Report on Credit Card Fraud Detection

By Arya Gowda

1. Introduction

Credit card fraud is a significant issue for financial institutions and consumers alike. Detecting fraudulent transactions promptly is crucial to prevent financial losses and maintain trust in the payment system. In this report, we present an analysis and modeling approach for credit card fraud detection using machine learning techniques.

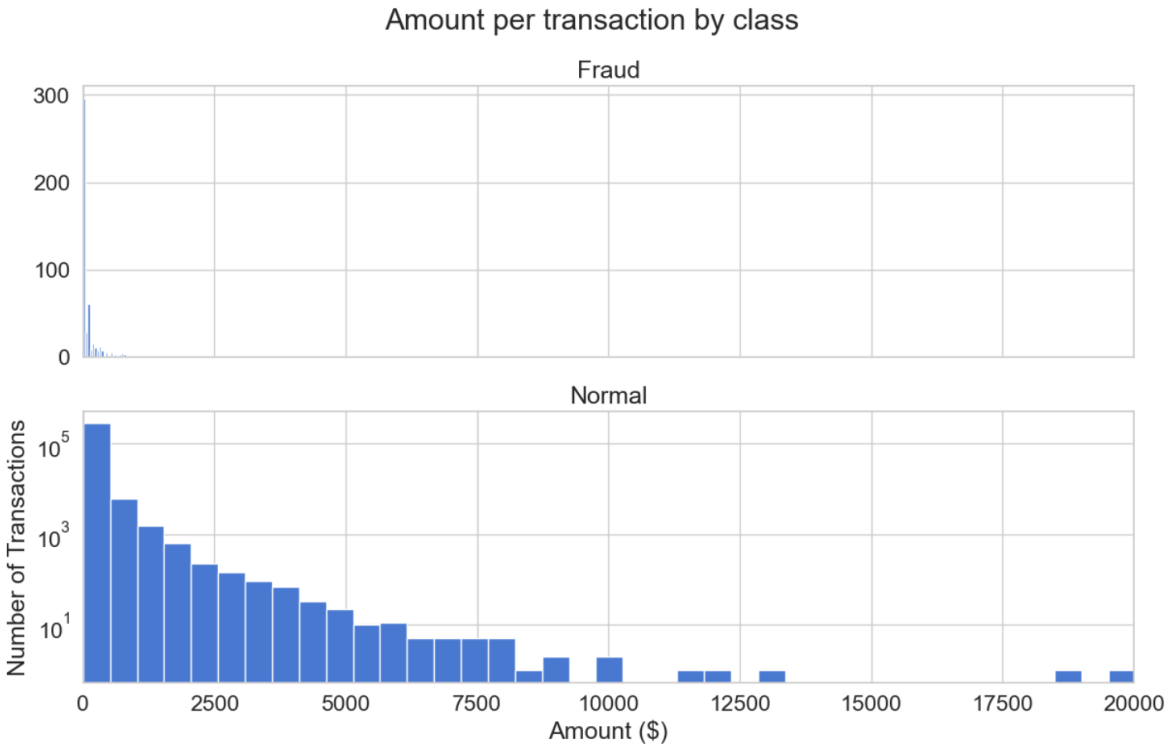
2. Data Overview

The dataset used for this analysis contains credit card transactions, with each transaction labeled as either fraudulent or non-fraudulent. The dataset includes features such as transaction amount, time, and various anonymized features (V1-V28).

