent quant à son application dans ce domaine.

## ***2.2. Formulation du problème générale***

De ce qui précède il convient de se poser la question suivante:

- ✓ Comment peut-on améliorer la détection de fraudes bancaire à l'aide de l'IA ?

## ***2.3. Problèmes spécifiques***

Cette interrogation fondamentale soulève les deux préoccupations subsidiaires suivantes :

- ✓ Peut-on appliquer les techniques d'apprentissage supervisé de manière efficace pour analyser et détecter les fraudes en temps réel tout en intégrant la gestion des faux positifs ?
- ✓ Quelles sont les différentes techniques et les modèles d'apprentissage les plus adaptés pour identifier les schémas de fraude et minimiser les pertes financières ?

# **3.Hypothèse de l'étude**

## ***3.1. Hypothèse générale***

L'application de l'IA dans le secteur bancaire, notamment pour l'analyse et la prédiction des fraudes, peut améliorer de manière significative l'efficacité des systèmes de détection, permettant ainsi une réduction substantielle des pertes financières causées par les fraudes et une protection accrue des clients.

### ***3.2. Hypothèse spécifique***

Cette hypothèse fondamentale est susceptible d'être décomposée en deux sous-hypothèses distinctes, à savoir :

- ✓ Une approche basée sur le machine Learning supervisé, nous permet de faire une classification en temps réel des transactions frauduleuses ou non.
- ✓ Une approche basée sur l'apprentissage non supervisé, facilite la détection d'anomalies dans les transactions bancaires.

## **4.Objectif de l'étude**

### ***4.1. Objectif générale***

Cette étude vise à démontrer comment l'utilisation de l'intelligence artificielle peut améliorer l'efficacité des systèmes de détection de fraudes, réduire les pertes financières associées et renforcer la protection des clients et des institutions financières.

### ***4.2. Objectifs spécifiques***

- ✓ Exploiter la puissance des algorithmes d'apprentissage supervisé, pour concevoir un modèle de classification capable d'identifier avec précision les transactions potentiellement frauduleuses.
- ✓ Concevoir et mettre en place un modèle de détection d'anomalies, capable d'identifier les schémas comportementaux relatifs aux potentiels fraudeurs.

## **5.justification de l'étude**

Cette étude présente un double intérêt majeur, à la fois sur le plan scientifique et pratique, en se penchant sur l'application de l'intelligence artificielle dans la détection et la prédiction des fraudes dans le secteur bancaire nous pouvons dire, qu'elle contribuera à l'élargissement des connaissances et des avancées dans ce domaine spécifique de la recherche en intelligence artificielle et en sciences des données. En évaluant les performances des différentes approches d'IA existantes, nous pourrions recueillir des informations précieuses sur leur précision et leur capacité à identifier des schémas frauduleux complexes et en constante évolution. Ces résultats fourniront ainsi une base solide pour l'amélioration continue des modèles et des algorithmes existants dans ce domaine spécifique de la recherche en intelligence artificielle.

Du point de vue pratique, cette étude revêt une grande importance pour les institutions financières, car elle offre des solutions concrètes pour renforcer leurs mécanismes de détection des fraudes. En utilisant l'intelligence artificielle, nous pouvons accroître considérablement l'efficacité de la détection précoce des fraudes, ce qui permettra de réduire les pertes financières associées. Les résultats de cette étude, ainsi que les recommandations qui en découlent, serviront d'une part, de guide pratique pour les institutions financières qui souhaitent mettre en place des systèmes basés sur l'intelligence artificielle pour lutter contre les fraudes et d'autre de renforcer la confiance des clients et des institutions financières envers ces nouvelles technologies en fournissant des preuves tangibles de leur efficacité dans ce domaine.

## **6.Délimitation de l'étude**

Cette étude se limite à l'utilisation des techniques de ML existantes afin de prédire les fraudes sur les transactions en ligne dans le secteur bancaire et ne vise pas à développer de nouveaux algorithmes.

## **7. Plan du mémoire**

Cette étude se compose de quatre chapitres. Le premier chapitre aborde les notions liées au cadre conceptuel et théorique. Le deuxième chapitre se concentre sur la méthodologie de l'étude, en incluant les définitions des termes clés ainsi que la présentation des outils et des méthodes utilisés dans la réalisation du projet. Le troisième chapitre est exclusivement consacré à la présentation de l'entreprise faisant l'objet de l'étude ainsi qu'à la description des ensembles de données recueillis. Enfin, le dernier chapitre présente une analyse de la situation et l'implémentation des solutions proposées, en passant par l'évaluation des résultats obtenus.

# CHAPITRE I : CADRE CONCEPTUEL ET THÉORIQUE

## Introduction

Chaque étude conceptuelle, aussi singulière soit-elle, s'inscrit nécessairement dans un cadre sémantique. De nombreux chercheurs se sont penchés sur le potentiel de l'intelligence artificielle afin de l'exploiter dans la lutte contre la fraude. Ce chapitre fera d'une part l'état de l'art des applications existantes de l'intelligence artificielle dans la lutte contre la fraude en présentant les méthodes employées ainsi que les résultats obtenus et d'autre part il présentera la chronologie de l'intégration de l'IA dans les systèmes de détection de fraude.

### *1.1. Cadre théorique*

Dans le domaine de la lutte contre la fraude, l'utilisation de l'intelligence artificielle a montré des avancées significatives. Les solutions basées sur l'IA pour la détection et la prévention des fraudes utilisent plusieurs techniques, dont : l'analyse des comportements, l'analyse des transactions, l'évaluation des risques et l'apprentissage automatique.

C'est ainsi que plusieurs approches ont été adoptées pour améliorer la précision des systèmes de détection de fraudes. Par exemple, l'utilisation de l'apprentissage supervisé permet de classer les transactions en frauduleuses ou non en se basant sur des modèles préalablement entraînés sur des données étiquetées. De même, des modèles d'apprentissage non supervisé sont utilisés pour détecter les anomalies dans les données et identifier ainsi les transactions potentiellement frauduleuses. La revue littéraire présentée ci-dessous est issue de plusieurs auteurs qui ont menés des études sur la problématique posée notamment sur des thèmes tels que :

- ✓ L'application de l'IA dans la détection d'anomalies
- ✓ La classification des transactions à l'aide de l'apprentissage automatique

La détection d'anomalies en data science consiste à repérer les observations ou les événements divergent significativement de la norme dans un ensemble de données. Son but est d'identifier les données inhabituelles, atypiques ou aberrantes par rapport à la majorité. Cette procédure

s'avère utile pour détecter des comportements rares, suspects ou potentiellement dangereux qui nécessitent une attention particulière. De nombreux chercheurs se sont penchés sur cette technique pour lutter efficacement contre la fraude, comme le data scientist Sanket Sawarde, qui a mené une étude visant à détecter les anomalies dans la fraude par carte de crédit. Dans cette étude, il utilise un ensemble de données de transactions par carte de crédit pour créer une base de référence du comportement normal d'un client. Cet ensemble de données contient un total de 284 807 transactions effectuées par des clients européens en septembre 2013, dont 492 sont des fraudes, soit 0,17% du total. Ensuite, il applique des algorithmes d'apprentissage automatique tels que le SVM à classe unique, qui est un algorithme de détection d'anomalies basé sur le concept d'hyperplans à marge maximale. Ce modèle fonctionne en créant un hyperplan qui sépare les points de données normaux des anomalies, en identifiant les points qui se trouvent du mauvais côté de l'hyperplan comme des anomalies. Ainsi, il peut identifier toutes les transactions qui s'écartent considérablement de cette ligne de base et les signaler comme potentiellement frauduleuses. Les résultats de cette étude sont bien plus que satisfaisants, car le modèle basé sur le SVM à classe unique a permis de détecter le nombre d'anomalies avec une précision de 99,7% (Sawarde, sanket, 2023).

Il existe aussi des logiciels, comme SAS Fraud Management qui est un logiciel de détection de fraude intégrant des fonctionnalités d'IA pour analyser les schémas et les comportements suspects, afin d'identifier et de prévenir les infractions financières.

Toujours dans la même optique la société Mastercard met en œuvre des modèles prédictifs basés sur l'IA pour analyser les schémas de transactions et détecter les comportements frauduleux. Ces modèles utilisent des algorithmes d'apprentissage automatique pour identifier les activités suspectes en comparant les transactions en temps réel avec des normes de comportement préétablies. Ce qui a permis de réduire de moitié le nombre de moitié le taux de transactions injustement refusées.

En se penchant sur la classification des transactions à l'aide du ML, de nombreux logiciels de lutte contre la fraude ont intégré cette fonctionnalité à fin d'offrir une protection proactive contre les activités illicites. C'est le cas de IBM Safer Payments qui utilise l'apprentissage automatique pour analyser en temps réel les transactions et détecter les activités frauduleuses potentielles, aidant ainsi les institutions financières à prévenir les pertes financières liées à la fraude. Cette solution d'IA comprend des fonctionnalités spécifiques pour protéger les cartes,

la banque en ligne et les paiements en temps réel. Profils comportementaux et flux de paiement à travers tous les canaux pour réduire les faux positifs.

Toujours dans le but de prédire la fraude un groupe de chercheurs dont Nouhaila Innan, Muhammad Al-Zafar et Mohamed Bennai, dans une étude comparative de quatre modèles d'apprentissage automatique quantique (QML), réalisée pour la détection de la fraude dans la finance. A prouvé que le modèle de classificateur vectoriel de support quantique a obtenu les meilleures performances, avec des scores F1 de 0,98% pour les classes fraude et non-fraude. D'autres modèles tels que le classificateur quantique variationnel, le réseau neuronal quantique estimateur (QNN) et le QNN échantillonneur démontrent des résultats prometteurs, propulsant le potentiel de la classification QML pour les applications financières (Nouhaila Innan, Muhammad Al-Zafar et Mohamed Bennai, 2023).

## *1.2. Historique*

Les origines de l'IA remontent aux années 1950, lorsque le mathématicien Alan Turing se posait la question de savoir si les machines pouvaient penser. En 1956, le terme "IA" aurait été inventé par John McCarthy du MIT<sup>3</sup>. Cette même année, une conférence sur l'IA a eu lieu à Dartmouth College, rassemblant des chercheurs de différents domaines pour discuter des possibilités d'implémentation de l'IA.

Dans les années 1960, l'engouement pour l'IA retombe car les machines disposaient de très peu de mémoire, rendant mal aisé l'utilisation d'un langage informatique. Le développement de l'IA entre donc en hibernation.

C'est avec l'avènement des premiers microprocesseurs fin 1970 que l'IA reprend un nouvel essor et entre dans l'âge d'or des systèmes experts qui sont des programmes informatiques qui utilisent des connaissances spécifiques pour résoudre des problèmes dans un domaine particulier. La voie avait été en réalité ouverte au MIT dès 1965 avec DENDRAL (système expert spécialisé dans la chimie moléculaire) et à l'université de Stanford en 1972 avec MYCIN (système spécialisé dans le diagnostic des maladies du sang et la prescription de médicaments). Cependant, la programmation de telles connaissances demandait beaucoup d'efforts et à partir de 200 à 300 règles, il y avait un effet "boîte noire" où l'on ne savait plus bien comment la

---

<sup>3</sup> Massachusetts Institute of Technology

machine raisonnait. La mise au point et la maintenance devenaient ainsi extrêmement problématiques et surtout on arrivait à faire plus vite et aussi bien avec d'autres manières moins complexes, moins chères. Il faut rappeler que dans les années 1990, le terme d'intelligence artificielle était presque devenu tabou et des déclinaisons plus pudiques étaient même entrées dans le langage universitaire, comme "informatique avancée".

