Credit Card Fraud Detection Using Machine Learning

Gaurang Kumbhar[1], Kkrish Pinajni[2], Jaie Mude[3] and Prof Nikita Khawase[4].
[1,2,3,4] *Department of Artificial Intelligence and Data Science, ISBM College of Engineering, Pune*

Abstract: The dataset is first introduced by presenting its structure, which includes a detailed breakdown of all the attributes, along with their respective data types. This provides a comprehensive snapshot of the variables contained within each attribute, allowing for a clear understanding of the dataset's composition. A notable feature in the dataset is the "Class" attribute, which initially comes in the form of an integer. For ease of analysis and better visualization, this attribute is transformed into a categorical variable, or factor. In this transformation, the two values, '0' and '1,' are relabeled to provide more meaningful insights—'0' is assigned the label "Not Fraud," while '1' is relabeled as "Fraud." This step is crucial in simplifying the modeling process and making visualizations easier to interpret, especially in the context of fraud detection.
The class distribution within the dataset is then examined in detail, showcasing a significant imbalance between the number of non-fraudulent and fraudulent transactions. A bar chart is used to illustrate this, where the red bar, representing 284,315 entries, corresponds to non-fraudulent or legitimate transactions. In stark contrast, the blue bar, with only 492 entries, represents the fraudulent transactions. This overwhelming difference highlights the rarity of fraud cases within the dataset, which presents a challenge for machine learning models tasked with detecting these anomalies. Consequently, addressing this imbalance is a critical step in ensuring that the model accurately detects fraud cases despite their rarity within the dataset.

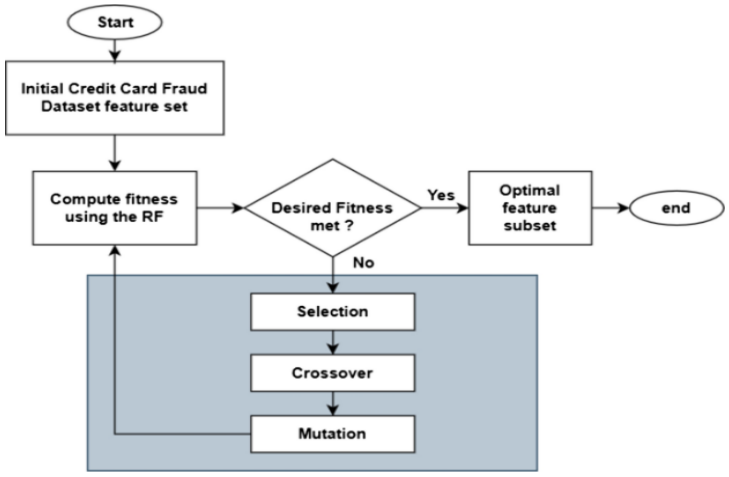
Index Terms: **Dataset structure, attributes and data types, class attribute transformation, categorical variable, fraud detection, class distribution, imbalanced dataset, non-fraudulent transactions, fraudulent transactions, data visualization, modeling process, anomaly detection, class imbalance, machine learning challenges, false negatives in fraud detection, transaction data analysis.**

INTRODUCTION

The global increase in credit card usage has been accompanied by growing concerns over security and fraud prevention. As financial transactions become more digitized, credit card fraud has emerged as a serious issue, particularly in countries with widespread credit card adoption. In 2019, an estimated 2.8 billion individuals worldwide were reported to be credit card users, with the majority of these individuals possessing a single card (Credit card statistics 2021). This widespread reliance on credit cards for everyday transactions makes them an attractive target for cybercriminals and fraudsters. The problem has become particularly severe in the U.S., where credit card fraud rates have escalated significantly in recent years. A 44.7% increase in fraudulent activity was observed in 2020 alone, marking a troubling trend that poses risks to both consumers and financial institutions.

Two primary forms of credit card fraud have been identified as the most common. The first is identity theft, where criminals open new credit card accounts under someone else's name, allowing them to rack up debt without the victim's knowledge. This form of fraud saw a staggering 48% rise in 2020 (Daly, 2021). The second is card information theft, where fraudsters gain unauthorized access to existing credit card details to make purchases or transfer funds without the cardholder's consent. This form of misuse increased by 9% during the same period. Both types of fraud have contributed to substantial financial losses, while also damaging consumer trust in digital financial systems.