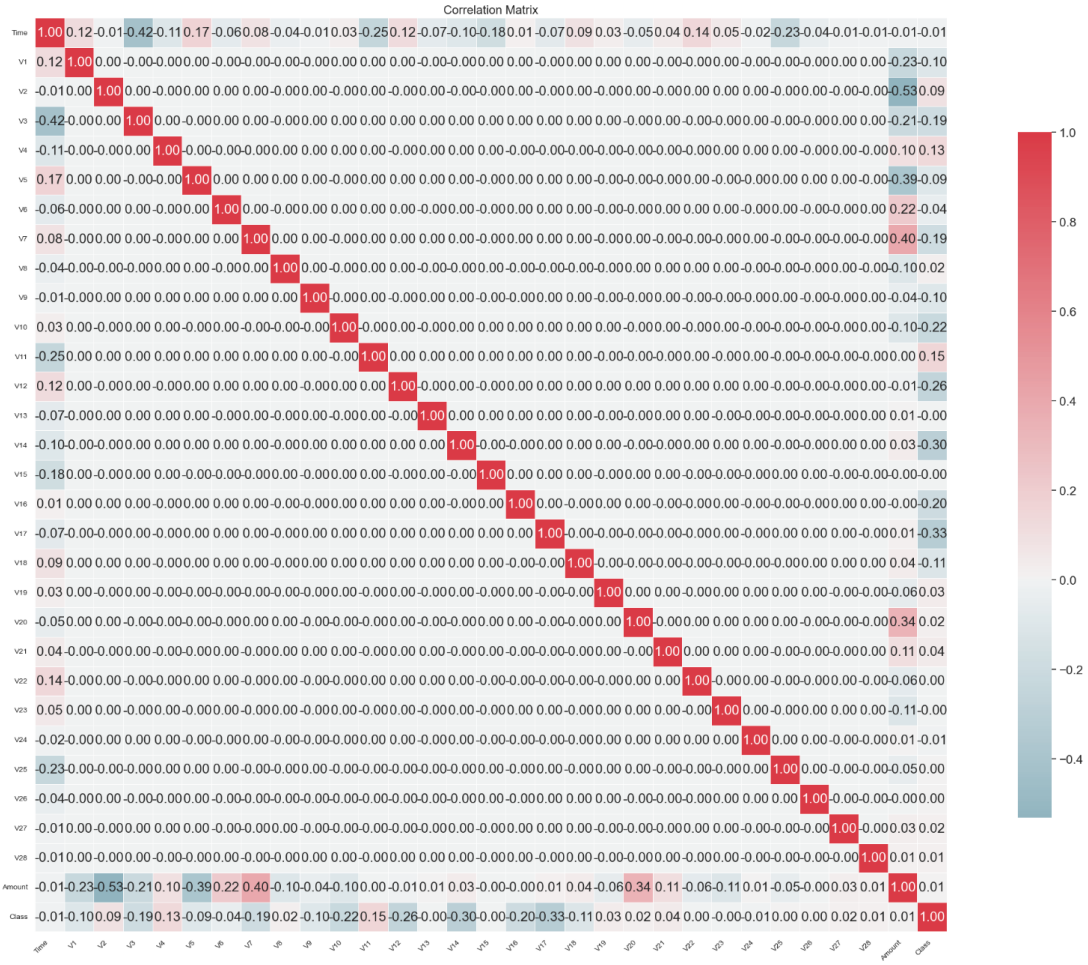
Upon loading the dataset, we performed initial data exploration, including checking for missing values, understanding the distribution of transaction classes (fraudulent vs. non-fraudulent), and analyzing the distribution of transaction amounts for each class.

3. Exploratory Data Analysis (EDA)

The dataset consists of 284,807 transactions, with a highly imbalanced class distribution, where fraudulent transactions account for only 0.17% of the total transactions. We visualized the class distribution and transaction amounts for both fraudulent and non-fraudulent transactions, providing insights into the differences between the two classes.