Le succès en mai 1997 de Deep Blue (système expert d'IBM) au jeu d'échecs contre Garry Kasparov concrétise 30 ans plus tard la prophétie de 1957 d'Herbert Simon mais ne permettra pas de soutenir les financements et les développements de cette forme d'IA. Le fonctionnement de Deep Blue s'appuyait en effet sur un algorithme systématique de force brute, où tous les coups envisageables étaient évalués et pondérés. La défaite de l'humain est restée très symbolique dans l'histoire mais Deep Blue n'était en réalité parvenu à ne traiter qu'un périmètre très limité (celui des règles du jeu d'échec), très loin de la capacité à modéliser la complexité du monde (<https://www.universalis.fr/encyclopedie/deep-blue-superordinateur/>).

Depuis les années 2010, l'IA connaît un nouvel essor qui peut être expliqué par deux facteurs. Tout d'abord, l'accès à des volumes massifs de données a joué un rôle clé. Auparavant, il fallait réaliser soi-même un échantillonnage pour utiliser des algorithmes de classification d'images ou de reconnaissance d'objets tels que les chats. Aujourd'hui, une simple recherche sur Google permet de trouver des millions de données disponibles. Ensuite, la découverte de l'efficacité remarquable des processeurs de cartes graphiques des ordinateurs a accéléré le calcul des algorithmes d'apprentissage. Avant 2010, le processus itératif pouvait prendre des semaines pour traiter l'ensemble d'un échantillonnage. Les cartes graphiques, capables de réaliser plus de mille milliards d'opérations par seconde, ont considérablement progressé tout en restant financièrement abordables (moins de 1000 euros la carte). (Histoire de l'IA , 2023)

### ***1.3. Cadre réglementaire***

Le cadre réglementaire de l'application de l'intelligence artificielle (IA) dans la lutte contre la fraude bancaire est un domaine en constante évolution. Les avancées technologiques et les préoccupations liées à la sécurité financière et confidentialité des données ont conduit à la mise en place de lois et réglementations spécifiques telles que le Règlement général sur la protection des données (RGPD) de l'Union européenne. Cela implique de garantir que les informations

sensibles des clients sont traitées de manière légale, éthique et sécurisée pour encadrer l'utilisation de l'IA dans ce contexte.

En ce qui concerne les lois spécifiques à l'application de l'IA dans la lutte contre la fraude bancaire, différents pays ont adopté des mesures réglementaires adaptées pour encadrer cette pratique. Il convient de noter que les références précises aux lois peuvent varier selon les juridictions, mais voici quelques exemples courants :

Directive européenne sur les services de paiement (DSP2) : Cette directive impose aux banques et aux fournisseurs de services de paiement d'adopter des mesures de sécurité renforcées, y compris l'utilisation de l'IA pour renforcer la détection de la fraude.

Gramm-Leach-Bliley Act (GLBA) aux États-Unis : Cette loi oblige les institutions financières à mettre en place des mesures adéquates pour protéger les informations personnelles des clients, y compris lors de l'utilisation de technologies comme l'IA dans la lutte contre la fraude.

La loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) au Canada : Cette loi régit la collecte, l'utilisation et la divulgation des informations personnelles. Les banques utilisant l'IA doivent donc respecter ces dispositions lors de la lutte contre la fraude. (Gérard V, 2023)

Les limitations et défis liés à l'application de l'IA dans la lutte contre la fraude bancaire sont également importants à souligner. La technologie de l'IA peut présenter des faiblesses, notamment en termes de biais algorithmique. Il est crucial d'adopter des modèles d'IA équitables et transparents pour éviter toute discrimination involontaire.

De plus, la complexité des modèles d'IA rend souvent difficile la compréhension de leurs décisions, ce qui peut entraîner des défis en matière de responsabilité et de reddition de comptes. Les régulateurs et les institutions financières doivent donc trouver un équilibre entre l'utilisation de l'IA pour lutter contre la fraude et la nécessité de garantir une prise de décision juste et transparente puissent être justifiées en cas de contestation. Cela permet de garantir une meilleure compréhension des processus décisionnels et d'identifier d'éventuels biais.

Enfin, les régulateurs encouragent les institutions financières à mettre en place des mesures de supervision et de gouvernance robustes pour s'assurer que les modèles d'IA utilisés dans la lutte contre la fraude sont rigoureusement testés, surveillés et mis à jour régulièrement. Ces mesures

visent à garantir la fiabilité et l'efficacité des systèmes d'IA, tout en minimisant les risques potentiels.

## **Conclusion**

En récapitulant, ce chapitre a exploré l'exploitation de l'intelligence artificielle (IA) dans la lutte contre la fraude, en mettant l'accent sur les aspects conceptuels et réglementaires, ainsi que sur la chronologie de son intégration au sein des systèmes de détection de fraudes. Il en découle que l'IA joue un rôle essentiel en permettant une détection proactive et une prévention efficace de la fraude, conférant ainsi aux institutions financières la capacité de réduire considérablement le taux de transactions frauduleuses. Toutefois, en réponse aux défis inhérents à la confidentialité des données des clients, une panoplie de lois et de régulations a été instaurée afin d'encadrer rigoureusement son application dans ce domaine. Dans le prochain chapitre, nous exposerons la nature de notre recherche et examinerons de manière approfondie les méthodes et techniques appliquées.

## CHAPITRE II : MÉTHODOLOGIE DE RECHERCHE

### Introduction

Dans l'optique de mener une étude rigoureuse et fiable il est nécessaire de garantir une approche méthodologique solide. La méthodologie de recherche joue un rôle fondamental dans la réalisation d'un projet. Elle permet de guider les différentes étapes de l'étude, de définir les approches, les outils et les techniques utilisés, ainsi que d'assurer la rigueur et la validité des résultats obtenus. Dans ce chapitre, nous allons aborder de manière exhaustive toutes les composantes de cette méthodologie, en mettant d'une part l'accent sur la nature de la recherche, d'autre part nous présenterons les variables utilisées en passant par la définition des concepts clés et pour finir il sera question pour nous d'indiquer les outils et techniques utilisés lors de la réalisation de cette recherche.

### 1.Nature de la recherche

La nature méthodologique de cette recherche s'inscrit dans un cadre perceptuel. Son objectif étant d'expliquer et décrire les variables ainsi que les méthodes et techniques utilisées dans les modèles prédictifs pour ainsi s'assurer d'une bonne compréhension du sujet de cette étude.

### 2.Variables de recherche

L'ensemble de données exploité pour ce devoir de recherche comporte des informations sur 6362620 paiements en ligne. On y retrouve les variables suivantes : le montant de la transaction, le solde du destinataire avant et après la transaction, le solde l'émetteur avant et après la transaction, le type de transaction et l'unité de temps.

## 2.1 Définitions conceptuelles

L'Intelligence Artificielle (IA) est un domaine de l'informatique qui vise à créer des systèmes capables de réaliser des tâches qui nécessitent normalement l'intelligence humaine. L'objectif de l'IA est de développer des machines et des algorithmes capables de percevoir, comprendre, apprendre, raisonner, décider et agir de manière autonome. Les principales sections de l'IA sont : machine Learning, Deep Learning, Natural language processing, computer vision et la Robotique.

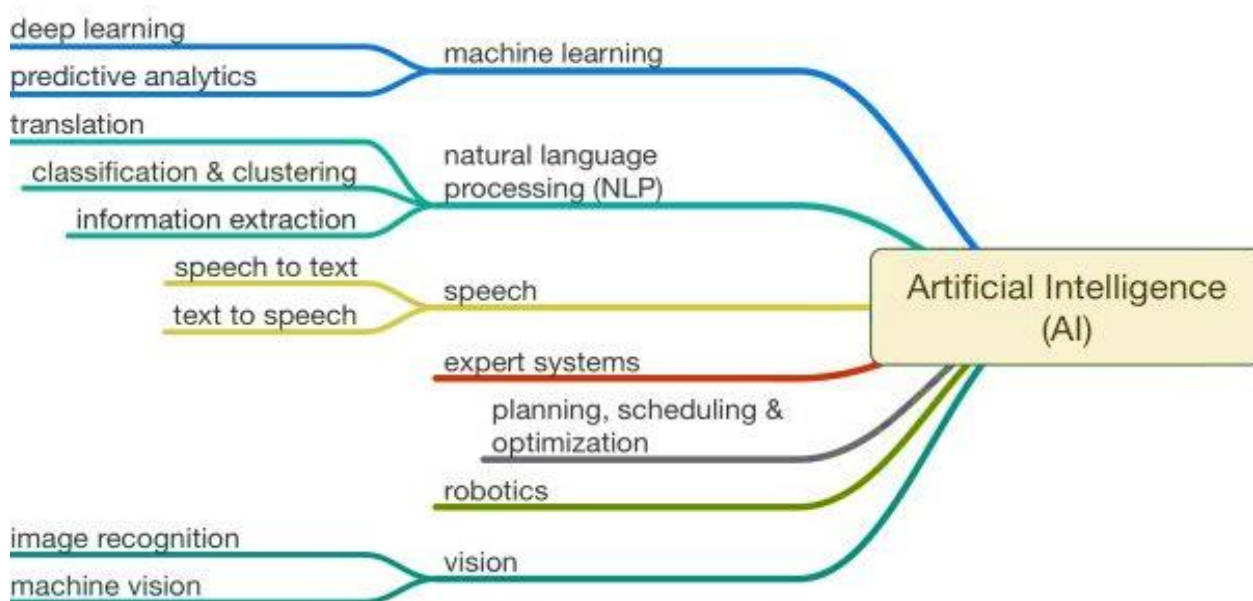


Figure 1: l'IA et ses sous-sections

**Le machine Learning (apprentissage automatique):** est une branche de l'IA qui se concentre sur le développement de techniques permettant aux machines d'apprendre à partir de données et d'expériences, sans être explicitement programmées. Le processus d'apprentissage se fait par l'intermédiaire de la création d'un modèle statistique basé sur des algorithmes qui peut généraliser à partir des exemples fournis. On distingue trois types d'apprentissage automatique :

- ✓ **L'apprentissage supervisé** est un type d'apprentissage durant lequel le modèle s'entraîne sur un ensemble de données étiquetées. Il permet de résoudre des problèmes de régression et classification.

- ✓ **L'apprentissage non supervisé** : dans ce type d'apprentissage le modèle se forme sur des données non étiquetées, dans le but de découvrir par lui-même des motifs cachés ou encore d'extraire des classes ou groupes d'individus présentant des caractéristiques communes.
- ✓ **L'apprentissage par renforcement** : est une branche de l'apprentissage automatique où un agent apprend à prendre des décisions et à prendre des actions dans un environnement afin de maximiser une récompense cumulative. Contrairement à l'apprentissage supervisé, il ne dépend pas de données étiquetées pour apprendre, mais plutôt de l'interaction directe avec l'environnement.

La figure ci-dessous (figure 2) présente les types d'apprentissage automatique, les algorithmes associés ainsi que leur potentielle application.

