–

***RAPPORT DE MINI-PROJET DE DEVELOPPEMENT***

* Réalisé par :

- AIT WAHMANE Elhoussaine

- IGAJANE Abdellah

- LACHEGUR Amine

- LAGHFIRI Oussama

- MOUISSET Hamza

**Credit Card Fraud Detection**

* Encadré par :

- Mr. BELMEKKI Abdelhamid

- Mr. KAMAL IDRISSI Hamza

- Mme HANIN Charifa

***REMERCIEMENTS***

Nous tenons à adresser nos sincères remerciements à Mr. BELMEKKI Abdelhamid, envers Mr. KAMAL IDRISSI Hamza et Mme HANINE Charifa pour votre précieuse contribution et votre soutien tout au long de notre projet. Votre expertise, votre disponibilité et vos conseils ont grandement enrichi notre travail et ont contribué à sa réussite.

Tout d'abord, nous souhaitons à exprimer notre reconnaissance envers Mr Abdelhamid BELMEKKI pour son rôle de superviseur. Votre guidance éclairée et vos conseils pertinents nous a permis d'avoir une vision claire et structurée de mon projet.

Nous voudrions également exprimer notre gratitude envers Mr. KAMAL IDRISSI Hamza pour son soutien tout au long de cette aventure. Votre disponibilité pour répondre à nos questions, discuter des idées et fournir des commentaires constructifs ont été d'une grande aide.

Enfin, nous tenons à exprimer nos sincères gratitudes à Mme HANINE Charifa pour sa contribution au projet. Votre expertise et vos conseils précieux ont grandement amélioré la qualité de notre travail et ont contribué à notre apprentissage.

Avec nos remerciements les plus chaleureux.

***ABSTRACT***

In recent years, the use of credit card as payment method has increased exponentially especially with the growth of E-commerce which results the risk of fraud transactions.

This project report explains the credit card fraud detection system using Django framework and artificial intelligence. The main objective of the project is to create an accurate and efficient fraud detection method using multiple algorithms that can identify fraudulent credit card transactions.

The report discusses the performance evaluation of fraud detection algorithms such as Logistic Regression, Random Forest and others by comparing its accuracy and precision in detecting fraudulent transactions.

***TABLE DES MATIERES***

1. **Introduction ……………………………………………..…… 1**
2. **Contexte général du sujet …………………………………… 3**
3. Présentation du sujet …………………………………… 3
4. Solution proposée ……………………………………… 3
5. **Application web (Credit Card Fraud Detection): …………. 4**
6. Structure de l’application ……...……………………… 4
7. Description partie HTML/CSS/JS .................................. 5
8. Principe de fonctionnement …………………………… 10
9. **Algorithmes appliqués ……………………………………. 11**
10. Méthodologie …………………………………………. 11
11. Résultats ………………………………………………. 12
12. Régression Logistique …………………. 12
13. Random Forrest ………………………... 13
14. KNN …………………………………… 14
15. SVM …………………………………… 15
16. Decision Tree ………………………….. 16
17. Résultat de détection de fraude ..................................... 17
18. Conclusion .................................................................... 17
19. **Conclusion ............................................................................... 18**
20. **Bibliographie ............................................................................19**
21. **Introduction :**

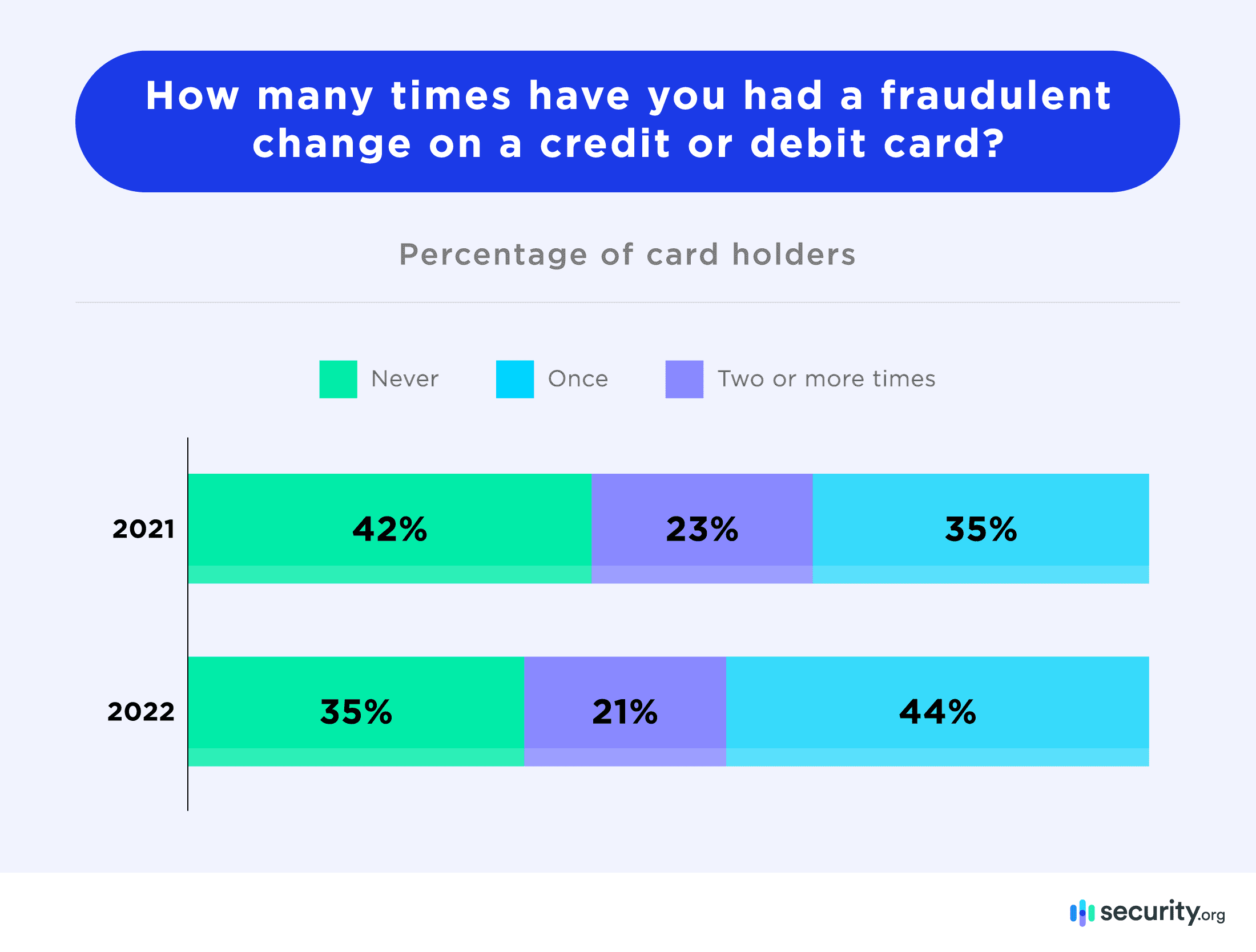
De nos jours, la fraude par carte de crédit est devenue un problème dans le domaine des transactions financières suite à l’augmentation de paiement par carte de crédit qui s’est évalué à 51% de toutes les transactions selon Federal Bank Reserve de San Francisco. L’avènement des technologies digitales et la popularité croissante des paiements par carte de crédit ont donné de nouvelles opportunités aux fraudeurs pour exploiter les vulnérabilités du système.