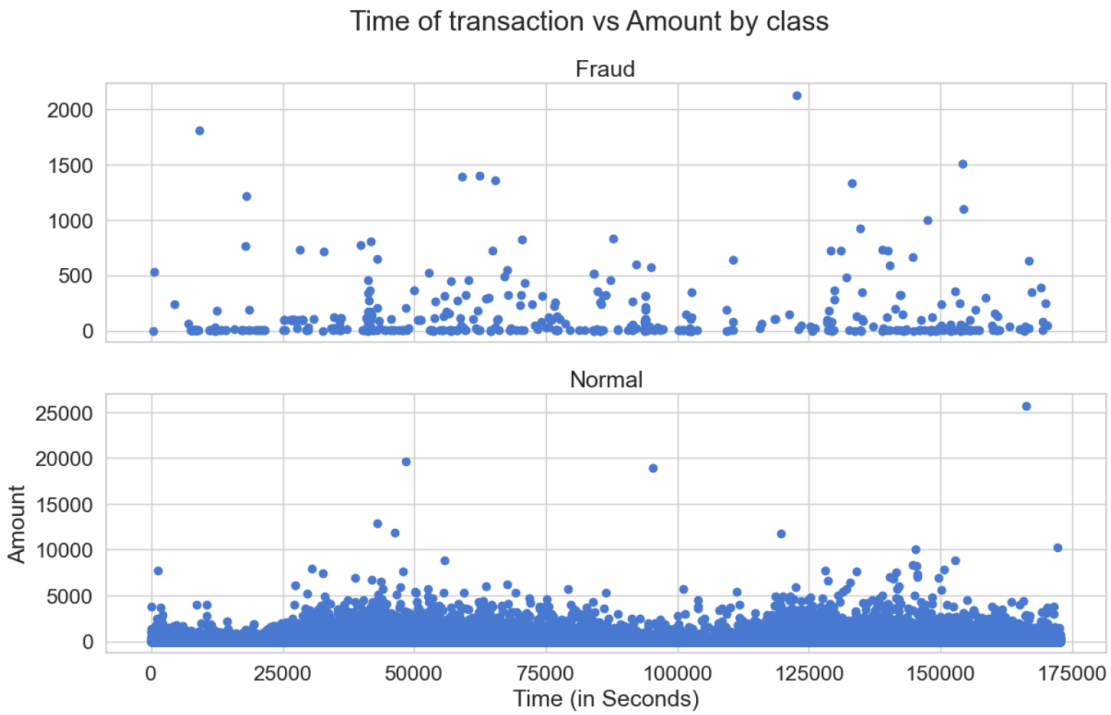


Additionally, we examined the correlation matrix to identify potential correlations between features and explored the relationship between transaction time and amount for both classes.



4. Preprocessing

Before training the models, we preprocessed the data by removing the 'Time' feature and splitting the dataset into training and testing sets (80% training, 20% testing). We also scaled the features using MinMaxScaler to ensure uniformity across features.