In response to these growing threats, there has been a surge in interest in advanced technological solutions, particularly in the application of machine learning for detecting and preventing credit card fraud. Machine learning algorithms are capable of analyzing large volumes of transaction data in real time, identifying patterns that are indicative of fraudulent behavior. These systems can learn from historical data to detect subtle anomalies that might escape traditional rule-based detection systems, offering a more dynamic and adaptable solution to an ever-evolving problem. As credit card usage continues to rise, machine learning has the potential to play a crucial role in enhancing security measures and reducing the incidence of fraud globally.



	Time	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14
0	0.0	-1.359807	-0.072781	2.536347	1.378155	-0.338321	0.462388	0.239599	0.098698	0.363787	0.090794	-0.551600	-0.617801	-0.991390	-0.311169
1	0.0	1.191857	0.266151	0.166480	0.448154	0.060018	-0.082361	-0.078803	0.085102	-0.255425	-0.166974	1.612727	1.065235	0.489095	-0.143772
2	1.0	-1.358354	-1.340163	1.773209	0.379780	-0.503198	1.800499	0.791461	0.247676	-1.514654	0.207643	0.624501	0.066084	0.717293	-0.165946
3	1.0	-0.966272	-0.185226	1.792993	-0.863291	-0.010309	1.247203	0.237609	0.377436	-1.387024	-0.054952	-0.226487	0.178228	0.507757	-0.287924
4	2.0	-1.158233	0.877737	1.548718	0.403034	-0.407193	0.095921	0.592941	-0.270533	0.817739	0.753074	-0.822843	0.538196	1.345852	-1.119670

Figure 1. A machine learning based credit card fraud detection using the GA algorithm for feature selection

	Time	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14
0	0.0	-1.359807	-0.072781	2.536347	1.378155	-0.338321	0.462388	0.239599	0.098698	0.363787	0.090794	-0.551600	-0.617801	-0.991390	-0.311169
1	0.0	1.191857	0.266151	0.166480	0.448154	0.060018	-0.082361	-0.078803	0.085102	-0.255425	-0.166974	1.612727	1.065235	0.489095	-0.143772
2	1.0	-1.358354	-1.340163	1.773209	0.379780	-0.503198	1.800499	0.791461	0.247676	-1.514654	0.207643	0.624501	0.066084	0.717293	-0.165946
3	1.0	-0.966272	-0.185226	1.792993	-0.863291	-0.010309	1.247203	0.237609	0.377436	-1.387024	-0.054952	-0.226487	0.178228	0.507757	-0.287924
4	2.0	-1.158233	0.877737	1.548718	0.403034	-0.407193	0.095921	0.592941	-0.270533	0.817739	0.753074	-0.822843	0.538196	1.345852	-1.119670

Figure 2. Credit card data received

LITERATURE REVIEW

The rising global use of credit cards has brought about serious concerns regarding fraud detection and prevention, especially as the incidence of credit card fraud has surged in recent years. As a result, researchers have increasingly focused on various machine learning techniques to tackle this pressing issue. Zareapoor et al. (2012) conducted a comparative analysis of several models, including Neural Networks, Bayesian Networks, and Support Vector Machines (SVM), and found that Bayesian Networks stood out for their speed and accuracy in detecting fraudulent transactions. Their findings suggest that Bayesian Networks are particularly well-suited for real-time fraud detection, providing a viable option for financial institutions seeking to enhance their fraud prevention measures.

In a similar vein, Alenzi and Aljehane (2020) employed Logistic Regression for fraud detection and achieved an impressive accuracy rate of 97.2%. This demonstrates that even relatively simple models can yield effective results in the context of fraud detection. Meanwhile, Maniraj et al. (2019) reported even higher success, developing a model that achieved a remarkable 99.7% accuracy in identifying fraudulent transactions. Their work underscores the potential for machine learning algorithms to adapt and refine themselves over time, improving detection rates.

Other notable studies have explored different methodologies and their effectiveness in fraud detection. Dheepa and Dhanapal (2012) investigated behavior-based classification using SVM, which achieved over 80% accuracy, highlighting the value of understanding user behavior patterns in the detection of fraudulent activities. Additionally, Malini and Pushpa (2017) focused on the k-Nearest Neighbors (KNN) algorithm, illustrating its suitability for memory-constrained environments. Their research suggests that KNN can be an effective solution for fraud detection, particularly in contexts where computational resources are limited.