La fraude par carte de crédit se produit par plusieurs manières :

* Vol de cartes : Il s'agit d'une méthode standard pour commettre une transaction de fraude par carte de crédit où le fraudeur prend possession de la carte et peut directement en abuser.
* Piratage des comptes de messagerie : Les pirates informatiques conçoivent des programmes ou des logiciels pour pirater les comptes de messagerie, car les banques envoient des e-mails aux clients avec des informations sur le compte.
* Scam : Les victimes reçoivent des appels ou des e-mails par des arnaques qui prétendent d’être des employés de banque ou distribuent des faux prix.
* Hameçonnage (Phishing) : Les titulaires de carte peuvent recevoir des messages mobiles ou des e-mails contenant des liens inconnus, qui, s'ils sont cliqués, débiteront directement de l'argent des comptes bancaires, ce qui est une méthode standard pour commettre une fraude par carte de crédit en ligne.
* Écrémage (Skimming) et clonage : De nombreux guichets automatiques bancaires (ATM) ou lecteurs de cartes sont équipés de dispositifs qui copient les informations de la carte dès qu'elles sont glissées, puis utilisées pour concevoir une fausse carte.

Ces actions résultent de multiples conséquences. Les victimes peuvent perdre une somme importante d’argent. Les institutions financières, quant à eux, subissent des pertes graves, et une diffamation. De plus, les consommateurs vont perdre confiance dans les systèmes de paiement par carte de crédit.

Suite au rapport annuel 2021 de l’équipe security.org sur la fraude par carte de crédit, et sont arrivés au résultat suivant :

* 65% des titulaires de carte de crédit en Amérique ont été victimes de fraude à un moment donné de leur vie ce qui est équivalent à environ 151 millions d’Américains.
* Un nombre croissant d’Américains ont été victimes à plusieurs reprises : en 2022, 44% des utilisateurs de cartes de crédit ont déclaré avoir au moins deux débits frauduleux contre 35% en 2021.
* L’accusation médiane a augmenté d’environ 27% qui est équivaut à environ 12 milliards de dollars de tentatives des transactions frauduleuses.
* Les personnes qui stockent les informations de leur carte de crédit dans leur navigateur Web et utilisent la même carte pour le paiement automatique que pour leurs dépenses quotidiennes étaient plus susceptibles d'être victimes.

1. **Contexte général du sujet :**
2. ***Présentation du sujet :***

Afin de lutter contre ce phénomène, les établissements financières et les autorités ont mis en place des mesures de sécurité et des technologies de détection avancées. Cela comprend l’utilisation de modèles d’apprentissage automatique et d’algorithmes pour détecter les schémas frauduleux, l’analyse des données en temps réel et la mise en place de protocoles de sécurité stricts pour protéger les données sensibles des clients.