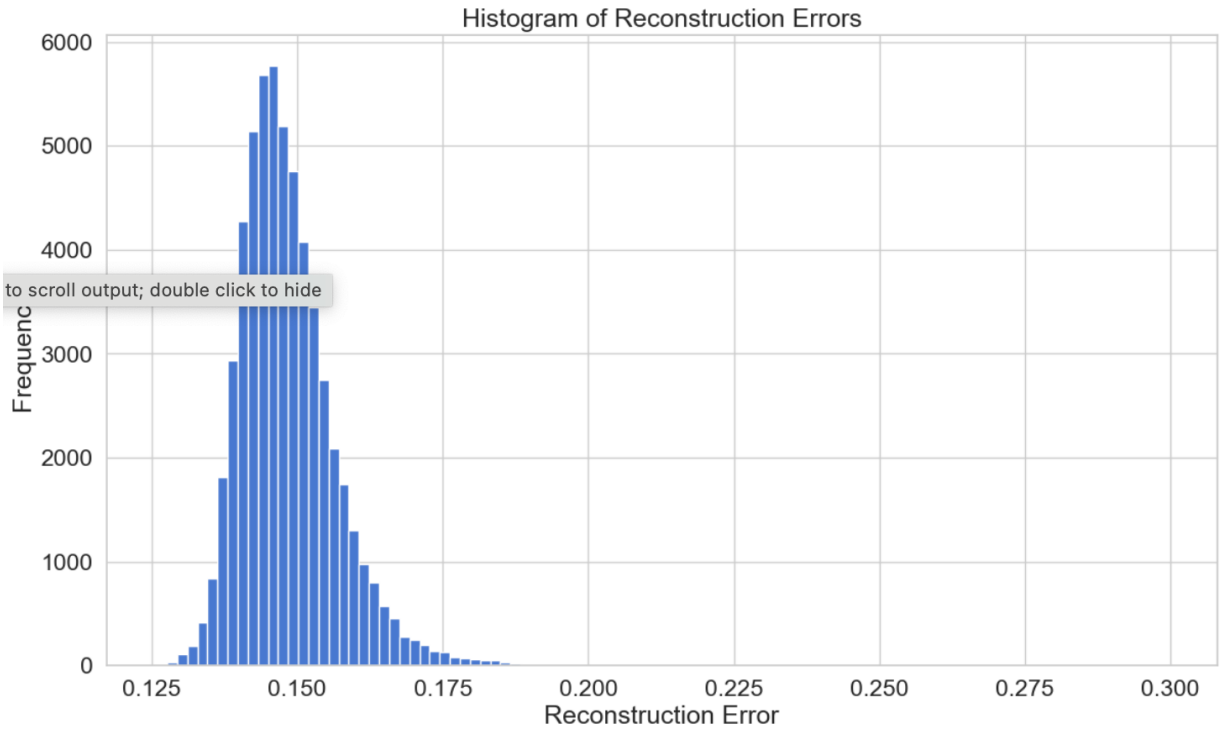


5. Model Development

We developed two models for credit card fraud detection:

- **Autoencoder Model:** An unsupervised learning approach using autoencoders to learn the underlying patterns in the data. The autoencoder was trained on the training data and used to reconstruct the input features. Anomalies were identified based on the reconstruction error.

```
ck to scroll output; double click to hide
              precision    recall  f1-score   support

         0.0       1.00      1.00      1.00     56859
         1.0       0.88      0.45      0.59       103

    accuracy                           1.00     56962
   macro avg       0.94      0.72      0.80     56962
weighted avg       1.00      1.00      1.00     56962


Accuracy Score: 0.9988939995084443
```

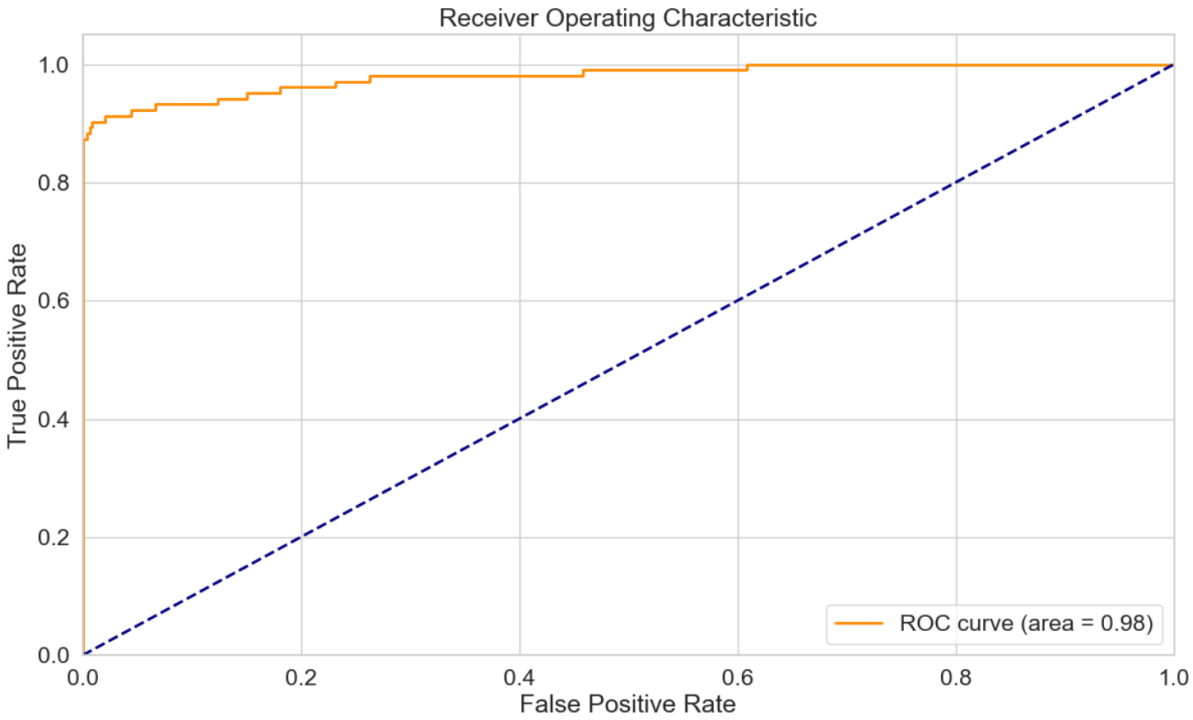


- **Logistic Regression Model:** A supervised learning approach using logistic regression. We extracted the hidden representations learned by the autoencoder as features and trained a logistic regression classifier on these representations.

