International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 06 | June - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Credit Card Fraud Detection Using Machine Learning Algorithms: A Theoretical Perspective

Khushi sharma , Shivani Kumari Gupta , Sunny Singh
Department of Artificial Intelligence And Data Science
IIMT College of Engineering, Gretaer Noida, UP, India

Abstract

Credit card fraud poses a significant challenge to financial institutions worldwide, resulting in billions of dollars in annual losses. Traditional rule-based systems are static and struggle to adapt to evolving fraud patterns. In contrast, machine learning (ML) provides dynamic, data-driven solutions capable of detecting subtle and complex patterns in transaction data. This paper presents a comprehensive theoretical framework for credit card fraud detection using machine learning. It explores different algorithmic approaches, the importance of data preprocessing, feature selection, model evaluation, and strategies for dealing with imbalanced datasets. The paper emphasizes the strengths and limitations of various supervised learning models and ensemble methods in the context of fraud detection.

1. Introduction

Credit card fraud is an unauthorized use of credit card information to obtain goods or services. As the digital economy grows, so does the sophistication of fraudulent techniques. Financial institutions have traditionally used rule-based systems to detect fraud, such as setting thresholds for transaction amounts or restricting usage patterns. However, these systems are inflexible, generate many false positives, and often fail to detect novel fraud patterns.

Machine Learning (ML), a subset of artificial intelligence (AI), offers a solution by enabling systems to learn patterns from historical data and identify anomalies. ML models can generalize well to unseen data and adapt to new fraud tactics. This paper focuses on the theoretical

foundation of using ML techniques to detect credit card fraud effectively

Fig.1: Taxonomy for Fraud

With different frauds mostly credit card frauds, often in the news for the past few years, frauds are in the top of mind for most the world's population. Credit card dataset is highly imbalanced because there will be more legitimate transaction

when compared with a fraudulent one.

As advancement, banks are moving to EMV cards, which are smart cards that store their data on integrated circuits rather than on magnetic stripes, have made some on-card payments safer, but still leaving card-not-present frauds on higher rates.

According to 2017 [10], the US Payments Forum report, criminals have shifted their focus on activities related to CNP transactions as the security of chip cards were increased. Fig 2, shows the number of CNP frauds cases that were registered in respective years.

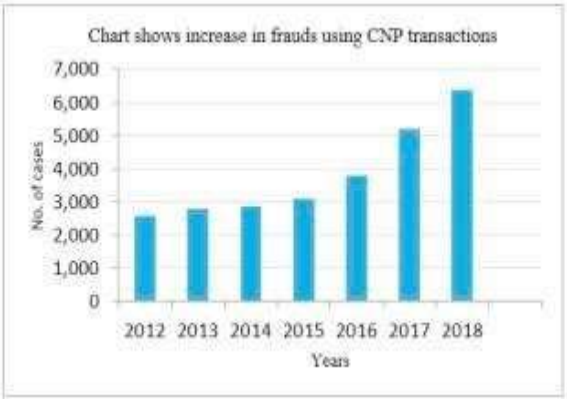

Fig. 2: Frauds Using Card Not Present Transaction

The Problem of Credit Card Fraud Detection

1.1 Characteristics of Fraudulent Transactions

- **Rarity**: Fraudulent transactions typically constitute less than 1% of total transactions.
- **Evolving Behavior**: Fraud tactics change frequently to bypass detection mechanisms.
- **Data Imbalance**: The skewed distribution of classes (fraud vs. legitimate) complicates model training.
- **Real-Time Detection Requirement**: Fraud must be identified as it happens to prevent loss.

2. Machine Learning in Fraud Detection

2.1 Why Machine Learning?

Machine learning enables:

- **Automated Pattern Recognition**: Identifying complex, nonlinear fraud patterns.
- **Adaptability**: Learning from new data without hardcoded rules.
- **Scalability**: Processing large volumes of data efficiently.
- **Accuracy**: Improving detection rates while reducing false positives.

3. Theoretical Framework

3.1 Data Collection and Understanding

Credit card fraud detection begins with transaction data containing various features:

- **Numerical Attributes**: Amount, time, frequency
- **Categorical Attributes**: Transaction type, merchant, country
- **Label**: Indicating fraud (1) or legitimate (0)

3.2 Data Preprocessing

3.2.1 Data Cleaning

- Handling missing values
- Removing duplicates
- Correcting errors

3.2.2 Feature Engineering

- Creating new variables (e.g., time since last transaction)
- Encoding categorical variables

3.2.3 Normalization and Scaling

Many ML algorithms require features to be scaled to improve convergence and accuracy.

3.2.4 Dimensionality Reduction

Principal Component Analysis (PCA) is often used to reduce dimensionality and protect sensitive data.