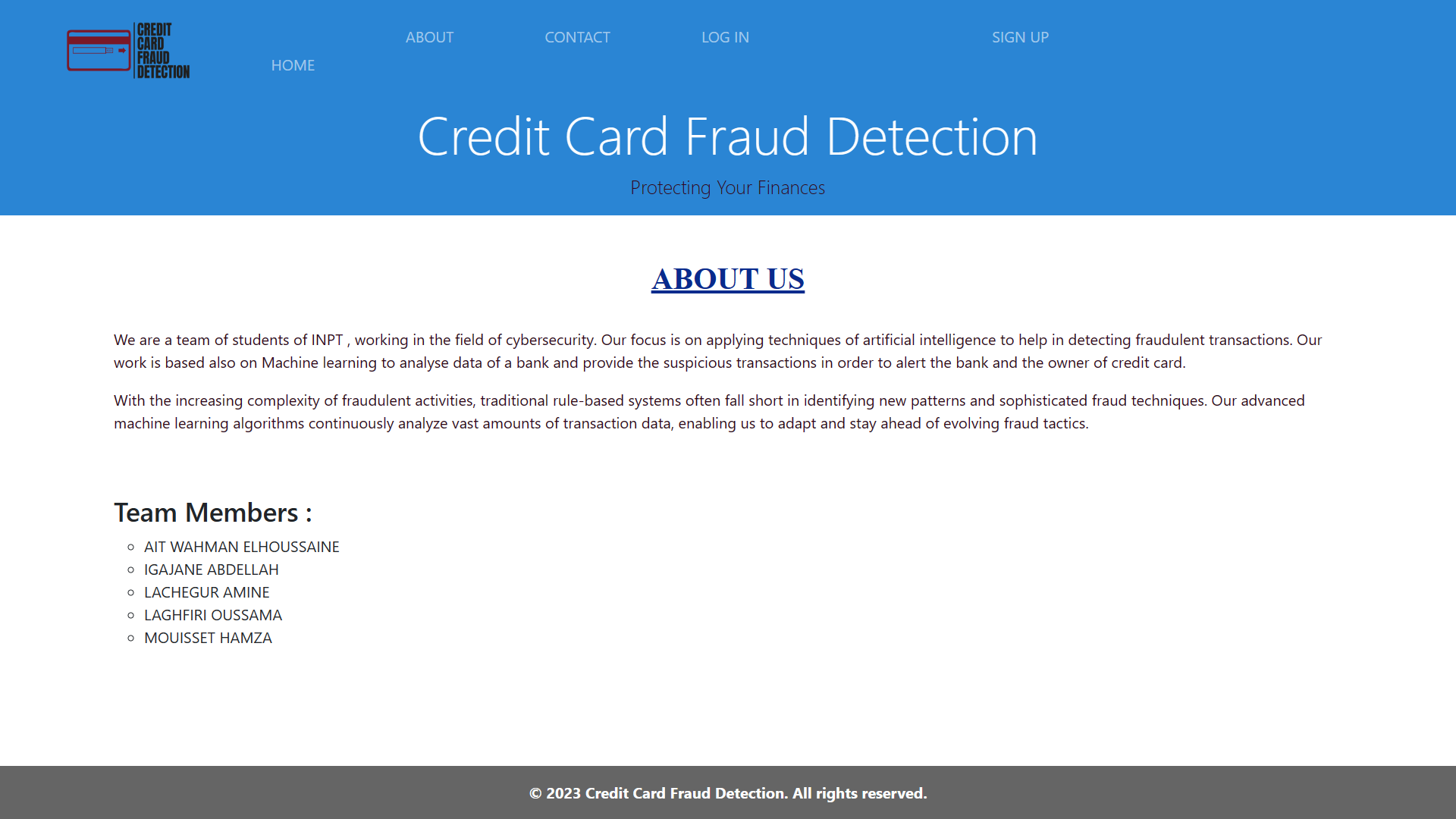
1. ***Solution proposée :***

Notre projet vise à créer une application web qui permet la détection des transactions frauduleuses d’une manière efficace en utilisant l’intelligence artificielle et l’apprentissage automatique et en exploitant une base de données des anciennes transactions frauduleuses.

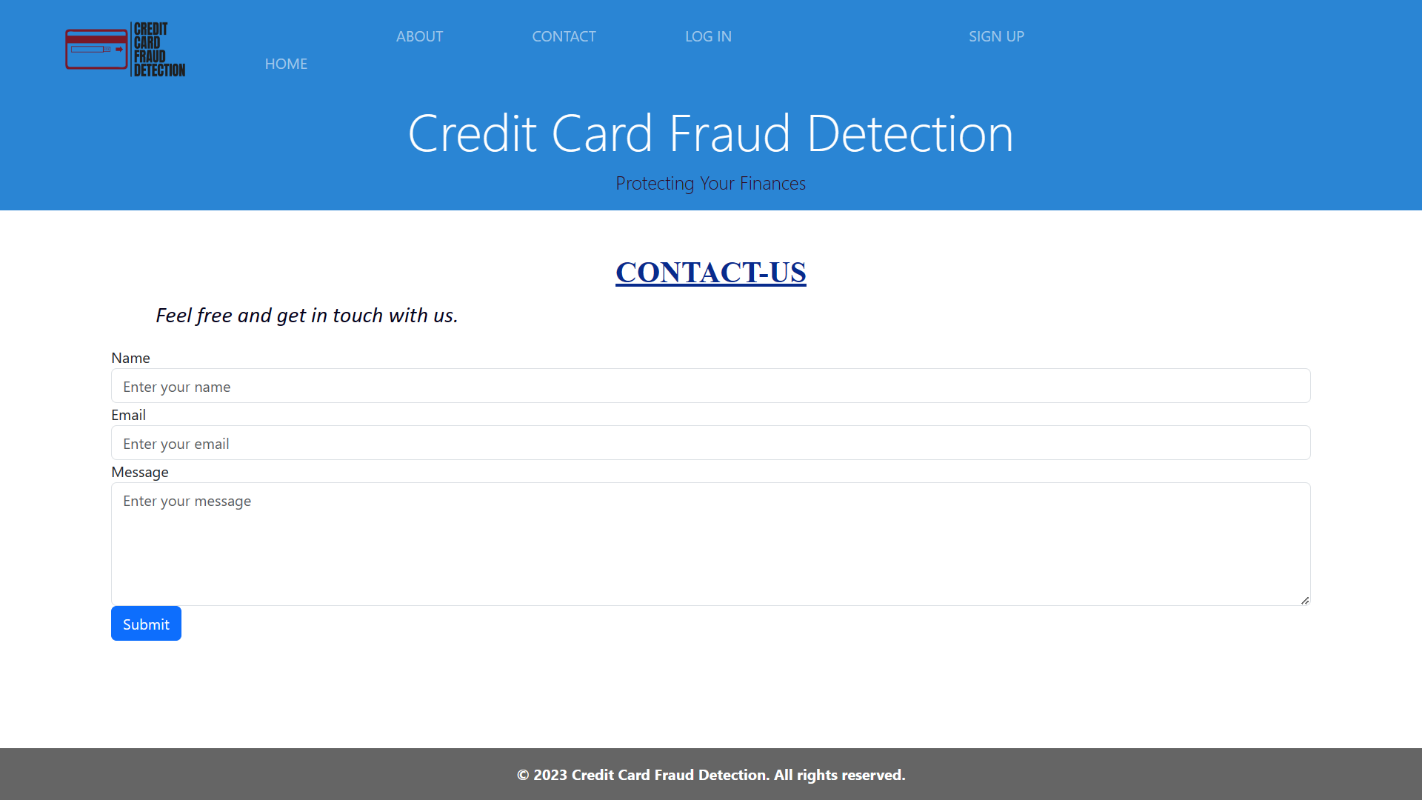
1. **Application Web (*Credit Card Fraud Detection*):**
2. ***Structure de l’application:***