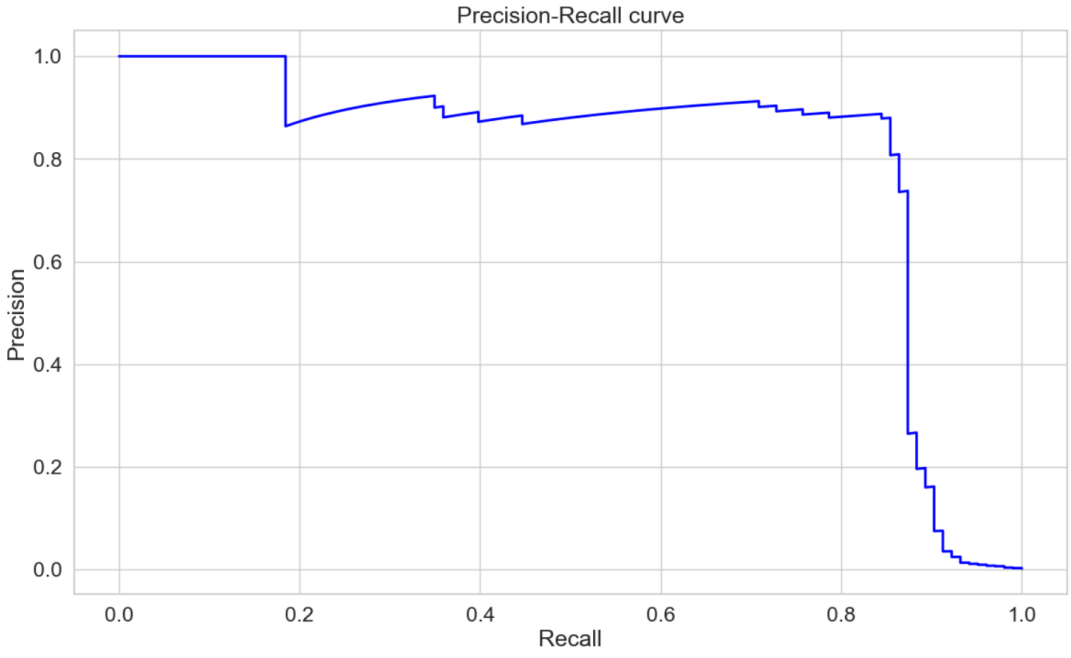
```
Classification Report (Logistic Regression):
              precision    recall  f1-score   support

         0.0       1.00      1.00      1.00     56859
         1.0       0.87      0.40      0.55       103

    accuracy                           1.00     56962
   macro avg       0.94      0.70      0.77     56962
weighted avg       1.00      1.00      1.00     56962


Accuracy Score: 0.9988062216916541
```

