COLLEGE OF ENGINEERING GUINDY
DEPARTMENT OF COMPUTER SCIENCE

CREDIT CARD FRAUD DETECTION

A Machine Learning Project

SUBMITTED BY

AKSHAYA SRIKRISHNA – 2022103065
ANAGHA SRIKRISHNA – 2022103066
KRISHNENDU M R - 2022103081

ABSTRACT - The rapid increase in online transactions has significantly amplified the risk of credit card fraud, leading to substantial financial losses. To combat this, machine learning (ML) and deep learning (DL) techniques have emerged as powerful tools in detecting fraudulent transactions. This project utilizes a European dataset containing anonymized credit card transaction data and applies state-of-the-art ML algorithms to detect fraudulent activities. A comparative analysis of various models, including Logistic Regression (LR), Decision Tree (DT), Random Forest (RF), and Convolutional Neural Networks (CNN), has been conducted. The Random Forest model, identified as the best-performing classifier, is integrated into a Flask-based application to provide predictions on transaction authenticity. This report also highlights the implementation of data balancing techniques like undersampling and oversampling to address class imbalance, and the results demonstrate an accuracy of over 99%, with significant improvements in precision and recall. The project offers an efficient, scalable, and interpretable solution for real-world credit card fraud detection.

TABLE OF CONTENTS

GLOSSARY

Supervised Learning - A type of machine learning where models are trained on labelled data to predict outcomes for unseen data.

Imbalanced Data - A situation where one class (e.g., fraudulent transactions) is significantly underrepresented compared to the other, complicating model training.

Logistic Regression (LR) - A statistical method used for binary classification that models the probability of a categorical outcome.

Random Forest (RF) - An ensemble learning method that builds multiple decision trees and combines their outputs to improve accuracy and reduce overfitting.

XGBoost - A gradient boosting algorithm that improves prediction accuracy through an ensemble of decision trees, widely used in competitive machine learning.

Convolutional Neural Networks (CNN) - A deep learning model primarily used in image recognition, but also effective for fraud detection when analyzing structured transaction data.

SMOTE (Synthetic Minority Over-sampling Technique) - A technique for addressing class imbalance by generating synthetic examples for the minority class.

Precision - A metric that evaluates the proportion of true positives among all predicted positives in a classification task.

Recall - A metric that measures the proportion of actual positives that were correctly identified by the model.

F1-Score - The harmonic mean of precision and recall, balancing the trade-off between the two metrics.

Area Under the ROC Curve (AUC) - A performance metric that evaluates how well a model distinguishes between different classes, particularly in imbalanced datasets.

OBJECTIVE

To develop a credit card fraud detection system that analyses transaction data to predict and identify potentially fraudulent activities. The system utilizes a publicly available European dataset containing 284,807 transactions from September 2018, of which 0.172% were fraudulent. Given the confidentiality of consumer transaction details, principal component analysis (PCA) is applied to reduce the dimensionality of the dataset, preserving interpretability while minimizing information loss. The dataset includes PCA-transformed features (V1 to V28), along with time, amount, and class labels. Machine learning algorithms are used to assess risk factors and predict the likelihood of fraud. The system aims to enhance security, minimize false positives, and optimize the overall transaction verification process, providing businesses with a reliable tool for detecting fraudulent activities in credit card transactions.

INTRODUCTION

The rise of digital payments and online shopping has led to an increased dependency on credit cards for transactions. While this provides convenience, it also opens the door to fraudulent activities that affect cardholders and financial institutions. Detecting credit card fraud is challenging due to the high dimensionality of transaction data, the presence of class imbalance, and the ever-changing patterns of fraudulent behaviour.

Machine learning and deep learning techniques offer a promising solution for automated fraud detection. Traditional methods often struggle with accuracy and scalability, but the integration of advanced ensemble methods and neural networks has shown significant improvements. This project leverages these advancements, combining robust feature engineering, model selection, and application integration to provide a practical approach to credit card fraud detection.

LITERATURE SURVEY

Objective

The primary objective of this research [1] conducted by F. K. Alarfaj, M. Ramzan, I. Malik, H. U. Khan, and M. Ahmed was to develop and implement an advanced fraud detection system for credit card transactions using state-of-the-art machine learning and deep learning algorithms. The researchers aimed to address several critical challenges in the field of fraud detection. First, they sought to overcome the inherent problem of high-class imbalance in fraud detection datasets, where legitimate transactions significantly outnumber fraudulent ones. Second, they aimed to improve the accuracy of fraud detection while minimizing false alarms, a crucial balance in real-world applications. Third, the research focused on developing a system capable of adapting to the evolving nature of credit card fraud, as fraudsters continuously modify their techniques. Additionally, the study aimed to compare the effectiveness of traditional machine learning approaches with modern deep learning techniques, particularly focusing on the application of Convolutional Neural Networks (CNN) for fraud detection.