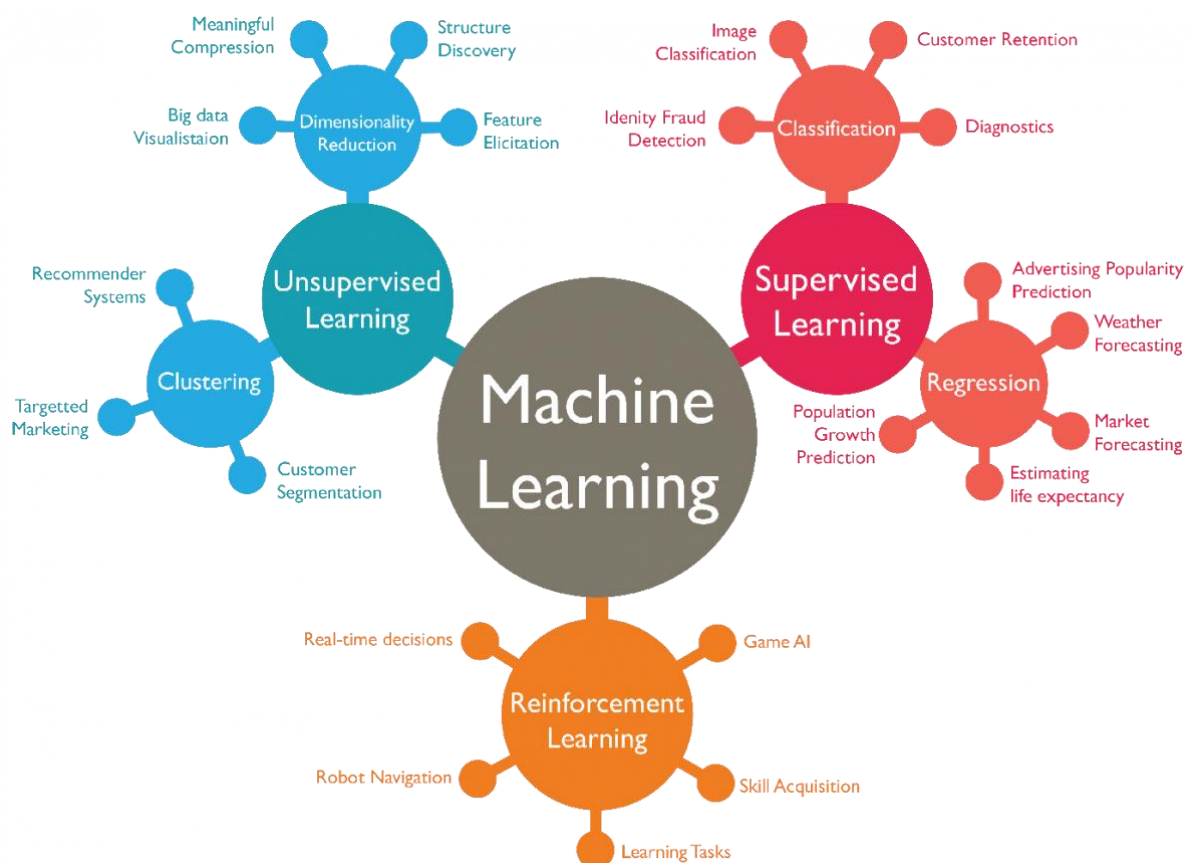


Figure 2: Types d'apprentissage automatique

**Un modèle informatique** : est une représentation mathématique ou statistique des données et des relations qu'elles contiennent. Il s'agit d'un ensemble de paramètres qui permettent au modèle de prendre des décisions ou de faire des prédictions sur de nouvelles données.

Dans cette étude nous avons utilisé deux types d'apprentissage afin de répondre à la problématique posée par le sujet. Tout d'abord l'apprentissage supervisé avec des algorithmes de classification dans le but de déterminer la classe d'une transaction. Ensuite l'apprentissage non supervisé à travers des algorithmes de détection d'anomalies. Pour parvenir à des résultats probants il était nécessaire de suivre un processus clairement défini qui se résume en sept grandes étapes qui sont :

- ✓ **L'acquisition des données :** elle consiste à collecter des données pertinentes pour le problème à résoudre. Celles-ci peuvent être étiquetées ou non.
- ✓ **Le prétraitement des données :** pour rendre exploitables les données brutes par les algorithmes de Machine Learning il est primordial de faire un prétraitement dessus. Cela peut inclure des étapes telles que l'élimination des valeurs manquantes, la normalisation des données, la réduction de la dimension, etc.
- ✓ **Le choix du modèle :** en fonction de la nature du problème et des types de données, il convient de choisir le modèle d'apprentissage approprié.
- ✓ **L'entraînement du modèle :** dans cette étape, le modèle est alimenté avec les données d'apprentissage dans le but de l'ajuster aux caractéristiques et aux patterns présents dans les données.
- ✓ **Évaluation du modèle:** Une fois que le modèle est entraîné, il est évalué sur des données non utilisées pendant l'entraînement pour évaluer ses performances. Cela permet de mesurer sa capacité à généraliser et à faire des prédictions précises sur de nouvelles données.
- ✓ **L'optimisation du modèle :** elle consiste à améliorer les performances du modèle ceci en ajustant ses paramètres internes pour minimiser l'erreur entre les prédictions du modèle et les étiquettes réelles (dans le cas de l'apprentissage supervisé).
- ✓ **Déploiement du modèle :** Une fois le modèle entraîné et évalué, il peut être mis en production pour effectuer des prédictions sur de nouvelles données.

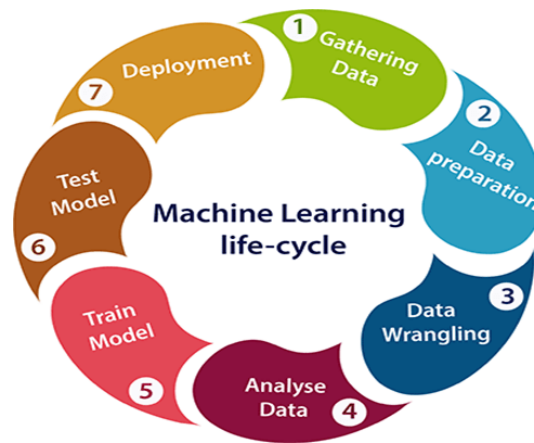


Figure 3: Cycle d'un projet de Machine Learning

**Donnée étiquetée** : est une donnée associée à une étiquette ou classe prédéfinie représentant des informations ou des catégories spécifiques auxquelles elle appartient.

Exemple : Dans le cas de la reconnaissance d'images d'animaux, les images représentent les données, et les étiquettes correspondantes pourraient être "chien", "chat" ou "oiseau".

## 2.2 Limites et difficultés

Lors l'application des modèles prédictifs d'IA dans la lutte contre la fraude on rencontre de nombreuses limites et difficultés notamment :

- **Déséquilibre des classes**

En effet les cas de fraude réelle sont souvent rares par rapport aux transactions légitimes. Cela crée un déséquilibre dans les données utilisées pour l'entraînement des modèles, ce qui peut entraîner un biais et une détection des fraudes moins efficaces.

- **Évolution des techniques de fraude**

Les fraudeurs sont constamment à la recherche de nouvelles méthodes et techniques pour éviter d'être détectés. Cela signifie que les modèles existants peuvent devenir rapidement obsolètes si les techniques de fraude évoluent plus rapidement et par conséquent ils doivent être en constante évolution et adaptés pour suivre les nouvelles tendances de fraude.

- **Vie privée et conformité**

L'utilisation de l'IA dans la lutte contre la fraude implique souvent la collecte et le traitement de données sensibles et personnelles. Il est essentiel de respecter les réglementations en matière de protection des données et de garantir la confidentialité et la sécurité de ces informations tout en utilisant des techniques d'IA appropriées.

- **Faux positifs et faux négatifs**

Les modèles d'IA peuvent parfois générer des faux positifs (détection erronée de fraude) ou des faux négatifs (non détection de fraude réelle). L'équilibre entre ces deux erreurs est un défi important pour s'assurer que la détection de fraude est précise tout en évitant les résultats excessivement conservateurs ou trop permissifs.

### *2.3 Utilisation des variables*

Dans la partie réservée à la classification des transactions en frauduleuses ou non, nous utiliserons des variables comme : le type de transaction, le montant, le solde de l'expéditeur avant et après la transaction ainsi que pour le destinataire, le nombre d'essais de la transaction. Ces données sont présentées dans fichier .csv comportant une étiquette marquant la transaction comme frauduleuse ou non. Ce qui permettra à notre modèle de classification lors de la phase d'entraînement d'identifier les facteurs propres à chaque type de transactions.

Pour la détection d'anomalies, nous utiliserons uniquement les données des variables sans leurs étiquettes que nous ferons passer dans notre modèle afin qu'il puisse faire une distinction entre les points de données normaux des points de données anormaux lors de la phase d'entraînement.

## **3.Outils de recherche**

### **Python**

Qui est un langage de programmation interprété, multi paradigme et multiplateformes. Il favorise la programmation impérative structurée, fonctionnelle et orientée objet. Il est au centre

de la réalisation de ce projet car dispose de toutes les caractéristiques essentielles (bibliothèque, package...), pour mener à bien n'importe quel projet d'intelligence artificielle. La version de python utilisée dans cette recherche est la python 3.11.3 qui présente les fonctionnalités et mise à jour (fr.wikipedia.org, n.d.).

## Visual studio code

Est un IDE extensible développé par Microsoft pour Windows, Linux et macOS. Il intègre des fonctionnalités comme la prise en charge du débogage, la mise en évidence de la syntaxe, la complétion intelligente du code, les snippets, la refactorisation du code et Git intégré. Il est idéal pour la gestion de projet car facilite la création d'environnements et la migration.

## Scikit learn

Est une bibliothèque libre Python destinée à l'apprentissage automatique. Nous l'utilisons dans cette recherche pour des actions comme le prétraitement des données, la séparation des données pour l'entraînement et l'évaluation et aussi pour la construction des modèles.



## Pycaret

Il s'agit d'une bibliothèque d'apprentissage automatique à code source libre en Python qui automatise les workflows (processus) d'apprentissage automatique. Il s'agit d'un outil d'apprentissage automatique et de gestion de modèles de bout en bout qui accélère de manière exponentielle le cycle d'expérimentation et booste la productivité.

## Pandas

C'est une bibliothèque écrite pour le langage de programmation Python permettant la manipulation et l'analyse des fichiers csv sous forme de dataframe. Elle sera utilisée pour manipuler les données recueillies pour cette recherche.

## Numpy

Il s'agit d'une bibliothèque de Python, intégrant des fonctions capables de manipuler des matrices ou tableaux multidimensionnels ainsi que des fonctions mathématiques opérant sur ces tableaux.

## Seaborn

Est une bibliothèque Python de visualisation de données basée sur matplotlib. Elle fournit une interface de haut niveau pour dessiner des graphiques statistiques attrayants et informatifs. Nous l'utiliserons pour visualiser les variables de notre recherche.

## Power Bi

Microsoft Power BI est une solution d'analyse de données de Microsoft. Il permet de créer des visualisations de données personnalisées et interactives avec une interface suffisamment simple pour que les utilisateurs finaux créent leurs propres rapports et tableaux de bord. Il sera utile pour présenter des graphiques relatifs à la fraude et à son impact dans le système financier.

## Streamlit

Est un module Python permettant de créer très simplement et rapidement des applications graphiques multi plateformes sous la forme d'applications web. Ce module est orienté présentation de données et Data Science et constitue donc l'une des pierres angulaires de ce travail de recherche car nous permettra de présenter nos analyses et les résultats obtenus sous forme d'application intégrant de nombreuses fonctionnalités.

## Conclusion

Au terme de ce chapitre axé sur la méthodologie de recherche, nous avons présenté dans un premier temps la nature de la recherche ainsi que les variables utilisées. Dans un second nous avons expliqué les concepts clés en relation à cette étude en passant par une exposition des limites et difficultés liées à son implémentation et pour finir nous avons fait un état des lieux des outils utilisés pour la réalisation de ce projet d'étude.

