Credit Card Fraud Detection

Dexter Schincke

Bellevue University

DSC: 680

Amirfarrokh Iranitalab

15 December 2024

Credit Card Fraud Detection

Business Problem:

Credit card fraud is pervasive in the financial sector, resulting in billions of dollars in losses annually. As digital transactions grow, so does the sophistication of fraudulent schemes. Financial institutions need robust, efficient, and scalable tools to detect real-time fraudulent transactions. This project addresses this critical challenge by building a machine-learning model to classify transactions as fraudulent or legitimate based on transaction data.

- Research Questions:
    - What machine learning techniques are most effective for detecting fraudulent transactions in highly imbalanced datasets?
    - How can class imbalance in the dataset be effectively managed to improve fraud detection accuracy?
    - Which features in the transaction data contribute most significantly to identifying fraudulent behavior?
    - How does model performance vary across different machine learning algorithms, and which provides the best trade-off between precision and recall in fraud detection?

Background:

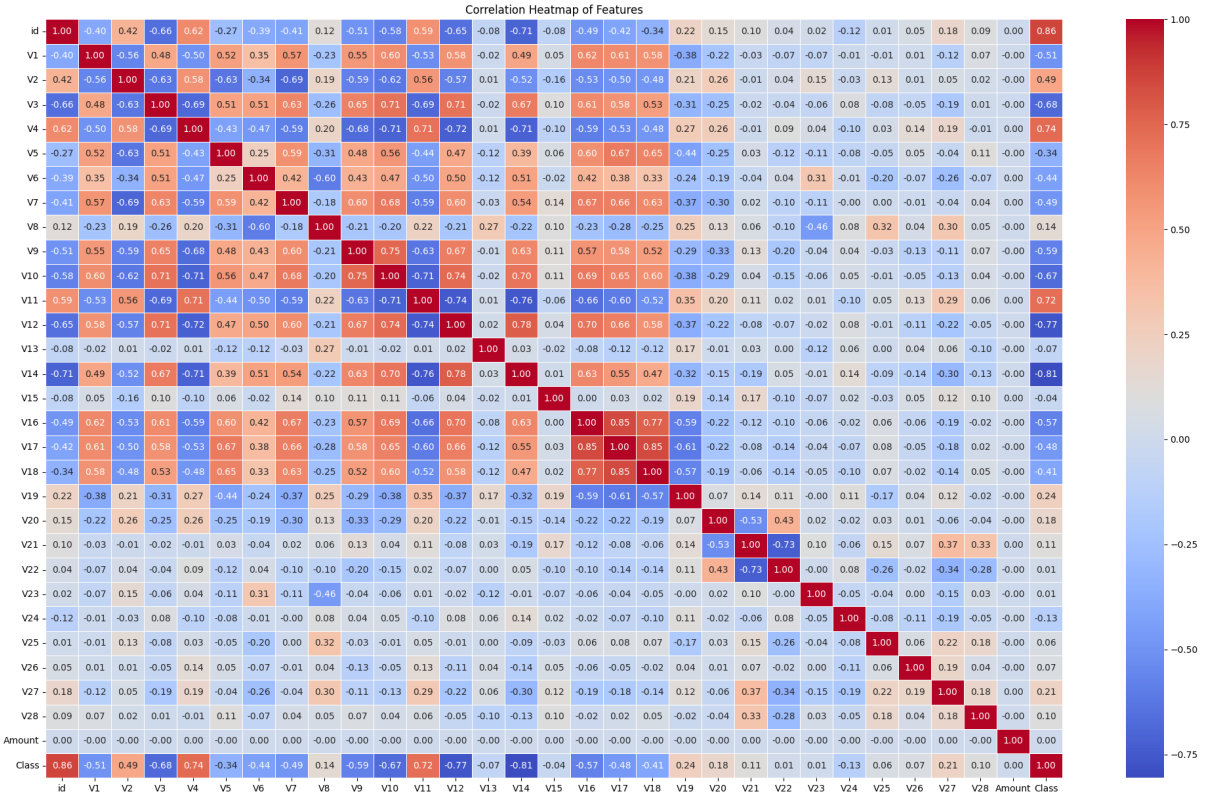
Credit card fraud has been an issue since the early days of electronic payments, initially tackled with manual and rule-based methods. As fraud tactics advanced, these approaches proved insufficient. Machine learning (ML) now plays a key role in fraud detection by analyzing transaction data to identify suspicious patterns. ML-based systems, particularly those using classification and anomaly detection, have replaced traditional methods to address the growing complexity of fraud with greater accuracy and automation.

Data Explanation:

This project uses a Kaggle Credit Card Fraud Detection dataset with approximately 570,000 transactions from 2023, featuring anonymized attributes (V1-V28), transaction amounts, and a target variable indicating whether a transaction is fraudulent (1) or legitimate (0). Since the data is anonymized, there is no risk of exposing sensitive information. Preliminary checks revealed no missing values or class imbalance, simplifying preprocessing. The data will be split into a training set (70%) and a testing set (30%) using sklearn's train_test_split, ensuring the model is well-evaluated and generalizes effectively to unseen data.