Methodology

The research methodology employed a comprehensive, multi-layered approach to achieve its objectives. The study utilized a European card benchmark dataset comprising 284,807 transactions, of which 492 (0.172%) were fraudulent, reflecting real-world class imbalance scenarios. The methodology can be broken down into several key phases. In the first phase, the researchers applied various feature selection algorithms to identify and rank the most relevant features from the dataset, which included 31 columns (time, amount, and 28 PCA-transformed features). The second phase involved implementing and testing multiple machine learning algorithms, including Extreme Learning Method, Decision Tree, Random Forest, Support Vector Machine, Logistic Regression, and XGBoost. Each algorithm was carefully tuned and evaluated for its performance in fraud detection. The third phase focused on deep learning implementation, where the researchers developed three distinct CNN architectures with varying layer configurations. They particularly emphasized the addition of specialized layers for feature extraction and classification. The methodology also included a novel approach to handling data imbalance through specialized techniques and

the application of different architectures of CNN layers. Throughout the process, the researchers maintained a rigorous comparative analysis framework, evaluating each model's performance against established benchmarks.

Result

The research yielded significant and promising results in credit card fraud detection. The proposed CNN-based model demonstrated exceptional performance, achieving an accuracy rate of 99.9%, significantly higher than traditional machine learning approaches. The model also achieved an impressive F1-score of 85.71%, precision of 93%, and AUC curves of 98%, indicating robust and reliable fraud detection capabilities. These metrics represent a substantial improvement over existing state-of-the-art solution. The comparative analysis revealed that while traditional machine learning algorithms performed adequately, the deep learning approaches, particularly the enhanced CNN architectures, showed superior performance in handling complex fraud patterns. The research also successfully addressed the class imbalance problem through their modified approach, resulting in a reduced false negative rate. The results demonstrated that the addition of specialized layers in the CNN architecture significantly improved feature extraction and classification accuracy. Furthermore, the experiments with balanced data showed promising results in minimizing false negatives, a crucial aspect in real-world fraud detection systems. The proposed model's performance remained consistent across different testing scenarios, indicating its robustness and reliability for practical implementation. The research also provided valuable insights into the effectiveness of different architectural choices in CNN design for fraud detection, contributing to the broader understanding of deep learning applications in financial security.

The research successfully achieved its objectives by developing a highly accurate fraud detection system that outperforms existing solutions. The comprehensive methodology, combining both traditional and modern approaches, provided valuable insights into the effectiveness of different techniques. The exceptional results, particularly in terms of accuracy and precision, demonstrate the potential of deep learning approaches in addressing complex financial security challenges. This research not only advances the field of fraud detection but also provides a solid foundation for future developments in financial security systems.

METHODOLOGY

Dataset description

The dataset contains transactions made by credit cards in September 2013 by European cardholders. This dataset presents transactions that occurred in two days, where we have 492 frauds out of 284,807 transactions. The dataset is highly unbalanced, the positive class (frauds) accounts for 0.172% of all transactions. It contains only numerical input variables resulting from a PCA transformation. Unfortunately, due to confidentiality issues, we cannot provide the original features or provide more background information about the data. Features V1, V2, and V28 are the principal components obtained with PCA, the only features that have not been transformed with PCA are 'Time' and 'Amount'. Feature 'Time' contains the seconds elapsed between each transaction and the first transaction in the dataset. The feature 'Amount' is the transaction Amount, this feature can be used for example-dependent cost-sensitive learning. Feature 'Class' is the response variable that takes value 1 in case of fraud and 0 otherwise.