* **Homepage:**

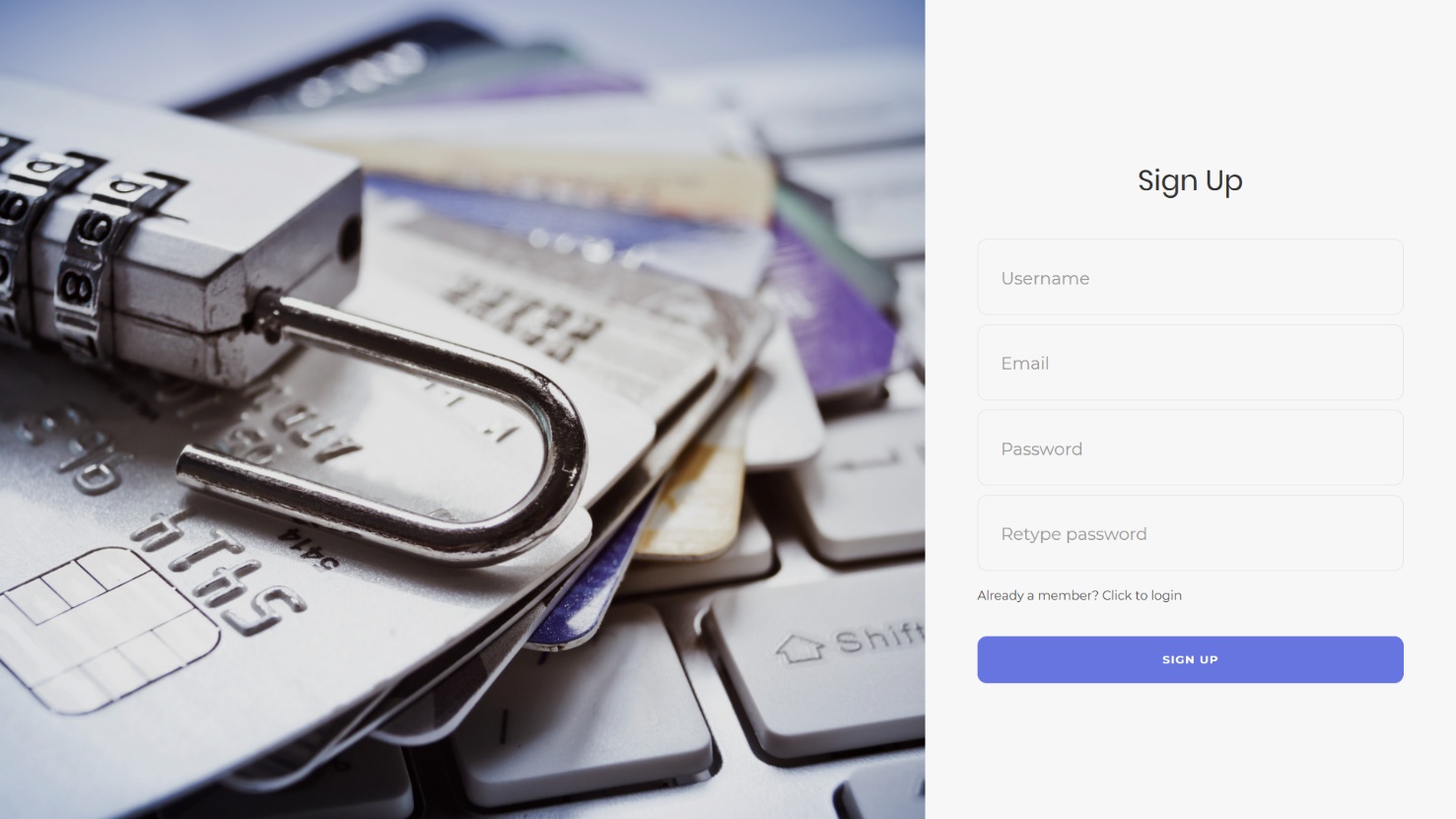
Homepage ou page d’accueil contient des informations sur l’application web.

* **About:**

Cette page contient des informations sur nous comme membres de l’équipe et notre objectif de ce projet.