## CHAPITRE III : PRÉSENTATION DU SITE ET DES DONNEES COLLECTEES

### Introduction

Ce chapitre est constitué de deux grandes parties, dans la première il sera question pour nous de faire une présentation de la structure d'accueil. Ceci sur le plan administratif et organisationnel. Dans la deuxième nous nous attarderons sur les données collectées durant ces mois de stage lors de la réalisation de nos différentes tâches ainsi que les données liées à la réalisation de cette étude.

### 1.Présentation de l'entreprise

#### 2.1 Genèse

GOHZE est une S.A.R.L fondée par 4 ingénieurs de conception en génie informatique de l'institut polytechnique de Yaoundé à savoir : Arnel MANFOUO, Boris FOADING, Raoul Dzoukou et Kevin Tegua. Elle a été immatriculée au N° RC/YAO/2019/B/187 en mars 2019 au nom d'UPGRADE GROUP SARL. Suite à la constatation qu'un grand nombre de jeunes entreprises proposant des services similaires utilisaient des noms communs, nos fondateurs ont pris la décision de se baptiser GOHZE, terme signifiant "upgrade, avancer, aller de l'avant" dans la langue Ghomala<sup>4</sup>. Ainsi, ils ont lancé leurs activités en proposant des produits tels que : OPEN-EXAM ou MOBILE PARTNER. Cependant, avec le temps, les défis financiers sont devenus de plus en plus pesants. Par conséquent, ils ont décidé d'élargir leurs services en incluant des domaines tels que le développement web et autres. De ce fait, ils ont eu l'occasion de collaborer avec des clients prestigieux tels que iziway Cameroun, PWC (PricewaterhouseCoopers) Cameroun, School good, etc. Aujourd'hui, GOHZE, encore en

---

<sup>4</sup>Le ghomala est l'une des 11 langues bamilékés parlées au Cameroun

pleine croissance, possède un unique centre d'implantation mais gère déjà des projets à travers le Cameroun et sur l'ensemble du continent africain

## **2.2 Produits et services**

GOHZE est une entreprise de prestation de services numériques, destinés à promouvoir la transformation digitale et optimiser le fonctionnement. Pour y parvenir l'entreprise propose de nombreux services à savoir :

- ✓ Développement web;
- ✓ Conseil et accompagnement IT;
- ✓ Développement mobile Android/iOS ;
- ✓ Maintenance et hébergement des plateformes ;
- ✓ Design ou remodelage d'interfaces (sites web, application mobile) ;
- ✓ Branding, Design graphique, conception de visuels et supports de communication.

Toujours dans l'optique d'assurer ses nombreuses missions Gohze a mis sur pieds de nombreux produits parmi lesquels on peut citer :

- ✓ **OPEN EXAM** : une plateforme permettant aux élèves d'apprendre de façon efficace et ciblée, grâce à des évaluations sur mesures et optimisées. En leur donnant accès à un contenu de qualité.
- ✓ **UP GESCO** : un ERP développé par GOHZE permettant la gestion optimisée et complète de 06 aspects de l'activité d'une entreprise (la relation client, les finances, la logistique, les ressources humaines et la production).
- ✓ **DSF GENERATOR** : une solution conçue par GOHZE pour assister les entreprises et comptables dans le processus de génération des déclarations statistiques et fiscales (DSF)
- ✓ **MOBILE PARTNER** : cette application offre la possibilité au grand public d'acheter du crédit de communication pour tous les abonnés de tous les réseaux simplement via un moyen de paiement mobile (Orange Money, MTN Mobile Money) ou par carte bancaire (VISA).

- ✓ **GLOBEED** : une plateforme de formation complète en ligne qui a pour mission d'assurer la préparation spécialisée aux concours nationaux et internationaux.

### *2.3 Missions de l'entreprise*

Dans l'optique d'assurer sa pérennité Gohze c'est doté de plusieurs missions qui s'articulent autour de cinq axes principaux à savoir :

- ✓ **Analyse et évaluation des besoins numériques** : Effectuez une analyse approfondie des processus commerciaux, des infrastructures technologiques existantes et des lacunes potentielles dans la transformation digitale de chaque client. Identifiez les domaines où l'adoption de nouvelles technologies ou l'amélioration des systèmes existants peuvent améliorer leur compétitivité.
- ✓ **Stratégie de transformation digitale** : Développez des stratégies de transformation digitale personnalisées pour chaque client, en alignant leurs objectifs commerciaux avec les possibilités offertes par les technologies numériques. Cela peut inclure la mise en place de plateformes de commerce électronique, l'intégration de solutions cloud, l'automatisation des processus...
- ✓ **Développement et mise en œuvre de solutions sur mesure** : Concevoir et développer des solutions logicielles sur mesure qui répondent aux besoins spécifiques de chaque client. Cela peut inclure le développement d'applications mobiles, de systèmes de gestion intégrée (ERP) ou de solutions analytiques pour les aider à prendre des décisions basées sur les données.
- ✓ **Formation et sensibilisation** : Organiser des programmes de formation et de sensibilisation pour les employés des clients afin de les aider à acquérir les compétences nécessaires pour tirer pleinement parti des nouvelles technologies mises en place. Cela peut inclure des sessions de formations sur l'utilisation de logiciels spécifiques, des ateliers sur la cyber sécurité ou des programmes de mentorat pour favoriser une culture de l'innovation.

- ✓ **Suivi et assistance technique continue** : Assurer un suivi régulier avec les clients pour évaluer l'efficacité des solutions mises en place, résoudre les problèmes techniques éventuels et fournir un support continu. Proposez également des services de maintenance préventive pour garantir que leurs systèmes restent à jour et sécurisés.

## 2.4 Structure Organisationnelle

GOHZE est structurée en trois directions (direction technique, direction financière et direction commerciale). La figure ci-dessous nous présente la structure de l'entreprise ainsi que les interactions entre services.

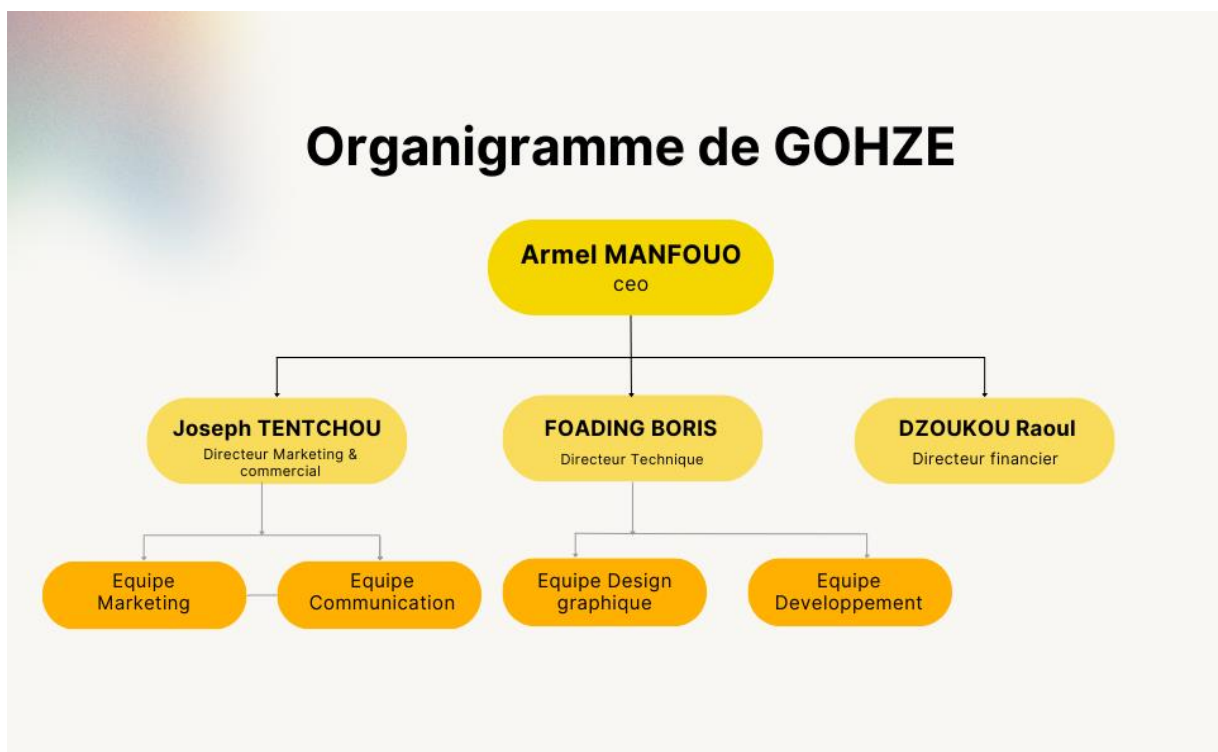


Figure 4: Structure hiérarchique de Gohze

**Note** : les équipes marketing, communication et Design sont principalement constituées de stagiaires ce qui permet à ces derniers d'acquérir une expérience socio-professionnelle.

## 2. Données collectées

Pendant cette période de stage à Gohze, nous avons été sollicités afin de mener à bien diverses missions visant à mettre en pratique nos connaissances acquises et à optimiser le fonctionnement de certains services de l'entreprise en y intégrant des solutions basées sur l'intelligence artificielle. Parmi ces missions, il nous a été demandé de réaliser une série de présentations portant sur l'utilisation des chatbots pour la création de contenu, dans le but d'informer et d'instruire les équipes de la direction marketing et commerciale sur les avantages considérables qu'offre l'application de solutions basées sur l'intelligence artificielle dans leurs domaines respectifs. Une fois ces tâches accomplies, nous avons ensuite procédé à la mise en œuvre concrète de ce projet.

### *2.1 Données pour la classification*

Pour identifier la fraude aux transactions en ligne avec l'apprentissage automatique, nous devons entraîner un modèle d'apprentissage automatique pour classer les paiements frauduleux et non frauduleux. Pour cela, nous avons besoin d'un ensemble de données contenant des informations sur la fraude aux paiements en ligne, afin de comprendre quel type de transactions entraîne la fraude. Pour cette tâche, nous avons collecté un ensemble de données à partir du site Kaggle (<https://www.kaggle.com/datasets/online-payment-fraud-detection>). Qui est une plateforme interactive proposant des jeux de données, compétitions d'apprentissage automatique ainsi que des didacticiels gratuits. L'ensemble de données que nous utilisons ici contient 6362620 (six millions trois cent soixante-deux mille six cent vingt) transactions étiquetées et présente les variables suivantes :

- **Amount** : montant de la transaction
- **NameOrig** : originaire de la transaction
- **Type** : type de de la transaction en ligne
- **NameDest** : destinataire de la transaction
- **OdlbalanceOrg** : solde avant la transaction
- **NewbalanceOrg** : solde après la transaction
- **OdlbalanceDest** : solde du destinataire avant la transaction
- **NewbalanceDest** : solde du destinataire après la transaction