Data preprocessing

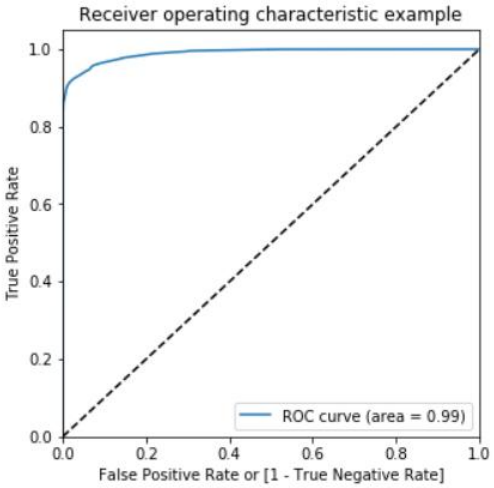
To address the class imbalance and improve the model's ability to detect fraudulent transactions, several data preprocessing techniques were applied. The imbalance, characterized by significantly fewer fraudulent transactions, was mitigated using the Synthetic Minority Oversampling Technique (SMOTE), which generates synthetic samples for the minority class by interpolating between existing instances and their k-nearest neighbours. To complement this, undersampling reduced the majority class size while retaining critical information. This combined approach resulted in a balanced dataset with an equal number of instances (275,190) for both classes. Performance evaluation prioritized metrics such as precision, recall, F1-score, and the ROC-AUC score over accuracy to provide a comprehensive assessment of the model's ability to detect true positives, minimize false negatives, and balance precision and recall. These steps ensured that the model could effectively learn patterns from both classes without bias. As a result, the model demonstrated improved generalization and reliability in real-world scenarios.

Algorithms and results

Logistic Regression

Logistic Regression performed as a baseline model for the credit card fraud detection project. It demonstrated an ROC-AUC score of **0.99**, indicating strong discriminatory power between fraudulent and legitimate transactions. The model effectively captured linear relationships in the dataset, offering quick training and interpretability. However, the simplicity of the model limits its capacity to handle more complex patterns in data. This was evident in cases where the fraud signals were subtle and nonlinear. Despite its limitations, Logistic Regression is reliable for initial evaluations and acts as a benchmark for more advanced models.

Observation: The model is lightweight, easy to implement, and useful for quick results but lacks the robustness required for higher accuracy in detecting fraud in complex datasets.



Model summary

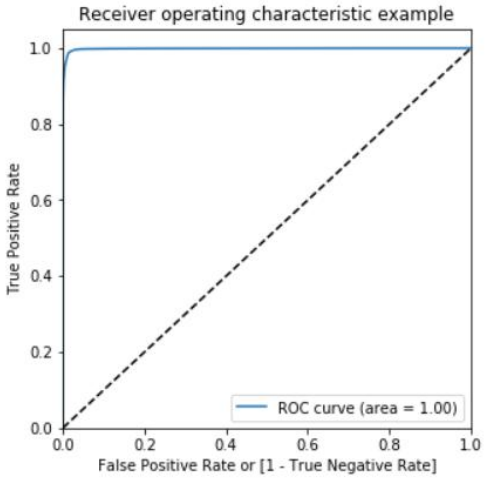
- Precision = 0.972
- Recall = 0.913
- Accuracy = 0.944
- F1 score = 0.942
- ROC-AUC = 0.99

Decision Tree

The Decision Tree model achieved an ROC-AUC score of **1.0**, slightly higher than Logistic Regression. While it excelled at capturing non-linear patterns and provided insights into feature importance, it tended to overfit the training data, especially with deep trees. This overfitting resulted in reduced generalization ability on unseen data. The model's interpretability and visual representation of decisions were strengths, but its performance was not sufficient to outperform ensemble-based approaches.

Output: The Decision Tree effectively identified key features influencing fraud detection, but its instability and sensitivity to data variations limited its overall performance.

Observation: It achieves high precision and recall, with perfect ROC-AUC, making it highly effective in binary classification. It works well for exploratory analysis but requires optimization (e.g., pruning or ensembling) to improve predictive power.



Model summary

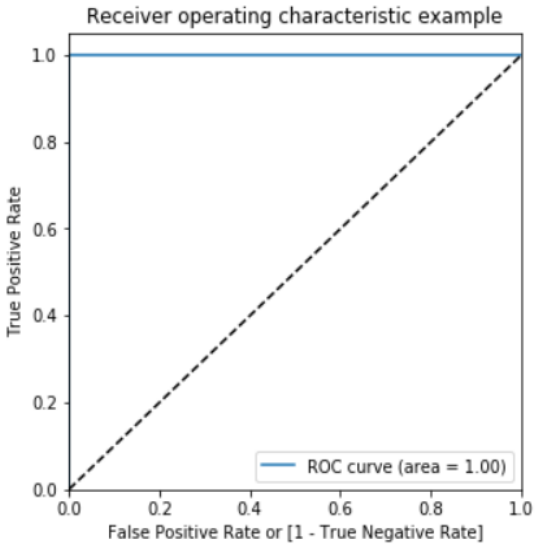
- Precision = 0.997
- Recall = 0.9989
- Accuracy = 0.99
- F1 score = 0.998
- ROC-AUC = 1.00

XgBoost

XGBoost delivered the best performance with an ROC-AUC score of **1.00**, solidifying its status as one of the most effective models for this dataset. Its ability to handle imbalanced data through advanced techniques like scale-positive weight and its support for regularization contributed to its superior results. The model effectively captured complex interactions between features and was highly robust against overfitting due to its iterative boosting approach. The computational efficiency and scalability of XGBoost make it an ideal choice for large and complex datasets.