6. Model Evaluation

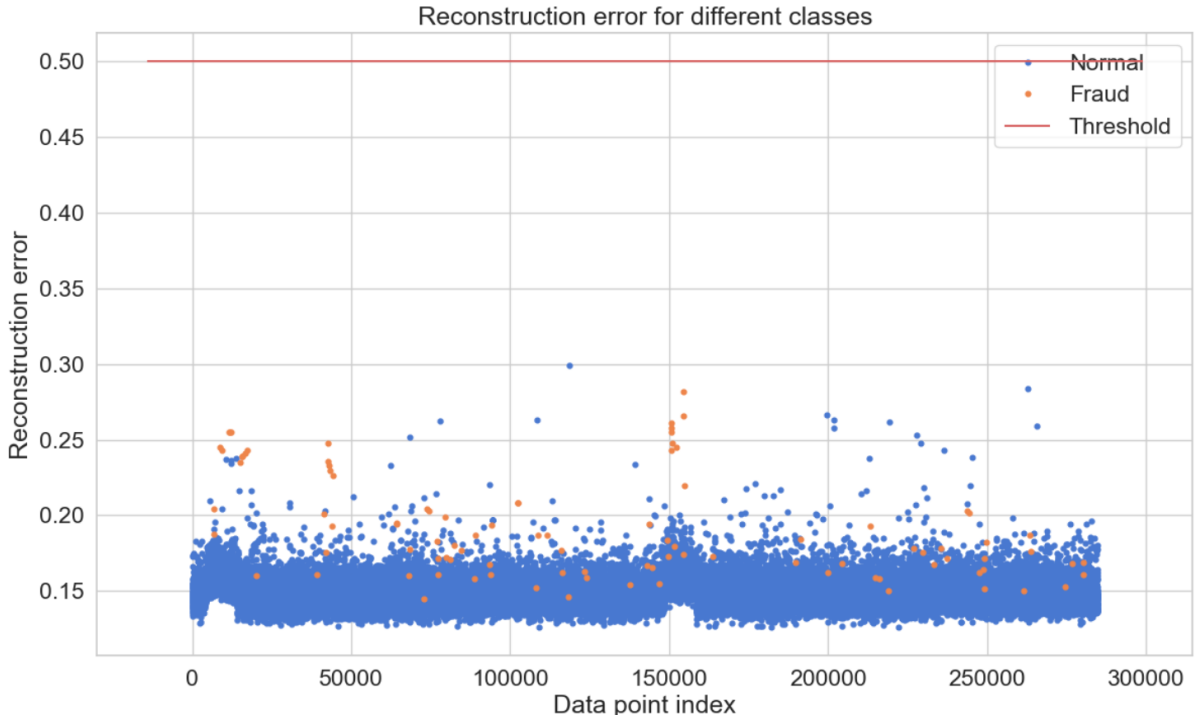
The classification report provides detailed insights into the performance of the logistic regression model for credit card fraud detection. Here are some key observations:



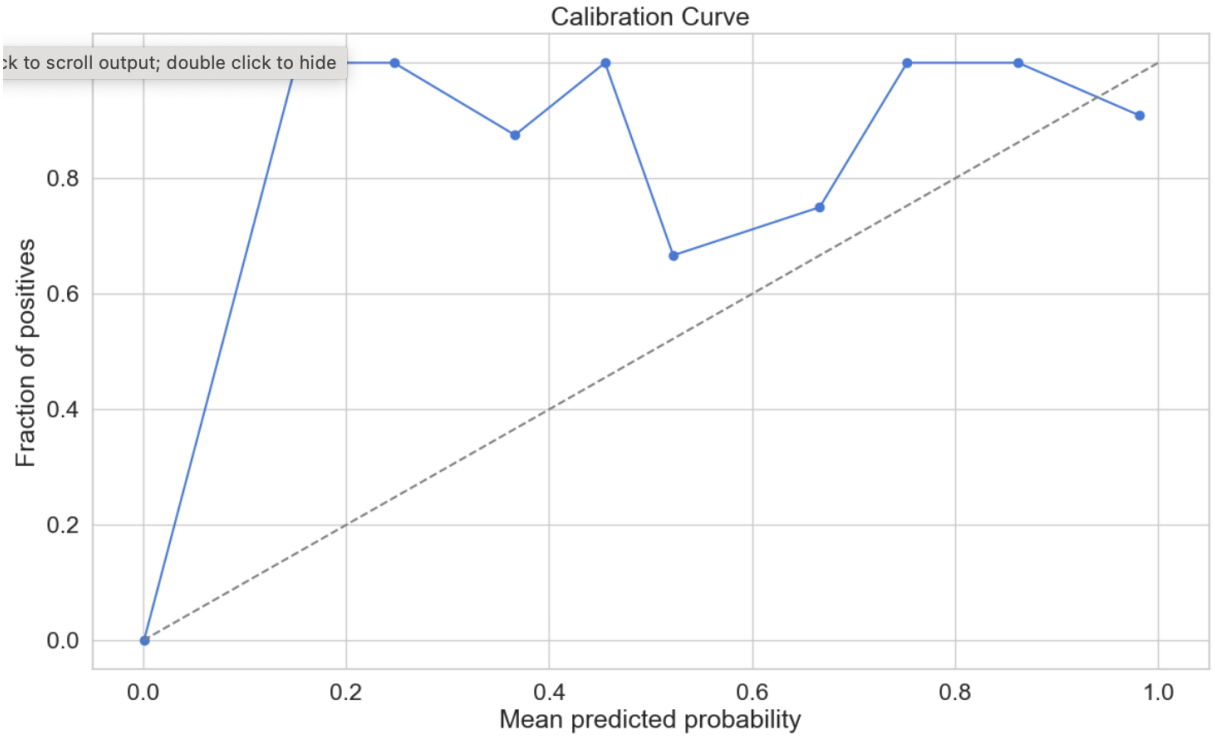
- **Precision and Recall**: The precision for non-fraudulent transactions (class 0) is exceptionally high, indicating that the model correctly identifies the vast majority of non-fraudulent transactions without misclassifying them as fraudulent. However, the precision for fraudulent transactions (class 1) is relatively lower, suggesting that there are false positives where normal transactions are misclassified as fraudulent. The recall for fraudulent transactions is also lower, indicating that the model fails to capture a significant portion of actual fraudulent transactions.