Methods:

After preprocessing, exploratory data analysis (EDA) will examine the distribution of fraudulent and legitimate transactions and the relationships between features, especially the anonymized ones (V1-V28). A correlation heatmap reveals strong correlations among V1-V19, with weaker patterns in V20-V28, providing insights into feature interactions.

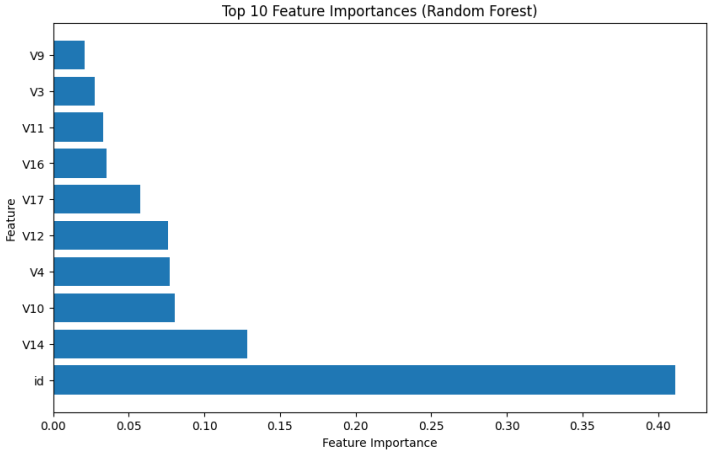


Logistic Regression will serve as a baseline for modeling due to its simplicity, followed by Support Vector Classifier (SVC), which optimizes hyperplanes to separate classes, and Random Forest, an ensemble method that aggregates predictions from multiple decision trees. Performance will be evaluated using metrics like accuracy, precision, recall, and F1-score, focusing on minimizing false negatives. A bar plot will compare model metrics, and Random Forest's feature importance analysis will identify key attributes for fraud detection. The best-performing model, such as the optimized SVC (C=10), will be selected for deployment, balancing performance and complexity.

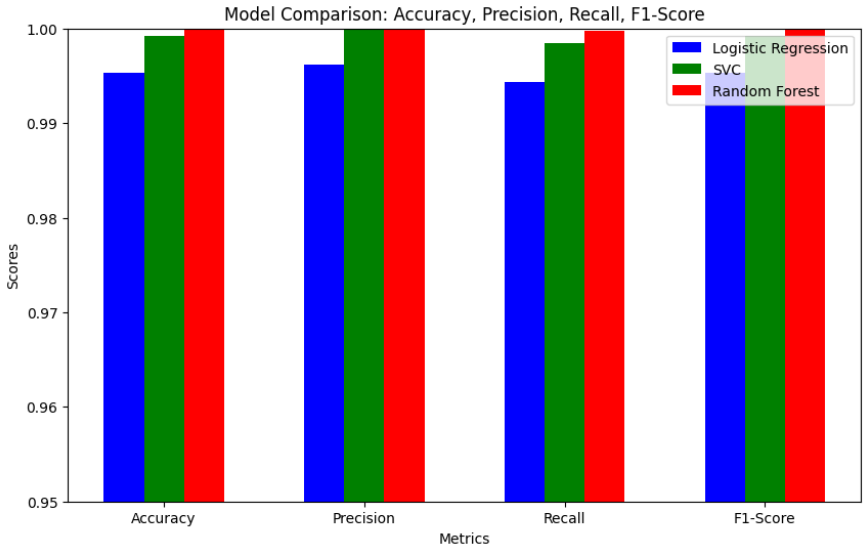
Analysis:

The models were evaluated using accuracy, precision, recall, F1-score, and confusion matrices to assess their performance in classifying fraudulent and legitimate transactions. Logistic Regression served as the baseline model, achieving good accuracy but requiring more

detailed metrics to evaluate its performance. The Support Vector Classifier (SVC) was fine-tuned with different regularization parameters (C=1 and C=10). This adjustment improved precision by better identifying fraudulent transactions, although recall slightly decreased.



The Random Forest Classifier, an ensemble model, provided the strongest performance across all metrics, demonstrating high precision, recall, and F1-score. Feature importance analysis revealed the most influential fraud detection features, helping to understand the model's decision-making process better. Overall, Random Forest outperformed Logistic Regression and SVC, making it the most suitable choice for this task.



Conclusion:

This project developed a machine-learning model for detecting fraudulent credit card transactions using a Kaggle dataset. The main challenge was accurately classifying transactions, and after evaluating several algorithms, Random Forest emerged as the most effective. It consistently outperformed Logistic Regression and SVC regarding precision, recall, and F1-score, crucial metrics for fraud detection.

The Random Forest model showed strong performance in training and testing, indicating its reliability for real-world applications. Future work could explore advanced techniques like Gradient Boosting or Deep Learning models for further improvements and refine feature engineering to enhance model performance. In conclusion, the Random Forest model is a promising solution for detecting credit card fraud, offering a solid foundation for financial institutions to combat fraud and improve security.