Output: The model consistently detected fraudulent transactions with high precision and recall, providing the most reliable results among all tested models.

Observation: XGBoost's performance makes it the top candidate for deployment in real-world fraud detection systems. Lower recall values on the test set (e.g., XG1 Test Sensitivity = 0.79), indicating potential overfitting issues.



Model summary

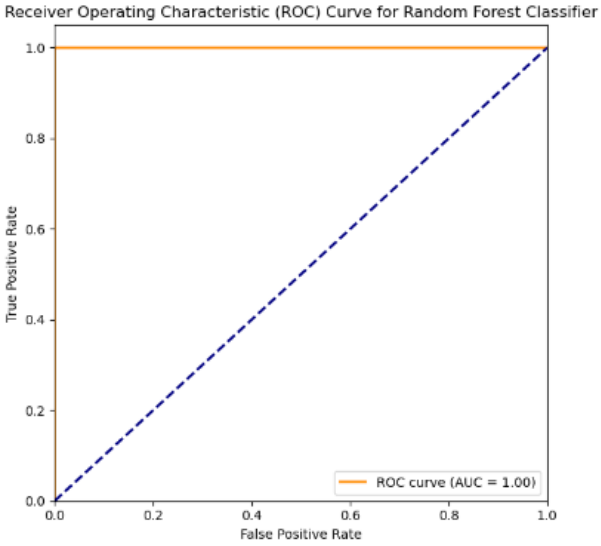
- Precision = 0.995
- Recall = 1.0
- Accuracy = 0.99
- F1 score = 0.997
- ROC-AUC = 1.00

Random Forest

Random Forest achieved an impressive ROC-AUC score of **1.00**, demonstrating its ability to manage non-linearities and reduce variance through ensemble learning. By aggregating predictions from multiple decision trees, the model balanced bias and variance, resulting in robust performance. It also provided insights into feature importance, helping identify critical predictors of fraud. However, its training time and computational cost were higher compared to Logistic Regression.

Output: Random Forest effectively flagged fraudulent activities with high reliability, achieving near-perfect scores in all metrics (Precision: 0.999, Recall: 1.0, F1 Score: 0.999, Accuracy: 0.999, ROC-AUC: 1.0) with excellent generalization.

Observation: Random Forest ranks higher than XgBoost because of its better test set generalization and consistent performance across metrics



Model summary

- Precision = 0.999
- Recall = 1.0
- Accuracy = 0.999
- F1 score = 0.999
- ROC-AUC = 1.00

Convolutional Neural Network

A Convolutional Neural Network (CNN) was explored for credit card fraud detection, achieving an impressive ROC-AUC score of **0.96**. By leveraging its ability to automatically extract intricate patterns and hierarchical features from data, the CNN demonstrated strong potential. However, training the model required significant computational resources and careful preprocessing of tabular data to adapt it for CNN input. Despite its strong performance, the additional complexity and resource requirements outweighed its benefits compared to Random Forest or XGBoost for this specific use case.

Output: Effective detection with high accuracy but resource-intensive training.
Observation: CNNs are powerful but better suited for image or unstructured data rather than structured datasets like credit card transactions.