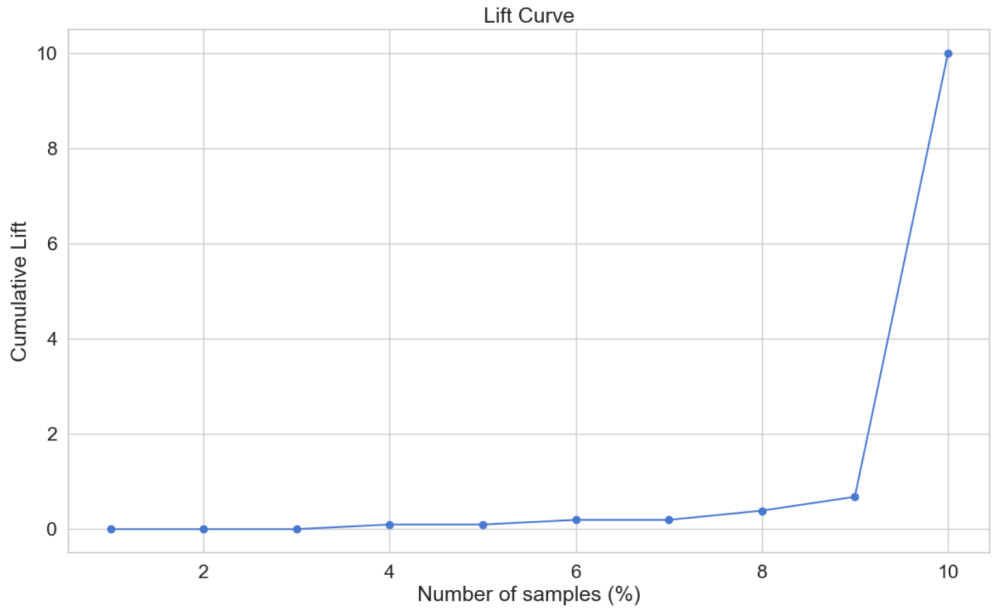
- **F1-Score**: The F1-score, which is the harmonic mean of precision and recall, is a balanced measure that considers both false positives and false negatives. For non-fraudulent transactions, the F1-score is near-perfect (1.00), reflecting the model's high accuracy in identifying non-fraudulent transactions. However, for fraudulent transactions, the F1-score is lower (0.59), indicating that there is room for improvement in correctly identifying fraudulent transactions while minimizing false positives.



- **Accuracy Score**: The overall accuracy score of the model is exceptionally high (0.9989), which might initially suggest excellent performance. However, due to the highly imbalanced nature of the dataset, where non-fraudulent transactions vastly outnumber fraudulent ones, accuracy alone might not be the most reliable metric for evaluating model performance. The high accuracy is largely driven by the correct classification of non-fraudulent transactions, while the relatively lower recall for fraudulent transactions indicates that the model may miss some instances of fraud.