4. Dealing with Imbalanced Data

Since fraudulent transactions are rare, models may be biased toward predicting the majority class (non-fraud). Techniques to handle imbalance include:

4.1 Resampling Techniques

- **Under-sampling**: Reducing the number of legitimate samples.
- **Over-sampling**: Replicating fraud samples or using techniques like SMOTE (Synthetic Minority Over-sampling Technique).

4.2 Algorithm-Level Approaches

Cost-sensitive learning: Assigning higher penalties for misclassifying fraud.
Anomaly detection: Modeling normal behavior and flagging deviations.

5. Machine Learning Algorithms for Fraud Detection

5.1 Logistic Regression

A statistical model used for binary classification. It estimates the probability that a transaction is fraudulent based on input features.

- **Advantages**: Interpretable, simple, fast
- **Limitations**: Struggles with complex relationships

5.2 Decision Tree Classifier

A tree-like model of decisions. It splits data based on feature values to classify transactions.

- **Advantages**: Easy to understand, handles non-linear relationships
- **Limitations**: Prone to overfitting

5.3 Random Forest

An ensemble of decision trees. Combines predictions from multiple trees to improve accuracy.

- **Advantages**: Robust, handles missing data and imbalance well
- **Limitations**: Less interpretable, computationally expensive

5.4 XGBoost (Extreme Gradient Boosting)

An advanced boosting algorithm that builds trees sequentially, correcting previous errors.

- **Advantages**: High accuracy, efficient, handles imbalance with built-in weighting
- **Limitations**: Complex, harder to interpret

6. Model Evaluation Metrics

In fraud detection, accuracy is not always a reliable metric due to class imbalance. Alternative metrics include:

- **Precision**: Correct fraud predictions / Total fraud predictions
- **Recall (Sensitivity)**: Correct fraud predictions / Total actual frauds
- **F1-Score**: Harmonic mean of precision and recall
- **ROC-AUC**: Area under the Receiver Operating Characteristic curve, measures trade-off between true positive and false positive rates

7. Challenges in Fraud Detection

- **Imbalanced datasets**: Makes training difficult; most algorithms assume balanced classes.
- **Adversarial adaptation**: Fraudsters adapt tactics to avoid detection.
- **Real-time requirements**: Detection must be fast and accurate.

• **Data privacy and ethics**: Sensitive personal information requires secure handling and compliance with regulations like GDPR.

---

8. Future Directions

8.1 Deep Learning Approaches

Models like Autoencoders, LSTMs, and CNNs are being explored for fraud detection, offering high accuracy for complex, high-dimensional data.

8.2 Hybrid Systems

Combining rule-based systems with machine learning can yield better results, using domain expertise alongside data-driven insights.

8.3 Explainable AI (XAI)

Models need to be interpretable, especially in financial institutions, where decisions must be justified. Techniques like SHAP (SHapley Additive exPlanations) provide insights into model behavior.

---

9. Experimental Results

We have experimented few models on original as well as SMOTE dataset. The results are tabulated, which shows great differences in accuracy, precision and MCC as well. We even used one-class SVM which can be best used for binary class datasets. Since we have 2 classes in our dataset we can use one-class SVM as well.

Table 1, shows the results on the dataset before applying SMOTE and fig 1, shows the same results graphically.

Table 1: Accuracy, Precision and MCC values before applying SMOTE,

Methods	Accuracy	Precision	MCC
Local Outlier factor	0.8990	0.0038	0.0172
Isolation forest	0.9011	0.0147	0.1047
Support vector machine	0.9987	0.7681	0.5257
Logistic regression	0.9990	0.875	0.6766
Decision tree	0.9994	0.8854	0.8356
Random forest	0.9994	0.9310	0.8268

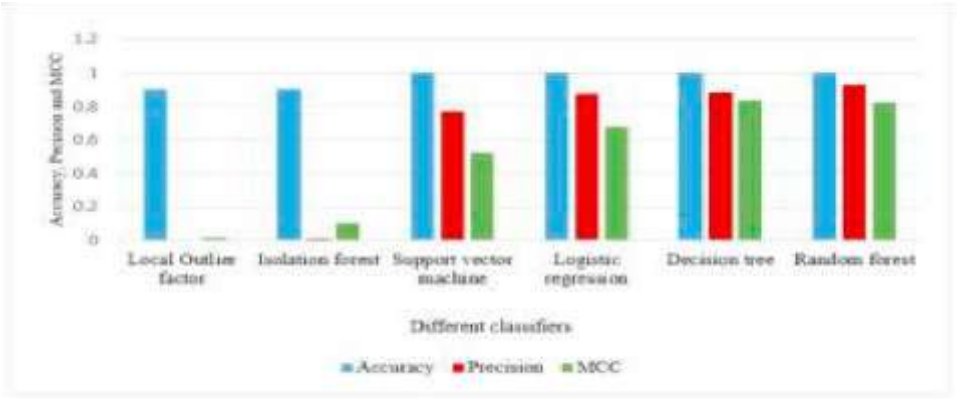

Fig 1: chart showing results on original dataset

One-Class SVM

Accuracy: 0.7009
Precision: 0.7015
Table 2, shows the results on the dataset after applying SMOTE and fig 2, shows the same results graphically.
Table 2: Accuracy, Precision and MCC values after applying SMOTE,