- **Step** : désigne une unité de temps où 1 pas équivaut à 1 heure

| step | type | amount   | nameOrig | oldbalanceOrg | newbalanceOrig | nameDest  | oldbalanceDest | newbalanceDest | isFraud  |   |
|------|------|----------|----------|---------------|----------------|-----------|----------------|----------------|----------|---|
| 0    | 1    | PAYMENT  | 9839.64  | C1231006815   | 170136.00      | 160296.36 | M1979787155    | 0.0            | 0.00     | 0 |
| 1    | 1    | PAYMENT  | 1864.28  | C1666544295   | 21249.00       | 19384.72  | M2044282225    | 0.0            | 0.00     | 0 |
| 2    | 1    | TRANSFER | 181.00   | C1305486145   | 181.00         | 0.00      | C553264065     | 0.0            | 0.00     | 1 |
| 3    | 1    | CASH_OUT | 181.00   | C840083671    | 181.00         | 0.00      | C38997010      | 21182.0        | 0.00     | 1 |
| 4    | 1    | PAYMENT  | 11668.14 | C2048537720   | 41554.00       | 29885.86  | M1230701703    | 0.0            | 0.00     | 0 |
| 5    | 1    | PAYMENT  | 7817.71  | C90045638     | 53860.00       | 46042.29  | M573487274     | 0.0            | 0.00     | 0 |
| 6    | 1    | PAYMENT  | 7107.77  | C154988899    | 183195.00      | 176087.23 | M408069119     | 0.0            | 0.00     | 0 |
| 7    | 1    | PAYMENT  | 7861.64  | C1912850431   | 176087.23      | 168225.59 | M633326333     | 0.0            | 0.00     | 0 |
| 8    | 1    | PAYMENT  | 4024.36  | C1265012928   | 2671.00        | 0.00      | M1176932104    | 0.0            | 0.00     | 0 |
| 9    | 1    | DEBIT    | 5337.77  | C712410124    | 41720.00       | 36382.23  | C195600860     | 41898.0        | 40348.79 | 0 |

Figure 5: Dataset de classification

## 2.1 Données pour la détection d'anomalies

Pour parvenir à identifier des comportements inhabituels il convient de définir une base de comportements normaux. Ceci à travers l'entraînement de notre modèle sur des données historiques pour comprendre les schémas normaux et les comportements attendus. L'ensemble de données collecté pour cette partie est le même que celui utilisé pour la classification à la seule différence que nous avons apporté quelques modifications notamment la suppression de l'étiquette et des colonnes nameOrg et nameDest.

| step | type | amount   | oldbalanceOrg | newbalanceOrig | oldbalanceDest | newbalanceDest |
|------|------|----------|---------------|----------------|----------------|----------------|
| 0    | 1    | PAYMENT  | 9839.64       | 170136.00      | 160296.36      | 0.0            |
| 1    | 1    | PAYMENT  | 1864.28       | 21249.00       | 19384.72       | 0.0            |
| 2    | 1    | TRANSFER | 181.00        | 181.00         | 0.00           | 0.0            |
| 3    | 1    | CASH_OUT | 181.00        | 181.00         | 0.00           | 21182.0        |
| 4    | 1    | PAYMENT  | 11668.14      | 41554.00       | 29885.86       | 0.0            |
| 5    | 1    | PAYMENT  | 7817.71       | 53860.00       | 46042.29       | 0.0            |
| 6    | 1    | PAYMENT  | 7107.77       | 183195.00      | 176087.23      | 0.0            |
| 7    | 1    | PAYMENT  | 7861.64       | 176087.23      | 168225.59      | 0.0            |
| 8    | 1    | PAYMENT  | 4024.36       | 2671.00        | 0.00           | 0.0            |
| 9    | 1    | DEBIT    | 5337.77       | 41720.00       | 36382.23       | 41898.0        |

Figure 6: Dataset pour la Detection D'anomalie

## **Conclusion**

En somme dans ce chapitre nous avons présenté d'une part l'entreprise GOHZE sur le plan technique et organisationnel en passant par l'énumération de ses principales missions. D'autre part nous avons fait une exposition exhaustive des données collectées pour l'implémentation de nos modèles prédictifs dans le chapitre suivant nous ferons une analyse et un diagnostic de la situation ainsi nos solutions envisagées.

## CHAPITRE IV : ANALYSE & DIAGNOSTIC ET PROPOSITION D'INTERVENTION

### Introduction

Une analyse est un processus qui consiste à faire ressortir les éléments propres à expliquer une situation afin d'acquérir une meilleure compréhension. Dans ce chapitre nous ferons tout d'abord une analyse de la situation à travers le décryptage de tableaux de bords et graphes. Ensuite présenterons tout en justifiant l'intervention proposée ceci en décrivant les étapes de réalisation des différents modèles d'apprentissage automatique avec des captures de code source et commentaires à l'appui. Pour finir nous évaluerons les performances de nos modèles ainsi les résultats obtenus en passant par une étude de faisabilité de ce projet.

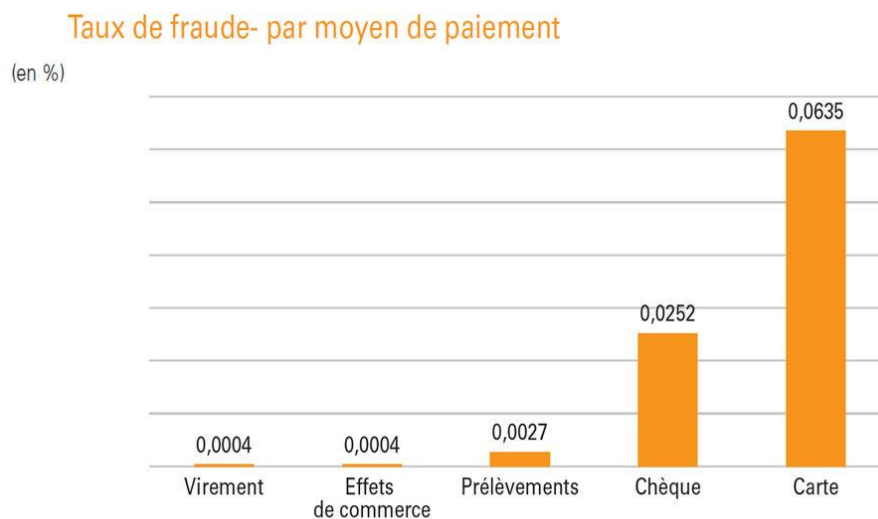
### 1.présentation et analyse de la situation

La fraude en ligne est devenue une préoccupation majeure dans le domaine des transactions numériques notamment avec l'essor du commerce électronique. Selon une étude récente de Cybersecurity Ventures, les pertes mondiales dues à la fraude en ligne devraient atteindre 6 milliards de dollars d'ici 2025. Ce chiffre alarmant démontre l'ampleur du problème auquel sont confrontées les institutions financières et les utilisateurs. Les méthodes de fraude en ligne sont de plus en plus sophistiquées. Par exemple, le phishing, qui consiste à tromper les utilisateurs en se faisant passer pour des entités de confiance, représente une menace majeure. Selon le rapport de l'Anti-Phishing Working Group, le nombre de tentatives de phishing a augmenté de 22 % en 2020 par rapport à l'année précédente.

Une autre méthode couramment utilisée est l'usurpation d'identité. En 2019, le Federal Trade Commission (FTC) des États-Unis a reçu près de 650 000 rapports d'usurpation d'identité liée à des fraudes en ligne. Les conséquences financières de la fraude en ligne sont significatives.

L'Association of Certified Fraud Examiners (ACFE) indique que les entreprises perdent en moyenne 5 % de leurs revenus chaque année en raison de la fraude, dont une grande partie est liée à des activités en ligne.

Pour lutter contre cette menace, les institutions financières investissent désormais dans des solutions de détection d'anomalies basées sur l'intelligence artificielle et l'apprentissage automatique. Une étude de Fraud.net a révélé qu'une approche basée sur l'IA peut réduire les fausses alertes de fraude de plus de 70 %. Car les méthodes conventionnelles présentent des limites telles que le manque de précision, la dépendance humaine et la capacité limitée à traiter de grandes quantités de données.



Source : Observatoire de la sécurité des moyens de paiement.

Figure 7: Taux de fraude par type de paiement

### **Analyse :**

Sur la figure (7) ci-dessus nous pouvons remarquer que le taux de fraude sur les paiements effectués par carte de crédit (0.0635%) est nettement supérieur au cumul de l'ensemble des taux sur les autres types de paiement (0,0252%). En effet depuis le début de la pandémie COVID19 en 2020, on relève une croissance exponentielle du commerce électronique avec l'essor des entreprises comme Amazone, Ali baba, Uber... Ce qui a ouvert la voie à une multitude de techniques de fraudes en lignes. Augmentant considérablement le taux de fraude par carte de crédit car celle-ci constitue le principal moyen de paiement en lignes

## **2.intervention proposée et justification**

L'utilisation des techniques d'intelligence artificielle pour la détection de fraude constitue un domaine de recherche très en vogue. En effet face à la constante évolution des techniques et mécanismes de fraude, les méthodes conventionnelles de détection de fraude présente de nombreuses limites. En utilisant des algorithmes avancés et des modèles prédictifs basés sur l'IA, nous pouvons analyser rapidement et efficacement de grandes quantités de données afin de mieux détecter. Ce qui permettra aux institutions financières d'améliorer leurs systèmes de détection de fraude et par conséquent de réduire les pertes financières liées aux activités frauduleuses.

## **3.Objectif de l'intervention – projet envisagé**

### ***3.1 Objectif Général***

Cette étude vise à démontrer comment l'utilisation de l'intelligence artificielle améliore l'efficacité des systèmes de détection de fraudes bancaire.

### ***3.2 Objectifs spécifiques***

Cette objectif général se décompose en deux objectifs spécifiques. Le premier étant la mise en œuvre d'un modèle d'apprentissage supervisé basé sur des algorithmes de classification permettant de prédire la fraude.

Le deuxième consiste à concevoir un modèle de détection d'anomalies afin d'identifier les comportements anormaux et prévenir les risques de fraudes.

## **4.composante de l'intervention**

Cette partie est principalement une description de la situation actuelle, concernant la fraude en ligne qui nous donne une idée sur les possibilités d'améliorations à long terme des systèmes de détection de fraude en se basant sur des techniques d'intelligence artificielle. L'intervention

envisagée dans cette étude se divise en deux parties : la première est la classification des transactions en frauduleuse ou non à partir d'un modèle d'apprentissage supervisé et la seconde consiste en la détection d'anomalies dans des transactions bancaires afin de prévenir les cas de fraude.

## 5.stratégie d'action et contenu

### 5.1 Conception d'un modèle de Machine Learning pour la prédiction de Fraude

Pour la conception de notre modèle de classification nous avons utilisé la bibliothèque scikit learn qui contient l'ensemble des modules et algorithmes nécessaires pour le prétraitement, l'entraînement, l'évaluation et l'optimisation du modèle. Les étapes de réalisation de ce modèle sont présentées ci-après :

#### 5.1.1 Prétraitement et Analyses des données

**Collecte et préparation des données :** après importé les données collectées dans un fichier notebook, nous avons effectué un prétraitement sur ces données afin de les rendre exploitables par nos algorithmes d'apprentissage. Ce prétraitement comprend la vérification des doublons, des valeurs manquantes (NaN) et l'identification des colonnes catégorielles ceci en utilisant les fonctions de la librairie pandas.

```

#vérification des valeurs nulles
sum = df.isna().value_counts()
print(sum)
[16] ✓ 3.6s Python
...
step    type    amount  nameOrig  oldbalanceOrig  newbalanceOrig  nameDest
dtype: int64

#vérification des doublons
df.duplicated().sum()
[17] ✓ 20.8s Python
...
0

#information sur le dataset
df.info()
[19] ✓ 0.0s Python
...
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 6362620 entries, 0 to 6362619
Data columns (total 11 columns):
#   Column          Dtype
---  -
0   step            int64
1   type            object
2   amount          float64
3   nameOrig        object
4   oldbalanceOrig  float64
5   newbalanceOrig  float64
6   nameDest        object
7   oldbalanceDest  float64
8   newbalanceDest  float64
9   isFraud         int64
10  isFlaggedFraud  int64
dtypes: float64(5), int64(3), object(3)
memory usage: 534.0+ MB

```

Figure 8: preprocessing des données

Note : l'ensemble de données ne contient aucun de NaN et doublons. La commande `df.info ()` nous révèle la présence de 3 colonnes catégorielles.