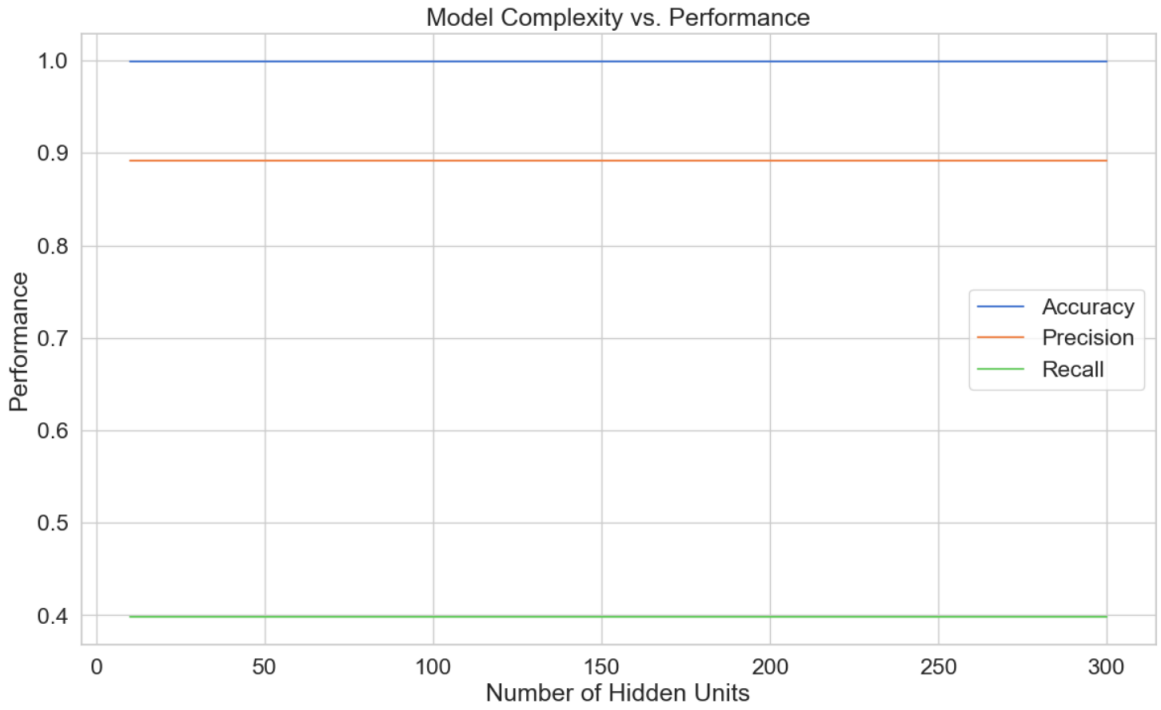


- **Insights**: The high precision for non-fraudulent transactions is crucial for minimizing false alarms and maintaining customer trust by avoiding unnecessary disruptions to legitimate transactions. However, the lower recall and precision for fraudulent transactions highlight the challenge of effectively identifying and mitigating fraud. False negatives (fraudulent transactions classified as non-fraudulent) can have significant financial implications for both consumers and financial institutions, underscoring the importance of improving the model's ability to detect fraudulent activity.



7. Conclusion and Recommendations

While the logistic regression model demonstrates impressive performance in accurately identifying non-fraudulent transactions, there is a clear opportunity for enhancement in detecting fraudulent transactions. To improve the model's effectiveness in fraud detection, several strategies can be considered:



- **Feature Engineering**: Exploring additional features or engineered features that capture subtle patterns indicative of fraudulent activity could enhance the model's discriminatory power.
- **Imbalanced Data Handling**: Implementing techniques such as oversampling minority class instances (fraudulent transactions) or using advanced algorithms specifically designed for imbalanced data can help address the imbalance issue and improve the model's ability to detect fraud.
- **Threshold Adjustment**: Fine-tuning the classification threshold based on the trade-off between precision and recall can optimize the model for detecting fraudulent transactions while minimizing false positives.
- **Ensemble Methods**: Leveraging ensemble learning techniques, such as combining multiple models or incorporating decision trees, can potentially enhance the model's robustness and performance in detecting fraudulent activity.

By iteratively refining the model and incorporating these recommendations, financial institutions can strengthen their fraud detection capabilities and effectively mitigate the risks associated with credit card fraud.