Comparison between models

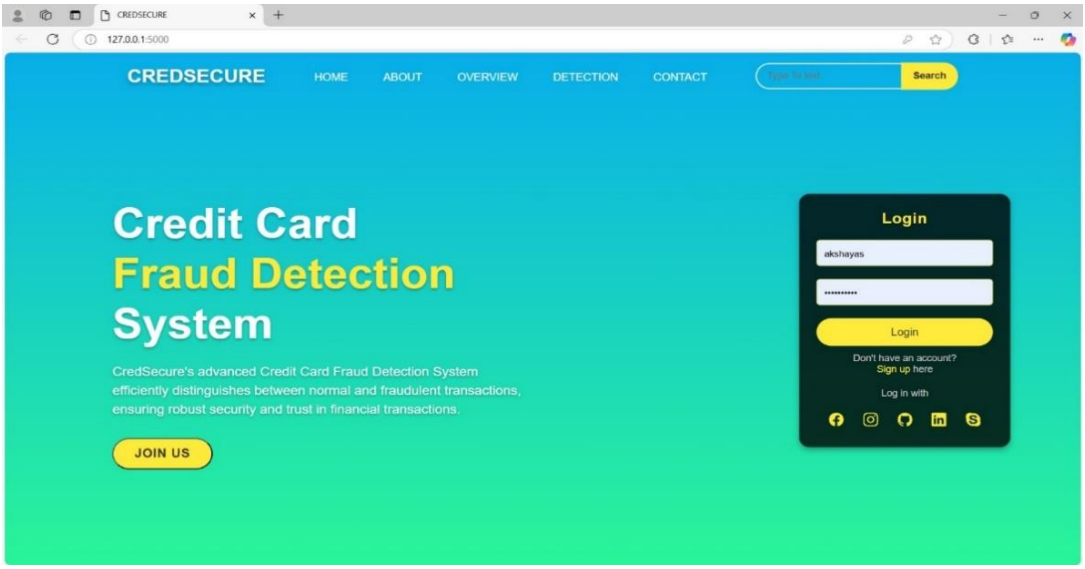
For credit card fraud detection, Random Forest is the top choice due to its strong performance in handling complex and imbalanced datasets, offering high accuracy, recall, and a perfect ROC-AUC. Its ensemble approach helps it capture intricate patterns without overfitting, making it ideal for fraud detection. XGBoost also performs well, excelling in accuracy and precision, but it can suffer from overfitting, which slightly lowers its recall on test data. Decision Trees are interpretable and effective for capturing non-linear relationships but are prone to overfitting and do not generalize as well. Logistic Regression, while simple and interpretable, lacks the ability to capture complex patterns, resulting in lower recall and precision. Convolutional Neural Networks, although powerful in pattern recognition, require substantial computational resources and preprocessing to adapt to tabular data, making them less practical for fraud detection. Overall, Random Forest is the most balanced and efficient model for credit card fraud detection, offering the best trade-off between performance and resource efficiency.

Choosing the best model

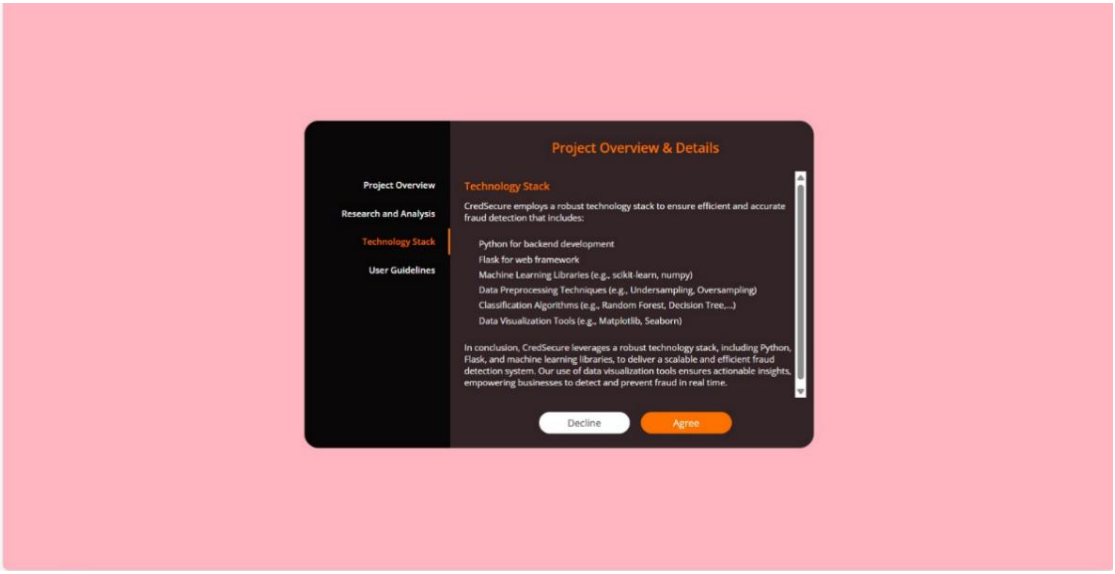
Random Forest was chosen for integration due to its strong performance, ease of implementation, and computational efficiency. It handles imbalanced datasets well and offers a good balance of accuracy, recall, and ROC-AUC, making it ideal for fraud detection. Its simplicity and scalability make it well-suited for deployment in production environments.