**Analyse et visualisation des données** : pour visualiser et analyser nos données nous avons utilisé les modules seaborn, matplotlib, numpy et pandas. Pour la partie analyse nous avons affiché les statistiques sommaires avec la fonction describe () et vérifié la distribution entre les classes. Après cela nous avons présenté la matrice de corrélation afin d'identifier les variables à fort coefficient de corrélation.

**Split des données** : après avoir retiré les variables corrélées, nous sommes passé à la séparation aléatoire de nos données en données d'entraînement (Trainset) et données de test (Testset) en utilisant l'algorithme TrainTestSplit du module sklearn. Model\_selection et enfin nous avons standardisé nos données en utilisant la fonction StandardScaler de sklearn. Preprocessing.

### 5.1.2 Construction du modèle

**Description du modèle** : L'algorithme d'apprentissage utilisé pour notre modèle de classification est le DecisionTreeClassifier qui fonctionnent selon une approche de type "if-then-else". Ils utilisent une structure d'arbre pour prendre des décisions basées sur les caractéristiques des données d'entraînement. Voici comment les arbres de décision fonctionnent :

- **Division des données** : L'algorithme de construction de l'arbre commence par le nœud racine, qui contient toutes les données d'entraînement. Il choisit une caractéristique (ou un attribut) sur la base duquel il peut diviser les données en sous-ensembles plus homogènes.
- **Mesure de l'homogénéité** : utilisée pour évaluer la pureté des sous-ensembles créés. L'objectif est de minimiser l'entropie dans chaque sous-ensemble et d'obtenir des groupes homogènes de valeurs similaires pour la variable cible (la classe à prédire). On distingue différentes mesures d'homogénéité, telles que l'indice de Gini ou l'entropie.
- **Création de branches** : L'arbre se développe en créant des branches pour chaque division. Chaque branche correspond à une valeur spécifique de la caractéristique choisie pour la division. Le processus de division et de création de nouvelles branches est répété récursivement pour chaque sous-ensemble jusqu'à ce qu'une condition d'arrêt soit atteinte, par exemple lorsque tous les sous-ensembles sont purs (homogènes) ou qu'une certaine profondeur maximale de l'arbre est atteinte.

- Prédiction : Une fois que l'arbre est construit, il peut être utilisé pour prédire la classe (ou la valeur) cible d'une nouvelle instance en descendant l'arbre en fonction des valeurs de ses caractéristiques. La prévision se fait en suivant les branches correspondantes aux valeurs des caractéristiques jusqu'à atteindre une feuille (nœud terminal) qui contient la prédiction finale.

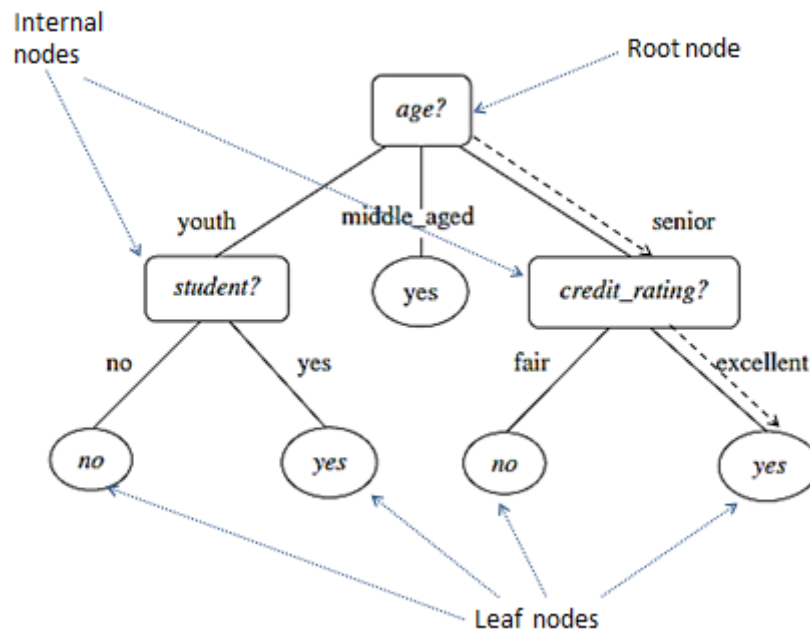


Figure 9: processus d'un arbre de décision

Pour initialiser notre modèle d'arbre de décision nous avons fixé des hyper paramètres tels que la profondeur de l'arbre, la taille minimale des feuilles et la stratégie de découpe ceci pour éviter les overfitting.

```

#Instance du modèle DecisionTreeClassifier
from sklearn.tree import DecisionTreeClassifier
model = DecisionTreeClassifier(criterion = 'gini', max_depth=10, min_samples_leaf = 1, min_samples_split= 8)
[60] ✓ 0.0s Python

#Entraînement du modèle
model.fit(X_train, y_train)
[61] ✓ 1m 4.0s Python

...
DecisionTreeClassifier
DecisionTreeClassifier(max_depth=10, min_samples_split=8)

```

Figure 10: Modèle DecionTreeClassifier

**Evaluation du modèle :** nous avons fait des prédictions en utilisant les données d'entraînement pour évaluer l'efficacité de notre modèle de classification en utilisant des métriques suivantes :

La précision (precision) : mesure le nombre de vrais positifs (observations correctement identifiées) parmi toutes les observations identifiées comme positives par le modèle. Elle indique la capacité du modèle à identifier de manière précise les instances positives. Une précision élevée signifie qu'il y a moins de faux positifs. La formule de la précision est :

$$\text{Précision} = \text{Vrais positifs} / (\text{Vrais positifs} + \text{Faux positifs})$$

Le recall (rappel) : mesure le nombre de vrais positifs parmi toutes les observations réellement positives. Il indique la capacité du modèle à identifier toutes les instances positives. La formule du recall est :

$$\text{Rappel} = \text{Vrais positifs} / (\text{Vrais positifs} + \text{Faux négatifs})$$

Le f1-score : est une mesure de l'équilibre entre précision et recall. Il est calculé comme la moyenne harmonique de la précision et du recall. Le F1-score est utile lorsque vous voulez trouver un équilibre entre la précision et le recall. Il est proche de 1 lorsque la précision et le recall sont tous deux élevés, et proche de 0 lorsque l'un des deux est faible. La formule du F1-score est :

$$\text{F1-score} = 2 * (\text{Précision} * \text{Rappel}) / (\text{Précision} + \text{Rappel})$$

Un rapport de classification est une mesure d'évaluation des performances en apprentissage automatique. Il est utilisé pour montrer la précision, le rappel, le score F1 et la prise en charge de votre modèle de classification entraîné.

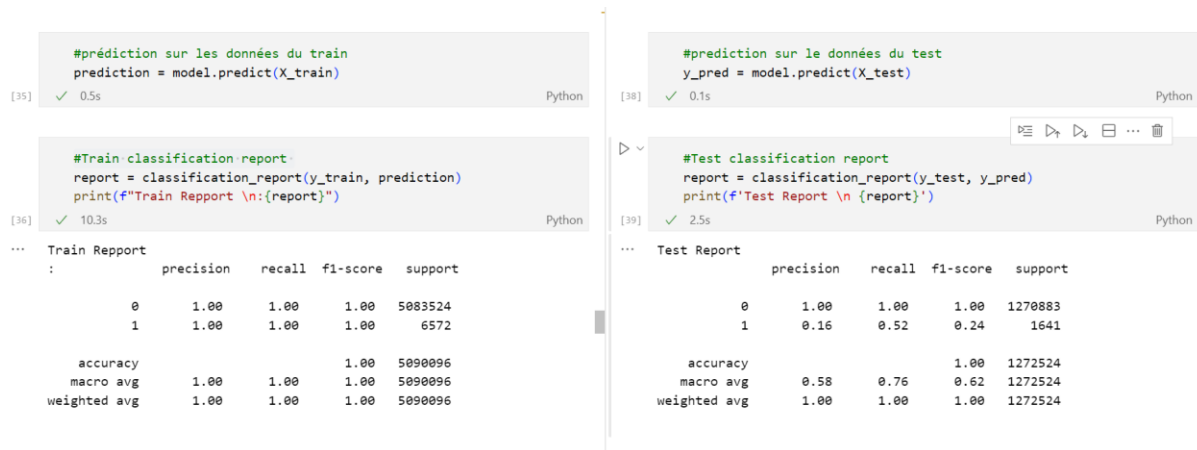


Figure 11: Rapport de classification

L'observation du rapport de classification du train et du test démontre que le modèle s'ajuste parfaitement aux données d'entraînement par contre à du mal à prédire les cas de fraudes sur des nouvelles données avec une précision de 16% et un rappel 52%. Deux facteurs peuvent expliquer ces mauvaises performances notamment le overfitting mais aussi le déséquilibre entre les classes.

Pour l'amélioration des performances de notre modèle, nous avons utilisé GridSearchCV qui consiste à effectuer une recherche exhaustive des hyperparamètres optimaux pour un modèle d'apprentissage automatique. Il évalue toutes les combinaisons possibles d'hyperparamètres spécifiées dans une grille prédéfinie. Pour chaque combinaison, il effectue une validation croisée pour estimer les performances du modèle.

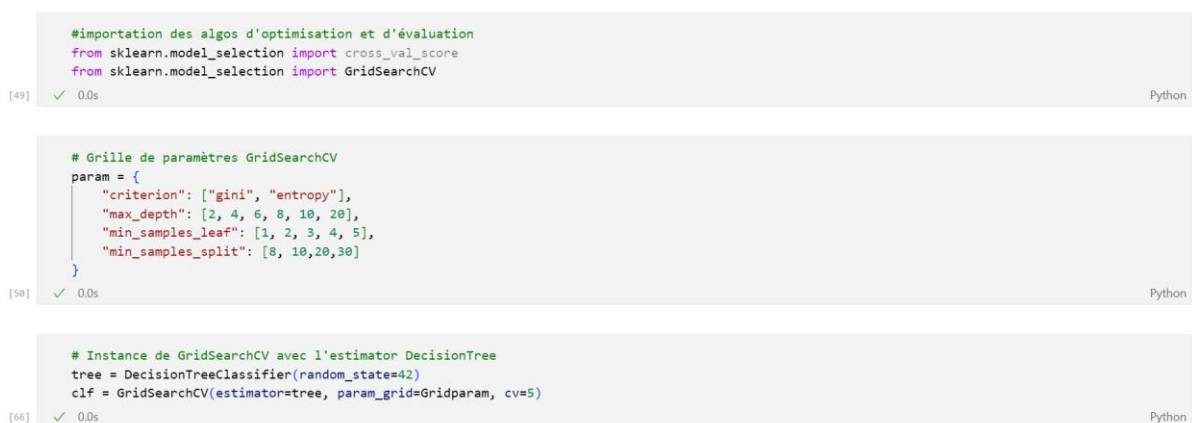


Figure 12: GridSearchCV

Après la phase d'entraînement, nous avons récupéré les hyper paramètres qui optimisent au maximum notre modèle d'apprentissage. Ensuite nous avons fait de nouvelles prédiction sur les données de test et obtenu les résultat ci-dessous :

| Classe         | Precision | Recall | F1-score | support |
|----------------|-----------|--------|----------|---------|
| Non-Fraude (0) | 100%      | 100%   | 100%     | 1270883 |
| Fraude (1)     | 97%       | 39%    | 56%      | 1641    |

Tableau 1: Performances du Modèle après optimisation

Analyse : Nous pouvons dire après observation des résultats ci-dessus que l'optimisation des hyperparamètres<sup>5</sup> de notre modèle a considérablement augmentée ses performances de prédiction. Notamment avec une précision qui passe de 16% à 97% ce qui augmente également le f1-score qui passe à 56%. Néanmoins on note une diminution du recall à 39% ce qui traduit l'incapacité de notre modèle à identifier toutes des instances positives.