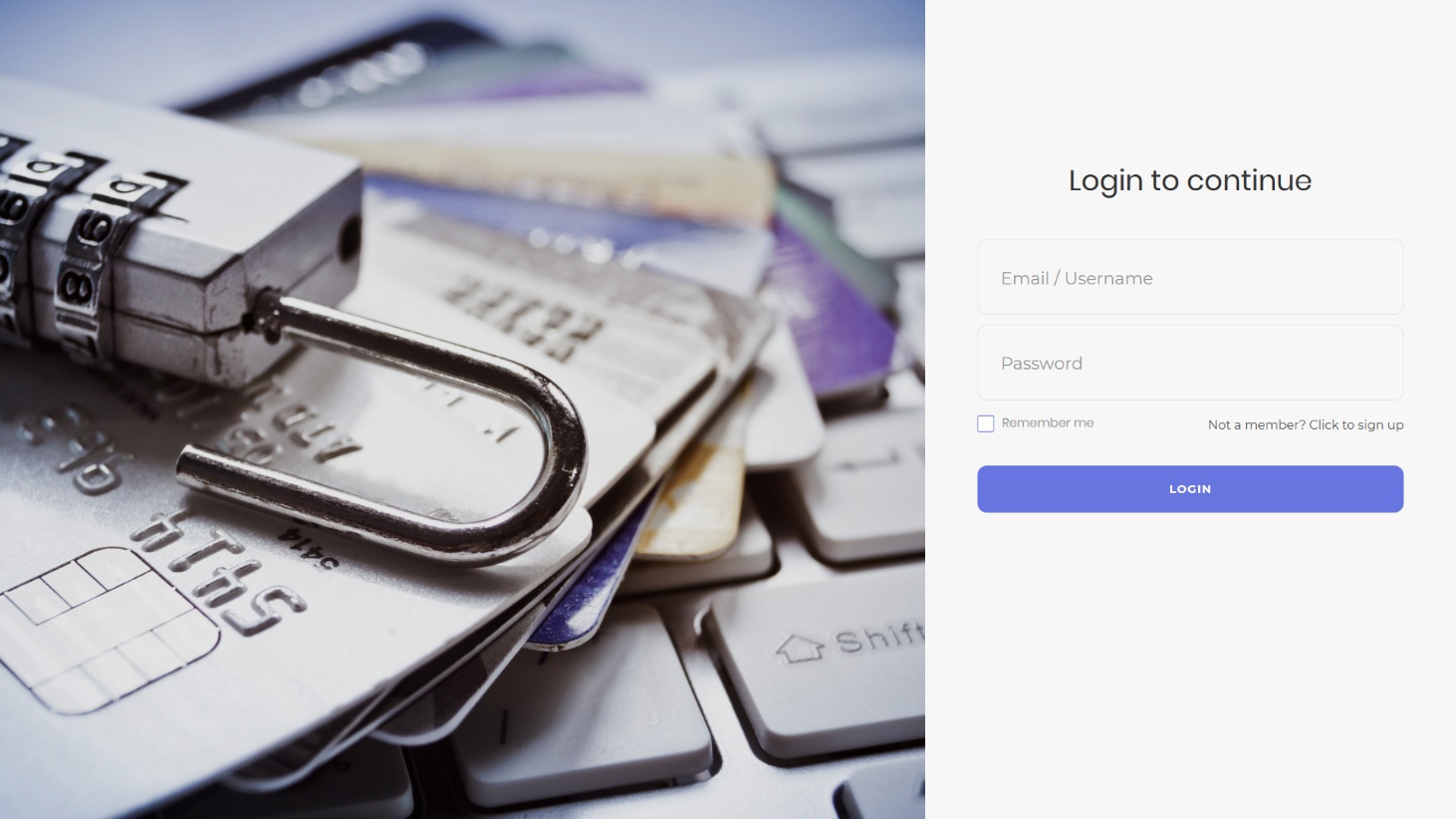
* **Contact:**

Cette page est destinée aux clients s’ils ont des questionnements ou donner leur point de vue.

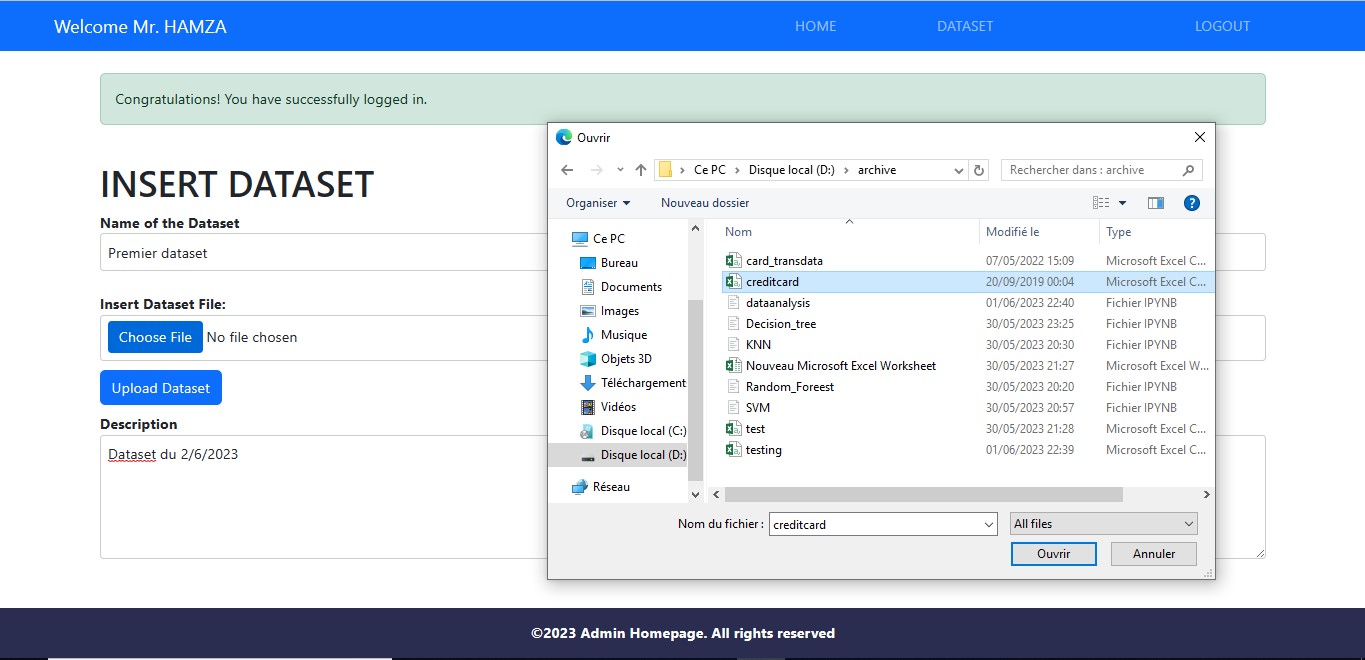
* **Login :**

Login ou page de connexion est la page d’authentification des administrateurs.