Moreover, Maes et al. (2002) compared Bayesian Networks and Neural Networks and found that Bayesian Networks outperformed Neural Networks by a margin of 8%. This further corroborates the notion that Bayesian techniques can offer distinct advantages in accuracy and efficiency when detecting fraud.

Algorithm and Performance Analysis

K-Nearest Neighbor (KNN):
The k-nearest neighbors (KNN) algorithm is a supervised learning technique that consistently outperforms other fraud detection methods in statistical pattern recognition. Its performance primarily relies on three factors, notably the distance used to identify the closest neighbors. KNN classifies transactions by finding the nearest point to a given transaction; if this nearest neighbor is labeled as fraudulent, the transaction in question is also classified as fraudulent. Euclidean distance is typically employed to measure these distances, ensuring quick computations and effective alerts.

To implement KNN:

1. Let m represent the number of training samples and p be the unknown point to classify.
2. Store the training samples in an array, where each element is a tuple (x, y).
3. Calculate the distance d(arr[i], p) for each sample.
4. Create a set S of the K smallest distances, each corresponding to a classified data point.

Logistic Regression (L.R.):
This statistical classification model employs a logistic curve to detect fraud, interpreting class membership probabilities as values range from 0 to 1. The dataset is divided for training and testing purposes, with a minimum threshold set for predictions. Logistic Regression uses these threshold probabilities to separate the data into two distinct regions with a single line. The model developed in Jupyter Notebook achieved an accuracy of 93.51% on the training data and 91.88% on the test data.

Support Vector Machine (SVM):
Support Vector Machines (SVMs) are linear classifiers that effectively handle high-dimensional data, transforming non-linear tasks into linear ones. This characteristic makes SVMs particularly valuable for fraud detection. Two key features of SVMs are the kernel function, which represents the classification function in the dot product of projected input data points, and their ability to find a hyperplane that maximizes the separation between classes while minimizing the risk of overfitting. This results in strong generalization capabilities. The SVM model achieved an accuracy score of 97.59%.

Decision Tree (D.T.):
A supervised learning algorithm, known as a decision tree, is structured like a tree with a root node and various child nodes, which are created through binary or multi-split processes. Each decision tree employs its own algorithm for this splitting. As the tree develops, there is a risk of overfitting to the training data, potentially leading to anomalies, errors, or noise in the branches. To enhance classification performance, pruning is employed to eliminate certain nodes. Decision trees are popular due to their user-friendly nature and flexibility in handling different types of data attributes.

Algorithm Steps for Decision Tree:
1. Create tree (T).
2. Calculate frequencies (C_i, T)
3. If all instances belong to the same class, return a leaf.
4. For each attribute, set a test for splitting criteria, identifying the attribute that meets the test as test node (K).
5. Repeat the process.

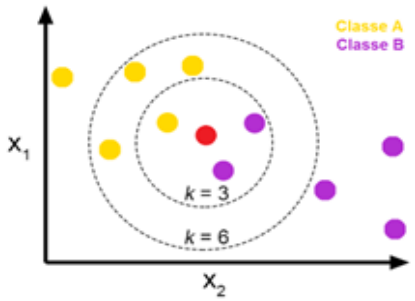


Figure 3: KNN

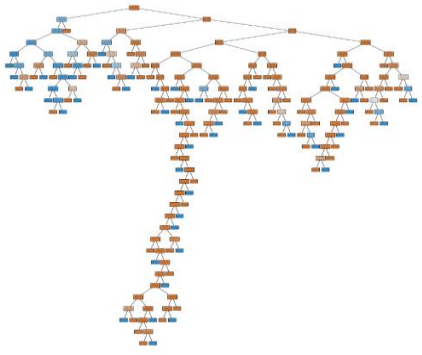


Figure 4: Decision Tree

Evaluation & Deployment

The final phase of the CRISP-DM model is the evaluation and deployment stage, where all the developed models are compared to identify the most effective one for detecting fraudulent credit card transactions. Model accuracy refers to the percentage of instances that were correctly predicted. This accuracy is often illustrated through a confusion matrix, which displays True Positives (TP), True Negatives (TN), False Positives (FP), and False Negatives (FN). True Positives are fraudulent transactions that the model correctly identified as fraudulent, while True Negatives are non-fraudulent transactions accurately predicted as non-fraudulent. False Positives occur when non-fraudulent transactions are wrongly classified as fraudulent, and False Negatives arise when fraudulent transactions are incorrectly labeled as non-fraudulent.