Ce biais est principalement causé par le déséquilibre entre les classes. Ce qui nous amène à employer des techniques d'équilibrage de classes sur nos telles que le OverSampling et UnderSampling.

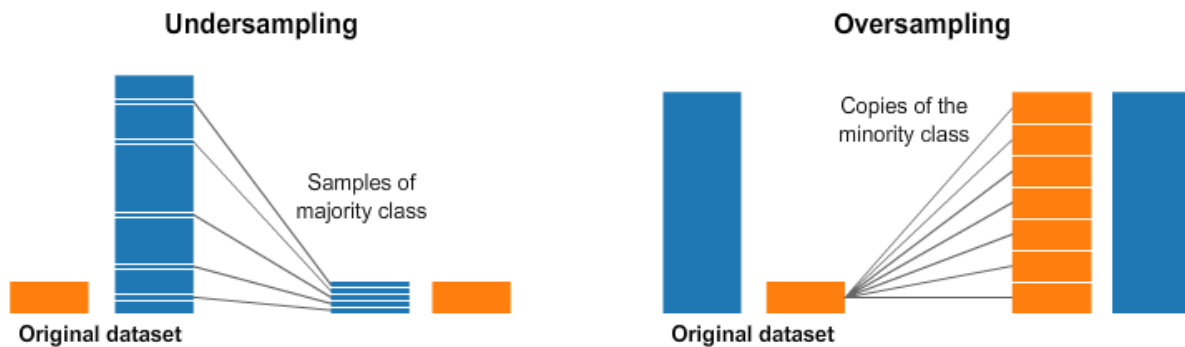


Figure 13: OverSampling & UnderSampling

**Modèle avec équilibre des classes :** pour équilibrer les classes nous avons opté pour le UnderSampling qui consiste à réduire le nombre d'exemples de la classe majoritaire au nombre

<sup>5</sup> Un hyperparamètre est un paramètre dont la valeur est utilisée pour contrôler le processus d'apprentissage

de la classe minoritaire. Dans notre jeu de données, on dénombre 8213 cas de fraude contre 6354407 pour les cas de non-fraude.

### 5.1.3 Résultats du modèle et discussion

Ci-dessous nous avons les résultats du rapport de classification de notre modèle entraîné sur des données équilibrées.

| Classe         | Precision | Recall | F1-score | support |
|----------------|-----------|--------|----------|---------|
| Non-Fraude (0) | 99,4%     | 100%   | 99,7%    | 1630    |
| Fraude (1)     | 100%      | 99%    | 99,5%    | 1630    |

Tableau 2: Performances du modèle avec équilibre entre les classes

Analyse : Nous pouvons observer une nette amélioration des performances de prédiction de notre modèle avec un recall qui passe à 99% pour les cas de fraude. Ce qui prouve que le déséquilibre des classes était la principale cause du biais de notre algorithme.

La matrice de confusion permet de mieux visualiser les résultats des prédictions par rapport aux données réelles, en présentant les prédictions correctes et incorrectes pour chaque classe prédite. La figure (16) nous présente la matrice de confusion de notre modèle de classification.

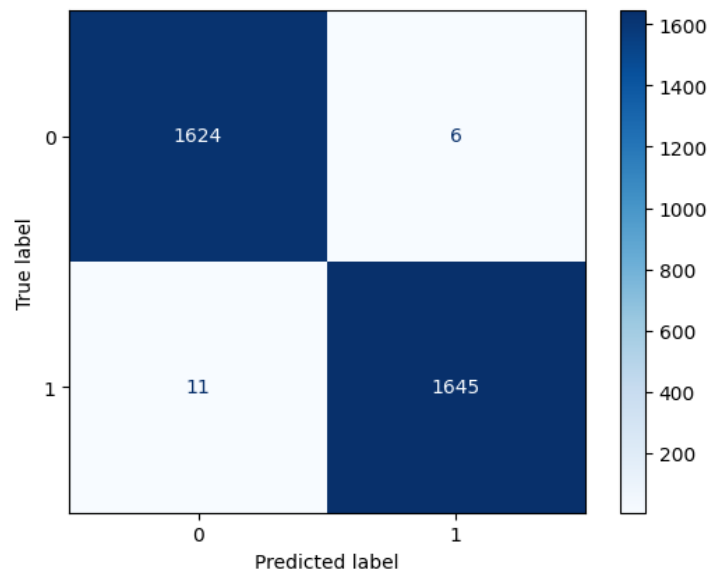


Figure 14: Matrice de confusion du modèle

La courbe d'apprentissage, ou "learning curve" en anglais, est un outil graphique utilisé pour évaluer les performances d'un modèle notamment les cas de sur apprentissage et de sous ajustement en fonction de la taille des données d'entraînement.

```
#affichage de la courbe d'apprentissage
n, train_score, val_score = learning_curve(model, X_train, y_train, cv=5, train_sizes=np.linspace(0.1,1.0,5))
plt.plot(n, train_score.mean(axis=1), label = 'train score')
plt.plot(n, val_score.mean(axis=1), label='validation score')
plt.xlabel('train_sizes')
plt.legend()
[113] ✓ 0.8s Python
```

Figure 15: Code de la courbe d'apprentissage

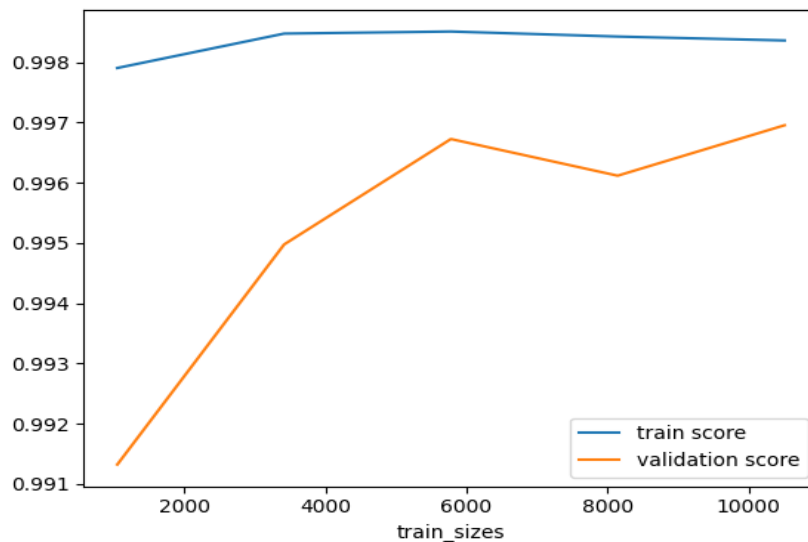


Figure 16: Learning Curve

## 5.2 Conception d'un modèle de Machine Learning pour la détection d'anomalies

### 5.2.1 Description du Modèle

Pour la conception du modèle de détection d'anomalies, nous avons utilisé le OneClassSVM qui est un algorithme d'apprentissage non supervisé. L'objectif principal du OCSVM est de séparer les points de données normaux du reste des données qui peuvent être considérées comme des anomalies, en se basant sur le principe de trouver l'hyperplan qui a la plus grande marge par rapport aux points de données normaux, ainsi les points qui se trouvent à l'extérieur de cette marge sont considérés comme des anomalies. Nous avons spécifié les paramètres  $\gamma$  à 0.1, qui permet d'ajuster la souplesse de la frontière de décision autour des données normales et  $\text{fraction}$  à 0.05, pour indiquer la proportion d'échantillons de données considérés comme des anomalies.

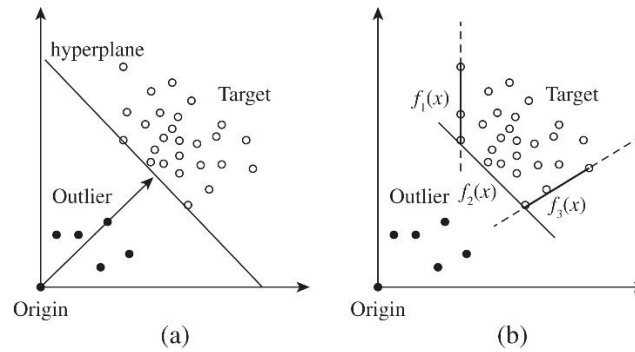


Figure 17: Principe du OCSVM

De plus nous avons décidé d'inclure une normalisation et un PCA (Principal Component Analysis) directement dans le pipeline de prétraitement de pycaret en utilisant la fonction setup.

```

Code Markdown
#pipeline de preprocessing de pycaret
exp = setup(data, normalize=True, pca=True, pca_components=2)
Python
[12] ✓ 14.1s

```

Figure 18: Code du Setup de PyCaret

Dans ce code, nous utilisons `normalize=True` pour réduire nos données à la même échelle et `pca=True` pour effectuer l'analyse en composantes principales (PCA) lors de l'initialisation de l'expérience PyCaret via la fonction `setup`. Le paramètre `pca\_components` spécifie le nombre de composantes principales souhaitées (pour ce modèle, nous utilisons 3 dimensions pour des fins de visualisation).

Ensuite nous avons généré de nouvelles prédictions à partir de notre modèle et de l'ensemble de nos données.

```

#instance du modèle OneClassSVM
ocsvm = create_model("svm", gamma=0.1, fraction=0.05)
Python
[ ]

# Génération des prédictions sur l'ensemble de données
predictions = predict_model(ocsvm, data=data)
Python
[18] ✓ 12m 40.3s

```

Figure 19: Modèle de détection d'anomalie et prédictions

### 5.2.2 Evaluation et Analyses des Résultats

Pour l'évaluation de notre modèle nous avons utilisé la fonction `evaluate_model` de `pycaret` qui permet d'afficher les graphiques présentant les anomalies et les valeurs normales. Notamment le Umap, qui est un type de visualisation utilisé pour réduire la dimension des données afin d'identifier des regroupements. Les distances entre les points dans la projection UMAP reflètent les similitudes locales dans les données d'origine. Les points similaires dans l'espace d'origine auront tendance à être regroupés ensemble dans le plot UMAP.