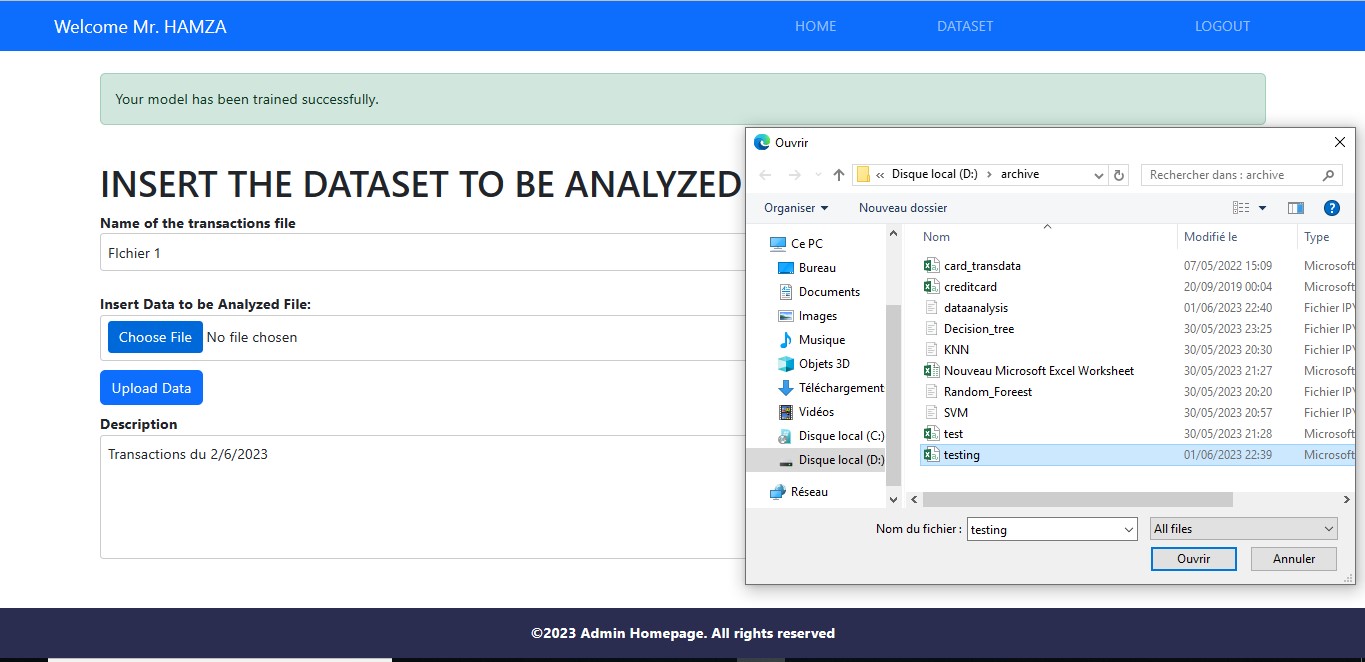
* **Signup:**



Cette page est destinée aux administrateurs pour créer leurs comptes.

* **Homepage administrateur :**

L’administrateur est orienté à la page d’accueil d’administrateur pour insérer la base de données (dataset) qui contient des anciennes transactions qui semblent frauduleuse.

* **Page de détection de fraude :**

Cette page est consacrée pour l’administrateur afin de charger la base de données des transactions qui doivent être vérifiés et détecter celles qui sembles être frauduleuses.

1. ***Description partie HTML / CSS / JS* *:***

À l'ère numérique d'aujourd'hui, les transactions financières se déroulent principalement en ligne, la menace de la fraude par carte de crédit est omniprésente. Pour contrer ce fléau, des technologies avancées telles que l'apprentissage automatique et le développement web convergent pour créer des systèmes intelligents capables de détecter et de prévenir les activités frauduleuses. Cette partie explore le parcours de création d'un site de détection de fraude par carte de crédit, en utilisant HTML, CSS, JavaScript, afin d'offrir une expérience sécurisée et conviviale.

Le langage de balisage hypertexte (HTML) forme le socle de notre site de détection de fraude par carte de crédit. En utilisant les éléments structuraux d'HTML, nous construisons la mise en page et le contenu du site. La page d'accueil agit comme une passerelle, présentant une barre de menu pour une navigation aisée et un carrousel pour mettre en avant les informations clés. La section du corps constitue le cœur de la page, présentant les détails pertinents sur le système de détection de fraude tel que la base de données à entrainer le modelé de détection de fraude.

Les feuilles de style en cascade (CSS) nous permettent d'améliorer l'attrait visuel et l'expérience utilisateur de notre site de détection de fraude par carte de crédit. Grâce à CSS, nous appliquons des styles personnalisés, choisissons des couleurs appropriées et concevons une interface utilisateur intuitive et réactive. En créant une mise en page attrayante et conviviale, nous visons à instaurer confiance et assurance chez les utilisateurs lorsqu'ils interagissent avec notre plateforme.

JavaScript joue un rôle essentiel en dotant notre site web des interactions et fonctionnalités nécessaires. En exploitant la puissance de JavaScript, nous intégrons des algorithmes d'apprentissage automatique qui analysent en temps réel les données des transactions afin de détecter les motifs et les anomalies. Le code JavaScript interagit avec le backend, traite et vérifie de manière sécurisée les transactions par carte de crédit. De plus, nous mettons en place une validation des formulaires et une gestion des erreurs pour garantir la saisie précise des données et offrir une expérience utilisateur fluide.

Intégration du Backend Django : Le Cœur de la Détection de Fraude : Au-delà du développement frontend, notre site de détection de fraude par carte de crédit repose sur l'intégration du backend Django pour traiter les données et exécuter les algorithmes de détection de fraude

Amélioration Continue et Sécurité : La création d'un site de détection de fraude par carte de crédit est un processus continu de raffinement et d'amélioration. Des mises à jour régulières sont nécessaires pour intégrer les dernières techniques de détection de fraude, s'adapter aux menaces évolutives et améliorer l'expérience utilisateur. La mise en place de mesures de sécurité robustes, telles que des protocoles de cryptage, une transmission sécurisée des données et des mécanismes d'authentification, garantit la confidentialité et l'intégrité des informations sensibles des utilisateurs.