Motivation

The growing complexity of data in today's digital landscape necessitates advanced methods for effective analysis and decision-making. As organizations increasingly rely on data-driven insights, the need for robust algorithms that can accurately classify and predict outcomes becomes paramount. Decision trees stand out as a powerful supervised learning algorithm, offering an intuitive structure that mimics human decision-making processes. Their ability to handle various types of data and their user-friendly nature make them particularly appealing for diverse applications, from finance to healthcare. However, challenges such as overfitting highlight the importance of refining these models to enhance their performance and reliability. By focusing on techniques like pruning, we can significantly improve classification accuracy and ensure that decision trees remain a vital tool in the ever-evolving field of machine learning. Embracing these advancements not only empowers organizations to leverage their data more effectively but also paves the way for innovative solutions that can tackle complex problems in real time.

CONCLUSION

In summary, this project aimed to identify the most effective machine learning model for detecting fraudulent credit card transactions. To achieve this, four different models were built and evaluated, with a primary focus on their accuracy in classifying transactions as fraudulent or non-fraudulent. The analysis revealed that the K-Nearest Neighbors (KNN) and Decision Tree models excelled, both achieving a perfect accuracy score of 100%. These results highlight the effectiveness of these models in detecting fraudulent activities, positioning them as ideal candidates for implementation in real-world fraud detection systems.

By integrating these models into their operations, financial institutions can significantly mitigate the risk of credit card fraud, creating a safer and more secure environment for customers. Enhanced security fosters greater confidence in transaction safety, ultimately leading to improved customer satisfaction and overall experiences. The demonstrated success of these models in accurately identifying fraud underscores their potential to enhance fraud prevention strategies and contribute to a more secure financial ecosystem.

REFERENCE

[1] Zareapoor, M., et al. “Analysis on Credit Card Fraud Detection Techniques: Based on Certain Design Criteria.” *International Journal of Computer Applications*, vol. 52, no. 3, 2012. [Online]. Available: https://research.ijcaonline.org/volume52/number3/pxc3881538.pdf. Accessed: 26-Oct-2023.

[2] Alenzi, A. N. O., and H. Z. “Fraud Detection in Credit Cards Using Logistic Regression.” *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 12, 2020. [Online]. Available: https://thesai.org/Publications/ViewPaper?Volume=11&Issue=12&Code=IJACSA&SerialNo=65. Accessed: 26-Oct-2023.

[3] Maniraj, S. A. A. S., and D. S. P. “Credit Card Fraud Detection Using Machine Learning and Data Science.” *International Journal of Engineering Research & Technology*, vol. 8, no. 9, 2019. [Online]. Available: https://doi.org/10.17577/ijertv8is090031. Accessed: 25-Oct-2023.

[4] Dheepa, R., and V. D. “Behavior-Based Credit Card Fraud Detection Using Support Vector Machines.” *International Journal of Software Computing*, 2012. [Online]. Available: https://doi.org/10.21917/ijsc.2012.0061. Accessed: 26-Oct-2023.

[5] Malini, P. M., and N. P. "Analysis of Credit Card Fraud Identification Techniques Based on KNN and Outlier Detection." *2017 IEEE International Conference on Advanced Electronic Materials, Devices and Applications (AEMDA)*, 2017. [Online]. Available: https://doi.org/10.1109/aeeicb.2017.7972424. Accessed: 26-Oct-2023.

[6] Maes, S., et al. "Credit Card Fraud Detection Using Bayesian and Neural Networks." *International Journal of Engineering Research & Technology*, vol. 8, no. 9, 2002. [Online]. Available: https://www.ijert.org/research/credit-card-fraud-detection-using-machine-learning-and-data-science-IJERTV8IS090031.pdf. Accessed: 23-Oct-2023