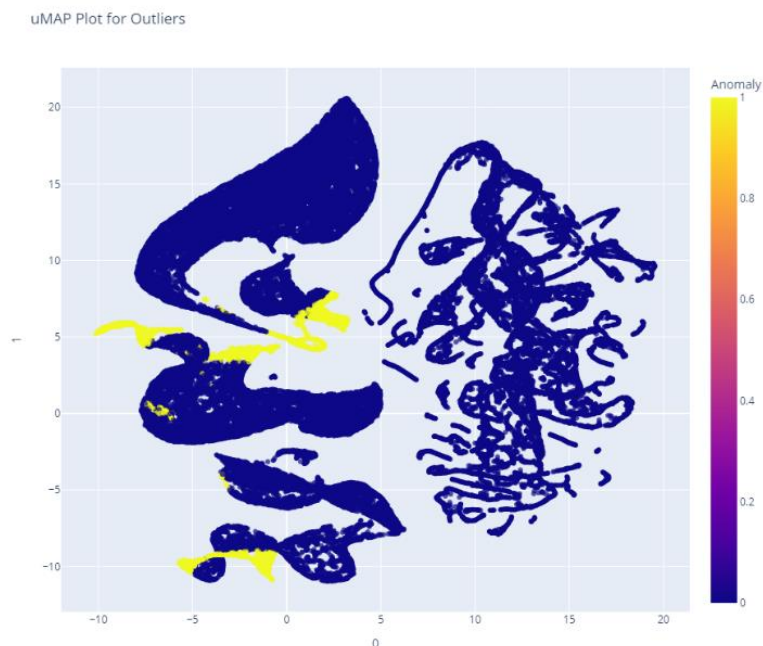


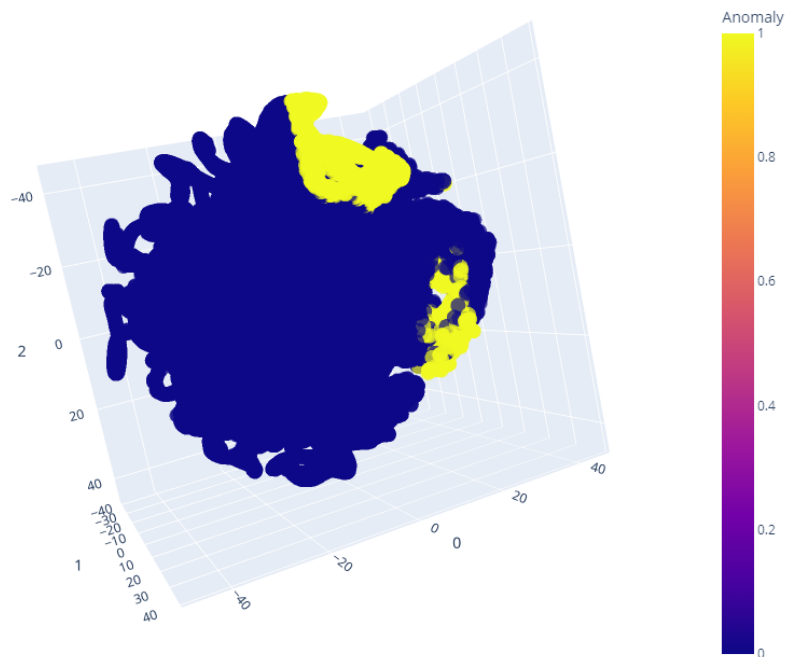
Figure 20: Umap Plot

#### Analyse

La figure (20) présente la répartition en 2 dimensions entre les valeurs normales et anomalies de notre jeu de données. Ainsi nous pouvons observer : plusieurs regroupements de points de données qui peuvent faire référence des clusters significatifs, les groupes de points bleus présentant les données normales et jaunes des anomalies. Cette proximité est due aux similitudes élevées entre ces observations.

Pour une visualisation optimale des différents groupes, nous avons utilisé l'algorithme t-SNE (t-Distributed Stochastic Neighbor Embedding) qui permet de représenter les données dans un espace en trois dimensions, ce qui facilite la visualisation de structures complexes et de relations entre les points de données. Contrairement à la représentation en deux dimensions, la représentation en 3D permet d'afficher des informations supplémentaires dans une troisième dimension.

3d TSNE Plot for Outliers

*Figure 21: t-SNE 3D Plot*

Analyse : la visualisation 3D offerte par le t-SNE plot nous permet d'identifier deux principaux clusters de points similaires d'anomalies ce qui nous permet de faire une distinction des axes des valeurs normales des axes présentant des anomalies.

## 6. Conception de l'application

### 6.1 Description

Pour la conception de l'application, nous avons utilisé la librairie streamlit de python. Elle présente quatre principaux menus :

Le menu Accueil, dans lequel on retrouve une description des différentes fonctionnalités intégrées dans l'application et une brève présentation sur la fraude en ligne et ses mécanismes et quelques recommandations pour éviter d'en être victime.

Le menu Data analysis, qui intègre des fonctionnalités comme la visualisation de l'ensemble des données, l'affichage du tableau des statistiques sommaires et la matrice de corrélation.

Le menu Anomaly Model, qui intègre le code permettant d'afficher le t-SNE 3D pour visualiser les anomalies présentes dans nos données mais aussi un formulaire permettant de faire une prédiction sur des transactions en déterminant s'il s'agit d'une anomalie ou non.

Le menu Classification Model, permet de charger un fichier .csv contenant des informations sur des transactions et de faire des prédictions dessus afin de déterminer s'il s'agit de fraude ou non et intègre une fonction pour télécharger les résultats sous forme de fichier csv.

### 6.2 Réalisation et résultats

Pour avoir accès à la plateforme il faut au préalable effectuer une authentification. Pour y parvenir, nous avons utilisé le module streamlit authenticator qui permet de générer des formulaires de connexion et d'enregistrement et le module Deta qui permet de stocker les informations de connexions des utilisateurs dans une base de données deta assignée à une clé.

Pour le déploiement de nos modèles prédictifs nous avons utilisé le module pickle pour l'interprétation des pipelines de nos modèles qui sont sous forme de fichier *pkl* et les fonctions `load_model` et `model_predict` pour le chargement du modèle et la prédiction sur nos données.

Pour le téléchargement de nos données avec les prédictions en fichier csv nous avons défini une fonction `download_file`, qui prend en paramètre le data frame avec les prédictions et le converti en fichier csv et effectue une conversion binaire.

Ci-dessous nous pouvons voir un aperçu de l'interface d'accueil de notre application ainsi que les différents menus.



Figure 22: Interface de l'application

## 7.Faisabilité

La faisabilité fait référence à l'évaluation de la possibilité de réalisation d'un projet ou d'une activité. Elle implique une évaluation approfondie des aspects techniques, économiques, opérationnels et organisationnels d'un projet pour déterminer s'il est réalisable dans des conditions spécifiques. Dans cette partie nous ferons une évaluation du coût de ce projet sur le plan technique.

| Ressources             | Description                           | Rôle                                       | Coût(FCFA) |
|------------------------|---------------------------------------|--|------------|
| Données                | Pertinentes et en quantité suffisante | L'entraînement des modèles d'apprentissage | 120 000    |
| Système d'exploitation | Windows ou MacOS                      | Pour le déploiement des applications       | 162 000    |

|              |   |                              |                |
|--------------|---|------------------------------|----------------|
| Ordinateur   | CPU 3.53GHz i7,<br>16Go RAM, 500Go<br>SSD | puissance de calcul          | 900 000        |
| Internet     | Haut débit                                | Installation des<br>plugins  | 40 000         |
| Ms PoweBi    | Pro                                       | Pour l'analyse de<br>données | 65520          |
| <b>Total</b> |   |                              | <b>1287520</b> |

Tableau 3: Evaluation du coût du projet en terme de ressource technique

## Conclusion

Dans ce chapitre, nous avons exposé les solutions envisagées afin de pallier à la problématique soulevée par cette recherche. Il en ressort que le modèle de classification obtient des performances remarquables lorsqu'il est entraîné sur un ensemble de données équilibré, se traduisant par un taux de f1-score de 99,5%. Ceci atteste de sa capacité à détecter avec précision toutes les instances positives, tout en minimisant les fausses alertes. En revanche, lorsque les classes sont déséquilibrées, le taux de classification descend à 24%. Quant au modèle de détection d'anomalies, il permet une meilleure appréhension de ce déséquilibre. En effet, son algorithme considère les points de données appartenant à la classe minoritaire comme étant des anomalies, et établit ainsi une démarcation entre ces anomalies et les valeurs normales. Grâce à l'utilisation du graphique t-SNE, nous avons pu identifier deux groupes présentant un comportement anormal, ce qui peut être assimilé à des mécanismes de fraude.

## CONCLUSION GENERALE

Nous voici parvenus au terme de notre recherche qui portait sur : "**L'utilisation de l'intelligence artificielle pour la détection de la fraude bancaire : le cas de la fraude sur les transactions en ligne**". Il en ressort que les progrès et avancées technologiques ont non seulement ouvert la voie au développement du commerce électronique ainsi que du nombre de transactions en ligne mais aussi offert une multitude de possibilités et mécanismes de fraude rendant ainsi les systèmes de détection traditionnelle quasi obsolète. Cette étude soulève l'hypothèse selon laquelle une approche basée sur des techniques d'intelligence artificielle améliore significativement les systèmes de détection de fraude.

Durant notre travail, nous nous sommes fixé comme objectifs de concevoir deux modèles prédictifs basés sur l'apprentissage automatique. Afin de vérifier nos hypothèses énoncées précédemment. Nous avons premièrement opté sur un modèle d'apprentissage supervisé pour prédire les cas de fraudes, en utilisant la méthode classification l'algorithme DecisionTreeClassifier. Le modèle établi a démontré une performance f1-score de 99,5% sur un jeu de données équilibré, comparé à 24% sur des données déséquilibrées.

Pour le modèle d'apprentissage non supervisé, nous avons utilisé le principe l'algorithme OCSVM, qui repose sur un principe d'hyperplan permettant d'établir une zone de décision entre les valeurs normales et anomalies. Cela nous a permis d'identifier deux principaux groupes de fraudeurs au sein de notre ensemble de données.

Cependant ce travail de recherche reste ouvert à diverses extensions. En guise de perspectives, nous envisageons d'améliorer la pertinence et la qualité de notre jeu de données, ce qui permettra d'accroître les performances de nos modèles et d'obtenir une meilleure interprétation des résultats.

## REFERENCES WEBOGRAPHIQUES

- [1] Modèle de détection d'anomalies, <https://www.analyticsvidhya.com/blog/2023/05/ anomaly-detection-in-credit-card-fraud/>
- [2] données sur les transactions en ligne, <https://www.kaggle.com/datasets/online-payment-fraud-detection>
- [3] DecionTreeClassifier, <https://scikit-learn.org/stable/modules/generated/sklearn.tree.DecisionTreeClassifier.html#sklearn.tree.DecisionTreeClassifier>
- [4] confusion-matrix, <https://scikitlearn.org/stable/modules/generated/sklearn.metrics.ConfusionMatrixDisplay.html>
- [5] Learning-Curve, [https://scikit-learn.org/stable/modules/generated/sklearn.metrics.roc\\_curve.html](https://scikit-learn.org/stable/modules/generated/sklearn.metrics.roc_curve.html)
- [6] missions de l'entreprise, <https://gohze.com/>
- [7] Classification report, [https://scikit-learn.org/stable/modules/model\\_evaluation.html#classification-report](https://scikit-learn.org/stable/modules/model_evaluation.html#classification-report)
- [8] GridSearchCV, [https://scikit-learn.org/stable/modules/generated/sklearn.model\\_selection.GridSearchCV.html](https://scikit-learn.org/stable/modules/generated/sklearn.model_selection.GridSearchCV.html)
- [9] One-classe SVM, <https://scikitlearn.org/stable/modules/generated/sklearn.svm.OneClassSVM.html>
- [10] Setup pycaret, <https://pycaret.gitbook.io/docs/get-started/functions/initialize>
- [11] Evaluate model, <https://pycaret.gitbook.io/docs/get-started/functions/analyze>
- [12] Streamlit authenticator, <https://blog.streamlit.io/streamlit-authenticator-part-1-adding-an-authentication-component-to-your-app/>
- [13] Deta Base, <https://docs.streamlit.io/knowledge-base/tutorials/databases/deta-base>

## **REFERENCES BIBLIOGRAPHIQUES**

- [1] Histoire de l'intelligence artificielle — Management Datascience
- [2] Introduction au Machine Learning & data mining
- [3] Intro to Python for Computer Science and Data Science 2022
- [4] Analyse en composantes principales — Wikipédia
- [5] DS\_Rarity Problem in Supervised Fraud Detection Insights Article\_3JUNE20
- [6] Module 3: Evaluating & Interpreting Models, Duke PRATT of ENGINEERING
- [7] Module 5: Trees, Ensemble Models and Clustering, Duke PRATT of ENGINEERING