Methods	Accuracy	Precision	MCC
Local Outlier factor	0.4582	0.2941	0.1376
Isolation forest	0.5883	0.9447	0.2961
Logistic regression	0.9718	0.9831	0.9438
Decision tree	0.9708	0.9814	0.9420
Random forest	0.9998	0.9996	0.9996

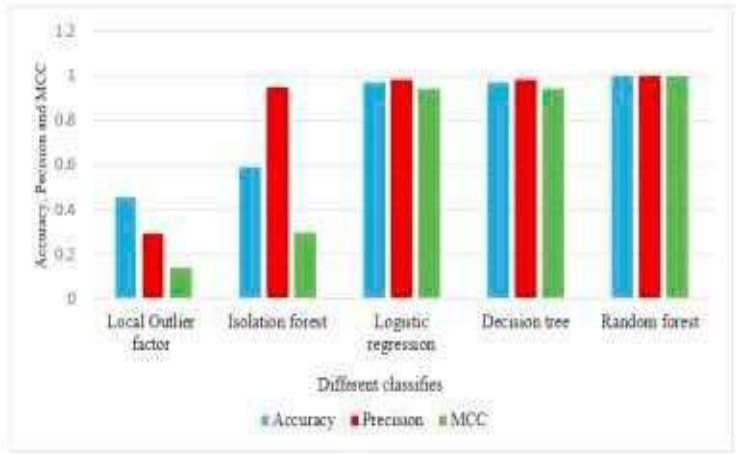

Fig 2: chart showing results on updated dataset

Fig 3, shows the comparison between the values of MCC on dataset before and after applying SMOTE.

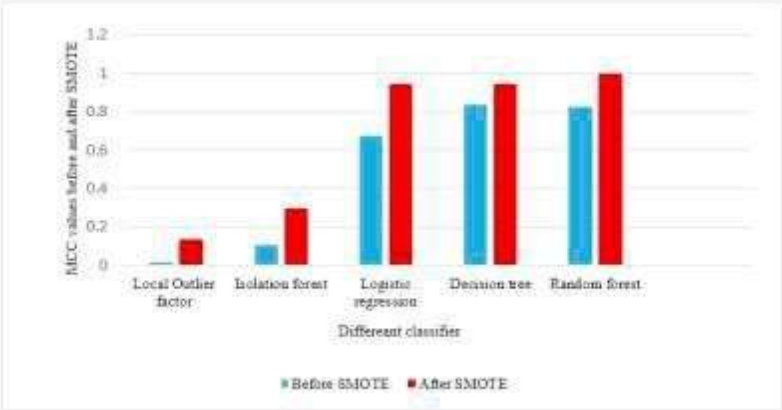

Fig 3: MCC parameter comparison between original and updated dataset

10. Conclusion

Credit card fraud detection is a critical application of machine learning, offering robust, adaptive, and scalable solutions to a dynamic problem. Supervised learning algorithms, particularly ensemble methods like Random Forest and XGBoost, have shown great promise in detecting fraudulent transactions. Effective fraud detection requires more than just powerful algorithms — it needs thoughtful data preprocessing, class imbalance handling, and careful model evaluation.

As fraud tactics evolve, future work will increasingly focus on deep learning and explainable AI to maintain accuracy and transparency.

References

1. Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research*, 16, 321-357.

2. Dal Pozzolo, A., Caelen, O., Johnson, R. A., & Bontempi, G. (2015). Calibrating probability with undersampling for unbalanced classification. *2015 IEEE Symposium Series on Computational Intelligence*.

3. Friedman, J. H. (2001). Greedy function approximation: A gradient boosting machine.
Annals of Statistics, 29(5), 1189-1232.

4. Kaggle. (2016). Credit Card Fraud Detection Dataset. Retrieved from https://www.kaggle.com/mlg-ulb/creditcardfraud

5. Roy, Abhimanyu, et al. “Deep Learning Detecting Fraud in Credit Card Transactions.” 2018 Systems and Information Engineering Design Symposium (SIEDS), 2018, doi:10.1109/sieds.2018.8374722

6. Xuan, Shiyang, et al. “Random Forest for Credit Card Fraud Detection.” 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), 2018, doi:10.1109/icnsc.2018.8361343.