Assumptions:

The project assumed the dataset was balanced, with an equal distribution of fraudulent and legitimate transactions, allowing for direct model comparisons. It was also assumed that the anonymized features (V1-V28) and transaction amount provided sufficient information for detecting fraud. Aside from minor issues like missing values, the dataset was expected to be clean, and the fraud patterns in the training set would remain consistent in the test set and future data. Additionally, it was assumed that the feature set would remain the same in future datasets, enabling the model to be reused without significant retraining.

Limitations:

This project's main limitations include using an anonymized dataset, which limits interpretability, and the fact that the dataset, while balanced, may not reflect real-world fraud patterns, where fraudulent transactions are typically much less frequent. Additionally, the data is

limited to 2023 transactions, which may not capture long-term trends, and the models might still be prone to overfitting, affecting their generalization to new data.

Challenges/Issues:

One significant challenge in this project is ensuring that the models effectively differentiate between fraudulent and legitimate transactions despite the anonymized nature of the features, which limits interpretability. Overfitting remains a potential issue, as the models might perform well on the training data but fail to generalize to unseen transactions. To mitigate this, techniques such as cross-validation, regularization, and feature selection can be employed. Another challenge is scalability, as the model must efficiently handle large transaction volumes, enabling real-time detection without compromising accuracy or processing speed.

Future Uses:

The techniques developed in this project can extend beyond credit card fraud detection to other areas like insurance claims, online banking, and network security. Retailers could use similar models to detect return fraud, while healthcare applications might include spotting irregularities in billing or patient records. These adaptable methods offer value wherever identifying anomalies or malicious behavior is essential.

Recommendations:

For the business problem of credit card fraud detection, future work should consider implementing more advanced machine learning models, such as neural networks, which may capture more complex patterns in transaction data. Testing the model with real-time streaming data is also essential to evaluate its effectiveness in live fraud detection scenarios and improve its response time. To maintain the model's accuracy over time, updating the training dataset to reflect emerging fraud trends regularly is crucial. Additionally, integrating the model into a

broader fraud prevention system, with complementary rule-based checks and human oversight, would provide a more robust and reliable fraud detection solution, ensuring better protection for users and businesses.

Implementation Plan:

The first step in implementing this project is to deploy the chosen model in a controlled, offline testing environment to ensure it performs reliably with real-world transaction data. This includes monitoring its precision, recall, and false positive rates. Once validated, the model can be integrated into the payment processing system using scalable APIs or cloud-based platforms to handle the high volume of incoming transactions. Regular monitoring and periodic retraining will be essential to adapt to evolving fraud patterns. Additionally, the system should incorporate alert mechanisms, flagging suspicious transactions for further review by fraud analysts, ensuring a balance between automation and human oversight.

Ethical Considerations:

Data privacy is crucial, even with anonymized datasets, requiring strict adherence to regulations like GDPR. The model must be fair, avoiding biases that could disproportionately affect any group, and transparent, allowing stakeholders to understand its decisions. These measures foster trust, accountability, and responsible use in fraud detection systems.

Potential Questions:

1. How did you handle potential overfitting in your models?
2. What was the reasoning behind selecting the specific machine learning models (Logistic Regression, SVC, Random Forest)?
3. Can you explain the impact of feature scaling in your models, especially since some features are monetary values?

4. Why did you choose precision, recall, and F1-score as your evaluation metrics over others like accuracy or ROC-AUC?
5. What insights did the correlation heatmap provide, and how did it affect your modeling decisions?
6. Were there any challenges or difficulties working with anonymized features (V1-V28)?
7. How would you adapt your approach if the dataset was highly imbalanced?
8. What measures would you take to ensure the model can be deployed for fraud detection in a real-world, high-volume setting?
9. How do you ensure that your model is not biased or unfair to certain demographic groups?
10. What would you do if the model performs well on the training data but not on the testing set?

References

Projects/Papers:

Abueltouh, A. (2024). Credit Card Detection. Kaggle. https://www.kaggle.com/code/abdallahabuelftouh/credit-card-detection

Fatima, S. (2024). Credit card fraud detection: Achieving 99% accuracy. Kaggle. https://www.kaggle.com/code/samanfatima7/credit-card-fraud-detection-achieving-99-acc

GeeksforGeeks. (2024, September 6). ML credit card fraud detection. GeeksforGeeks. https://www.geeksforgeeks.org/ml-credit-card-fraud-detection/

Ileberi, E., Sun, Y., & Wang, Z. (2022). A machine learning-based credit card fraud detection using the GA algorithm for feature selection. Journal of Big Data, 9, 24. https://doi.org/10.1186/s40537-022-00573-8

Datasets:

Elgiriye Withana, N. (2023). Credit card fraud detection dataset 2023. Kaggle. https://www.kaggle.com/datasets/nelgiriyewithana/credit-card-fraud-detection-dataset-2023/data