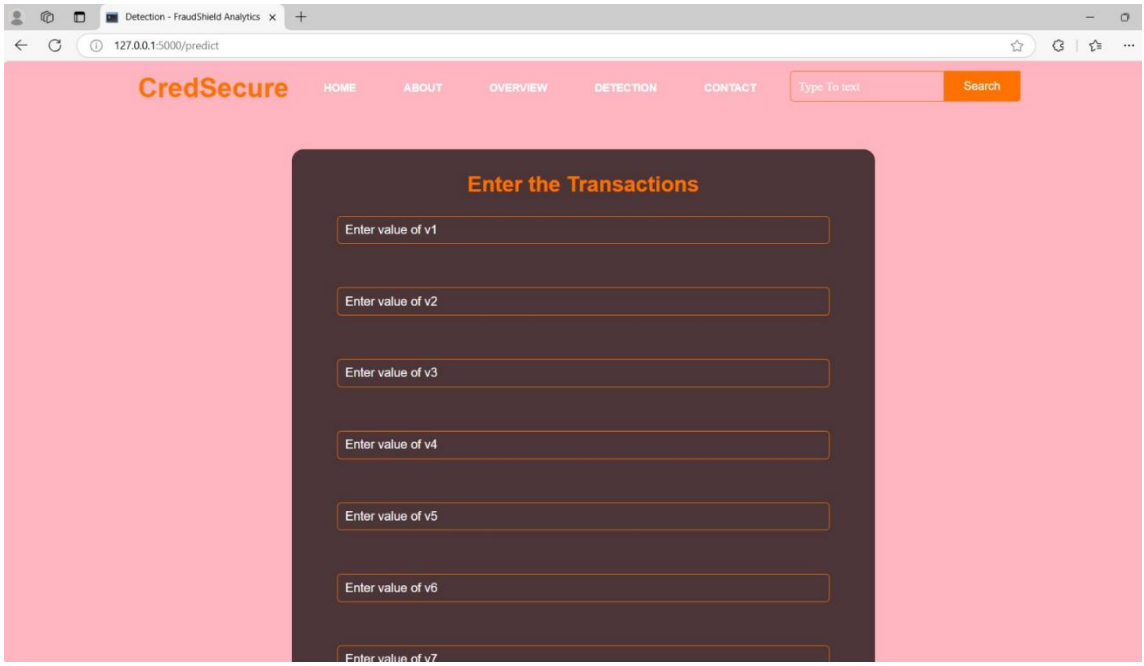
RESULT

1. Home Page

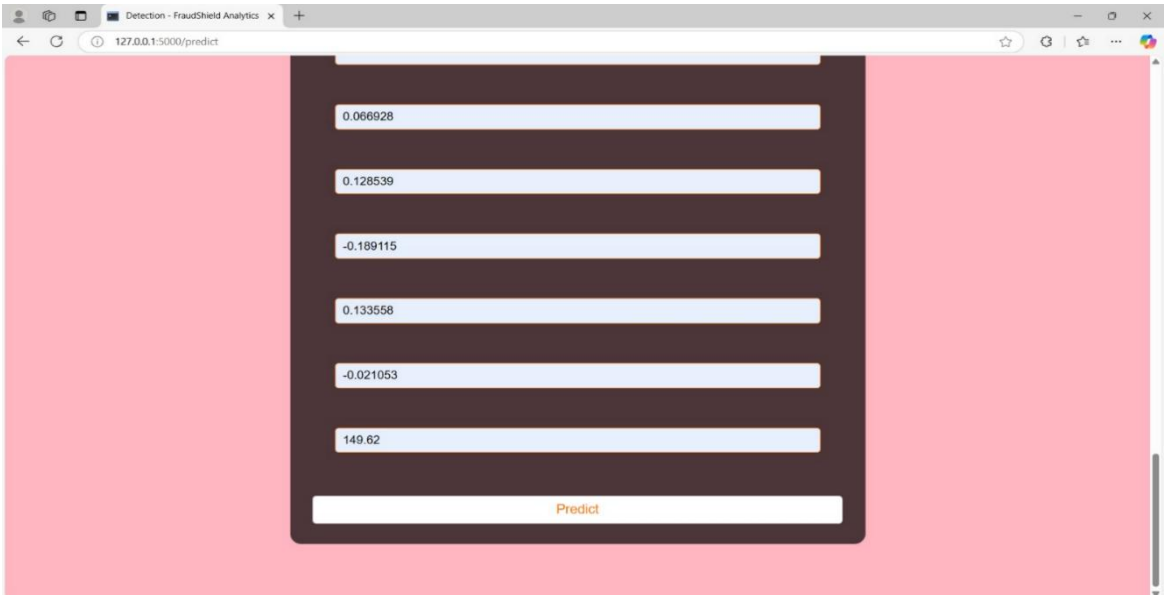


2. Overview Page

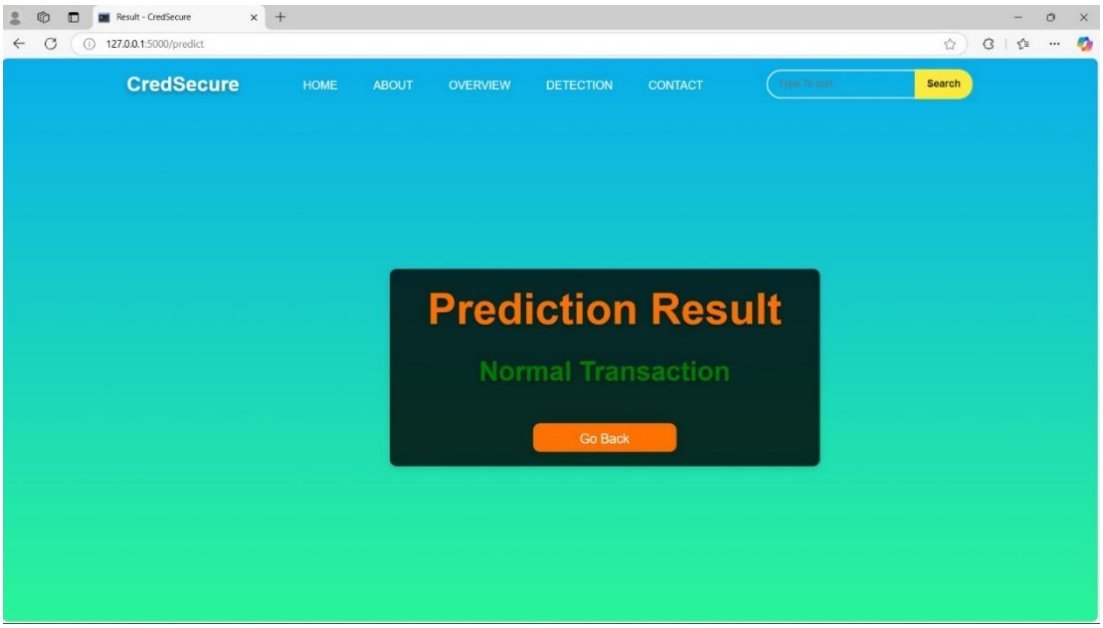




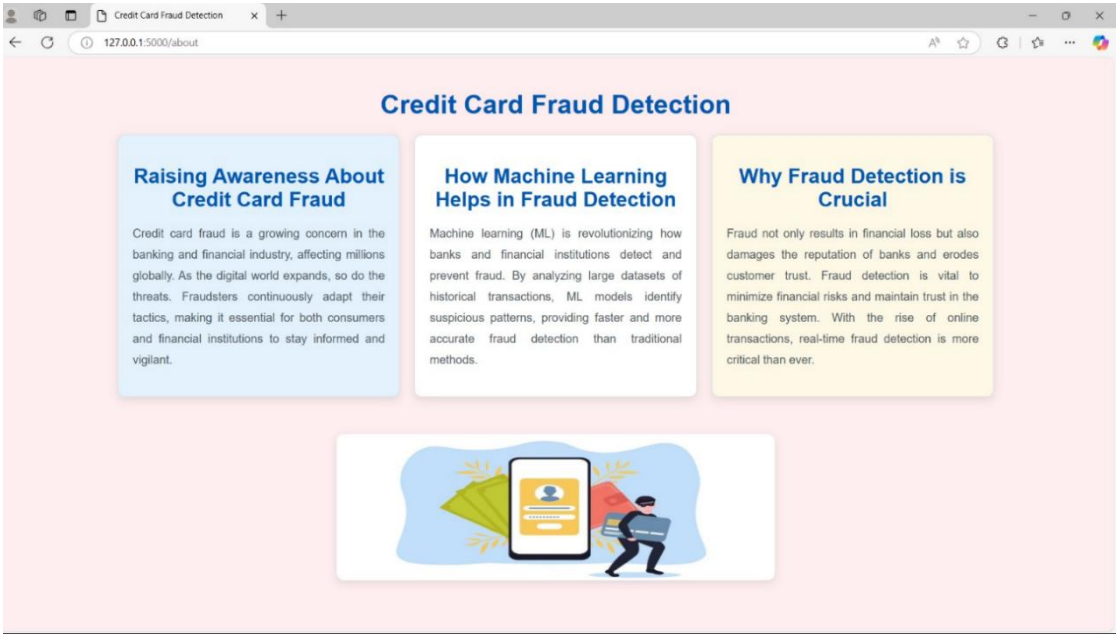
2. Prediction Page



2. Result Page

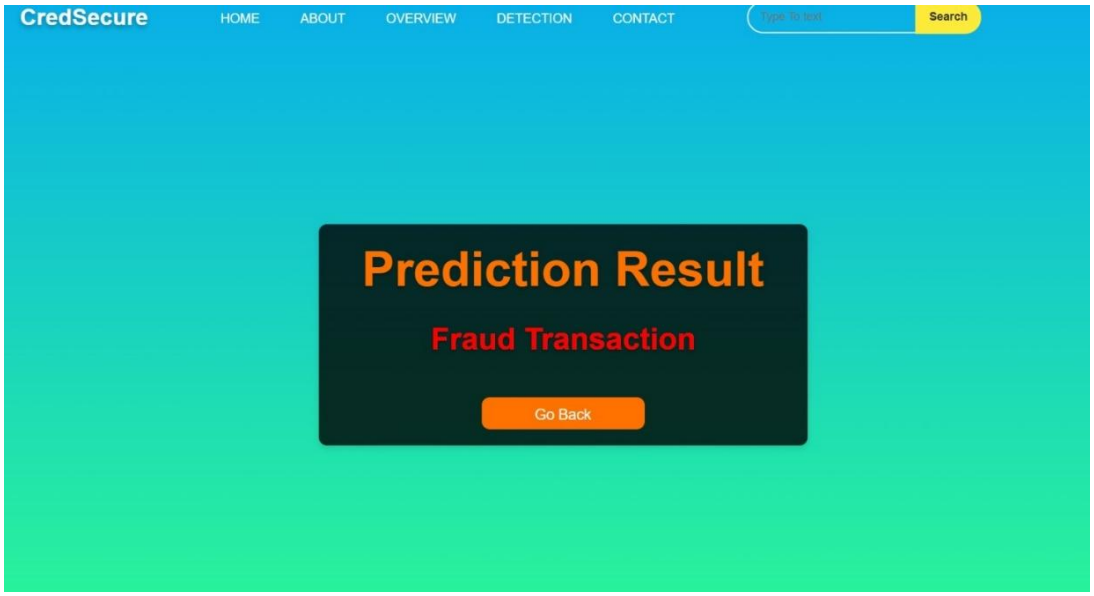


2. About Page



The credit card fraud detection app leverages the Random Forest (RF) model to classify transactions as either normal or fraudulent. Upon inputting transaction details, the app processes the data through the trained RF model and displays a clear result to the user, indicating whether the transaction is normal or fraudulent. This straightforward outcome ensures ease of use for end-users while maintaining high accuracy and reliability in fraud detection.

Accuracy	**0.999**
Precision	**0.999**
F1 Score	**0.999**
ROC-AUC	**1.00**