Conclusion : La fusion d'HTML, CSS, JavaScript et de l'intégration du backend Django nous permet de créer un site de détection de fraude par carte de crédit qui protège les transactions financières des utilisateurs. En utilisant la puissance de l'apprentissage automatique, nous pouvons analyser en temps réel les données de transaction et identifier les activités frauduleuses potentielles, offrant aux utilisateurs tranquillité d'esprit et protection de leur argent durement gagné. Avec une amélioration continue et un engagement envers la sécurité, notre site de détection de fraude par carte de crédit constitue un outil précieux dans la lutte contre la fraude financière dans le domaine numérique.

1. ***Principe de fonctionnement :***

Une fois l’administrateur s’authentifie, il est demandé d’insérer une base de données (dataset) qui contient des transactions connues frauduleuses afin de les comparer avec.

Dans notre cas, on a utilisé une base de données qui présente les transactions qui se sont effectuées par des titulaires de cartes de crédit européens en septembre 2013, où nous avons 492 fraudes sur 284 807 transactions, la classe positive (fraudes) représente 0,172 % de toutes les transactions.

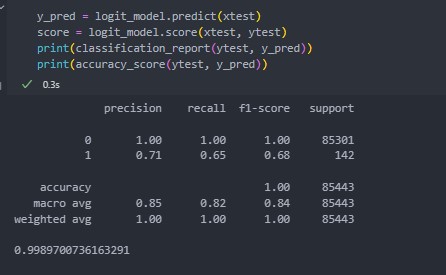
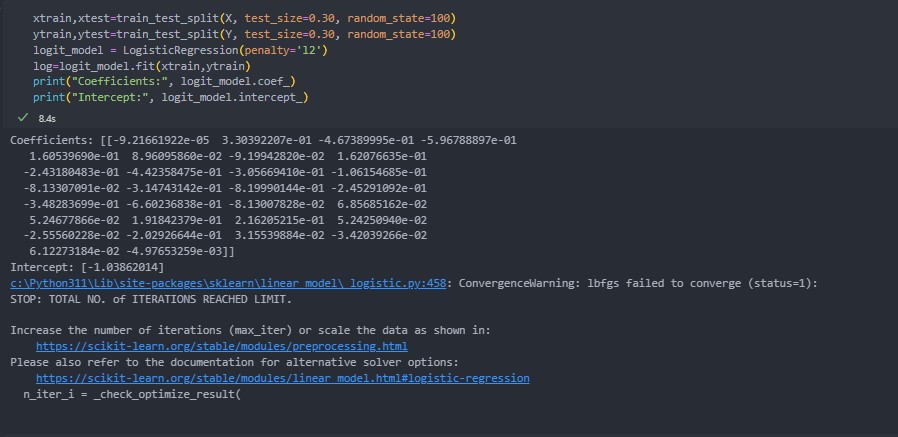
1. **Algorithmes appliquées et résultats :**

Dans cette section, nous avons évalué les performances de plusieurs algorithmes d'apprentissage automatique couramment utilisés pour détecter les transactions frauduleuses. Les algorithmes que nous avons comparés sont : régression logistique, KNN, SVM, Random Forest et Decision Tree. L'objectif était de déterminer quel algorithme offre les meilleures performances pour notre tâche de détection de fraude.

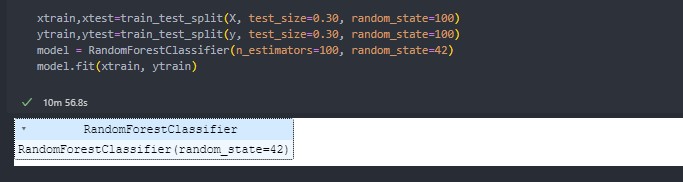
1. ***Méthodologie :***

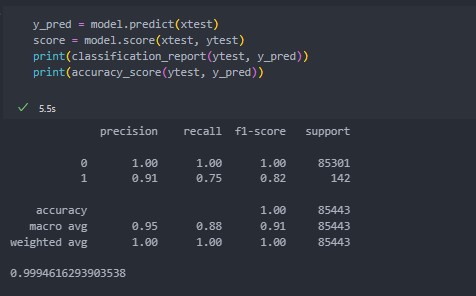
Nous avons suivi la méthodologie suivante pour la comparaison des performances :

* Métriques d'évaluation : Nous avons choisi l'exactitude (accuracy) L'exactitude nous permet de mesurer la performance globale de chaque algorithme.
* Configuration des algorithmes : Pour chaque algorithme, nous avons utilisé les paramètres par défaut recommandés par la documentation respective. Cela garantit une comparaison équitable des performances entre les algorithmes.
* Entraînement et évaluation : Nous avons divisé notre ensemble de données en ensembles d'entraînement et de test selon un ratio de. Nous avons entraîné chaque algorithme sur l'ensemble d'entraînement et évalué sa performance sur l'ensemble de test.