Recall	**1.00**



This is another example of result page showing the transaction is indeed fraud based on the Random Forest algorithm implemented.

FUTURE SCOPE

1. Real-Time Integration: Enhance the system for real-time fraud detection in live transaction environments.
2. Improved Algorithms: Explore advanced DL architectures like Transformer models for better adaptability.
3. Feature Engineering: Incorporate domain-specific knowledge for feature creation to improve interpretability.
4. Broader Applications: Extend the methodology to detect fraud in other financial domains, such as insurance or loans.
5. Cloud Integration: Migrate the application to a cloud-based infrastructure for scalability and performance optimization

CONCLUSION

This project successfully demonstrates the application of machine learning to detect credit card fraud. By addressing class imbalance and evaluating multiple models, the Random Forest algorithm was identified as the optimal choice for this dataset. The Flask-based web application provides an interactive platform for end-users to utilize the detection system. While the current implementation is non-real-time, future developments could focus on real-time detection and integration with financial systems, paving the way for more robust fraud prevention strategies.

REFERENCES

1. F. K. Alarfaj, M. Ramzan, I. Malik, H. U. Khan, and M. Ahmed, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," IEEE Access, vol. 10, 2022.
2. Dataset https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud
3. Scikit-learn documentation https://scikit-learn.org/stable/
4. researches on undersampling and oversampling datasets. https://link.springer.com/