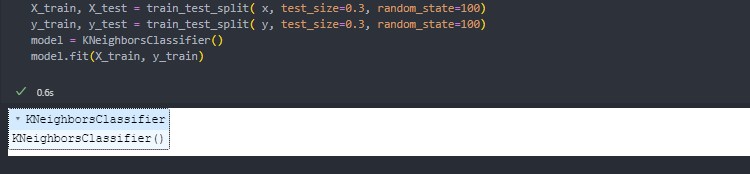
1. ***Résultats :***
2. ***Régression Logistique :***

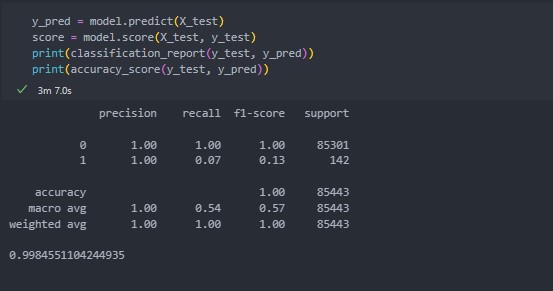
* Précision : **99.89%**
* Temps d’entrainement : **8.4 s**
* Temps de test : **0.3 s**

1. ***Random Forrest :***

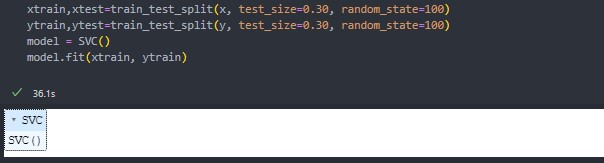


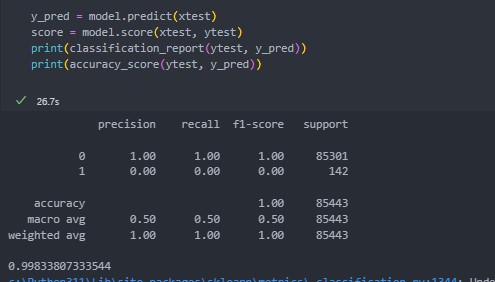
* Précision : **99.94%**
* Temps d’entrainement : **10min 56s**
* Temps de test : **5.5 s**

1. ***KNN :***

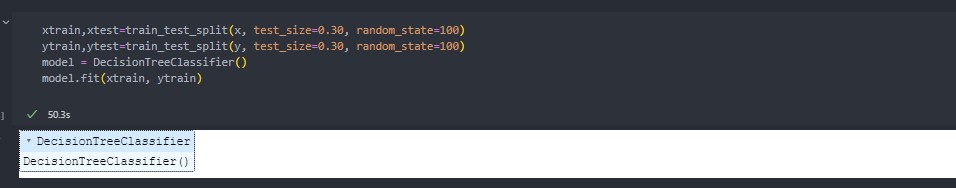


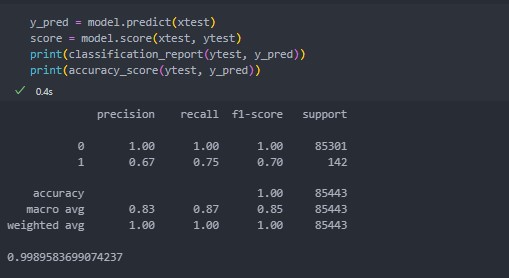
* Précision : **99.84%**
* Temps d’entrainement : **0.6 s**
* Temps de test**: 3min 7s**

1. ***SVM :***



* Précision : **99.83%**
* Temps d’entrainement : **36.1 s**
* Temps de test : **26.7 s**

1. ***Decision Tree :***



* Précision : **99.89%**
* Temps d’entrainement : **50.3 s**
* Temps de test : **0.4 s**

1. ***Résultat de détection de fraude :***
2. ***Conclusion :***

En analysant les résultats on observe que tous ces algorithmes donnent des bons résultats au niveau d’exactitude avec un valeur de 99% avec des différences minimes. La contrainte qu’on a considérée pour choisir le meilleur algorithme et le temps pris dans la phase d’entrainement et test. Ici la Régression Logistique prend la moindre durée pour s’entrainer et faire le test ; ce qui nous encourage à le considérer comme solution optimale pour notre projet.

1. **CONCLUSION :**

Dans le cadre de notre projet de détection de fraudes par carte de crédit, nous avons développé une application web robuste et utilisé des algorithmes de machine learning pour entraîner et tester notre modèle de détection. Notre objectif principal était de construire un système capable d'identifier les transactions frauduleuses de manière précise et efficace. Grâce à notre approche basée sur l'apprentissage automatique, nous avons réussi à obtenir des résultats prometteurs. Les algorithmes de Machine Learning, tels que la régression logistique, le KNN, le SVM, le Random Forest et le Decision Tree, ont démontré leur utilité dans la détection de fraudes.

L'application web que nous avons développés offre une interface conviviale pour les utilisateurs, leur permettant de soumettre leurs transactions pour être évaluées. Le modèle formé sur notre ensemble de données d'entraînement a été intégré à l'application pour effectuer des prédictions en temps réel. Les résultats de la prédiction sont ensuite présentés à l'utilisateur, l'informant si la transaction est susceptible d'être frauduleuse ou non.

Il convient de noter que la détection de fraudes par carte de crédit est un défi continu, car les fraudeurs évoluent constamment leurs techniques. Notre modèle actuel peut présenter des performances élevées, mais il est essentiel de le mettre à jour régulièrement avec de nouvelles données et de continuer à améliorer notre système pour rester en avance sur les fraudes potentielles.

En conclusion, notre projet de détection de fraudes par carte de crédit a été un succès, tant sur le plan de l'application web développée que sur les performances des algorithmes de Machine Learning utilisés. Nous sommes fiers des résultats obtenus et sommes convaincus que notre travail contribuera à renforcer la sécurité des transactions par carte de crédit et à protéger les utilisateurs contre les activités frauduleuses.

1. **Bibliographie :**

Documentation Django :

[**https://docs.djangoproject.com/en/4.2/**](https://docs.djangoproject.com/en/4.2/)

Statistiques de fraudes 2023 :

[**https://www.security.org/digital-safety/credit-card-fraud-report/**](https://www.security.org/digital-safety/credit-card-fraud-report/)

Module Scikit-learn :

[**https://scikit-learn.org/stable/index.html**](https://scikit-learn.org/stable/index.html)

Site du Dataset :

[**https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud**](https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud)