Motivation

The issue of credit card fraud is prevalent in the modern world and is one of the most important threats to businesses, companies and consumers' finances. The current location-based payments and e-commerce are proving to be difficult when it comes to fraud detection. Rule-based systems that are used conventionally have inherent problems, namely, they cannot be adjusted for new kinds of fraud or their indicators, which in turn leads to two main inefficiencies: a significant increase in the number of false positives or complete failure to notice fraudulent activities. These limitations justify the use of sophisticated methods for dealing with the high levels and fluctuating nature of transactional data.

Through machine learning methods we can diagnose fraudulent credit card transactions. Machine learning models use huge amounts of historical transaction data to 'look in between the lines' and detect subtleties as fraud indications. These types of models are highly extensible, and they are also viable options for totally real-time fraud detection systems. Furthermore, the approach proposed herein offers an opportunity to increase the effectiveness of detection while reducing the number of false alarms and, therefore, to improve users' trust and performance in the financial environment.

Research Question

The project seeks to address the question: "Which machine learning model demonstrates the highest effectiveness for detecting fraudulent credit card transactions?"

Literature Review

Financial fraud has emerged as an increasingly pervasive threat, with far-reaching implications for the finance industry, corporate organizations, and governments [1]. In the field of payments using credit cards as a mode of payment preferred today security has been a subject of worry due to increased cases of fraud. Credit card fraud detection (CCFD) is the activity, which takes an attempt to distinguish between the fraudulent and genuine transactions by taking into account the patterns of the consumption and deviations from the patterns. But the handling of this problem has some difficulties: fraud patterns are not stationary, fraud datasets are inherently imbalanced, it is also challenging to select the proper features and the proper evaluation metrics for this type of data [2]. Machine learning is widely adopted in CCFD where different methods are used to detect fraud and differentiate normal and anomalous activity patterns. For example, Random Forests (RF) is a stable classification algorithm which training uses decision trees in order to increase the probability of correct classification. Compared to other models, RF performs extremely well for large, overly unbalanced datasets, as it combines contribution of multiple trees reducing a disadvantage of individual tree such as over- fitting. However, despite RF being efficient, it is precise in classification problems, though it performs poorly in some regression tasks and is sensitive to variance in large datasets that need more refined adjustments [3]. Nonetheless, because of the aforementioned characteristic of RF it is still the most useful approach to perform the CCFD for the data set in question because of the high robustness of the algorithm.

Another algorithm is the Support Vector Machines (SVM) which is also used in classification model for detecting fraud. SVM specifically searches for a legitimate and fraudulent transactions' feature space, and develops decision boundaries for them. The key factor is that this method demonstrates high efficiency on small and very structured data sets, achieving high accuracy with a small number of features added. Nonetheless, the computations for SVM become expensive for realtime applications specially on large databank containing more than 100,000 records. These restrictions make it less suitable for use in high velocity transactional situations [4].

KNN, under the family of supervised learning algorithms have been seen effective in detecting fraudulent activities during transactions. In other words, KNN analytically identifies and models outliers in transactional data by measuring correlation coefficients or distances between transaction points. Due to the nature of this research, this method proves most effective in low memory and low computation contexts while also outperforming other methods in reducing false

alarms while preserving overall detection efficacy [5,6] However, the detection of anomalies very much depends on the quality of the data set and the parameters set, which somewhat reduces the applicability of KNN compared with other approaches based on anomalies.

At its simplest, Logistic Regression (LR) allows an easy and understandable way of detecting fraud which comprises of regression analysis of the connection between predictor variables and a response variable that is binary in nature. That is why this model is most valuable precisely in understanding how different predictors affect the probability of fraudulent transactions. Although the method is not as complex as in other techniques, the usage of linear models may not reveal many features of datasets [7].

Another often used technique in CCFD is Decision Trees (DT) owing to their fast calculations, easy implementation, and the fact that they can deal with noise. Since DT models divide datasets repeatedly, the resulting models are easy to explain to the audience and are also hierarchical in nature, which are always wanted by researchers as well as practitioners. However, DT models can over-fit the data they are trained on and, therefore, may not work well when applied to different data; this is averted by fine tuning such as shrinking the trees or using a bagging model [8].

Another important issue relates to the dependent variable, which is common for credit card fraud datasets – these data are typically private, and the problem is concentrated in the fact that fraudulent controls are relatively rare. Previous research has mitigated these issues by employing oversampling, undersampling strategies and synthesis of datasets. Some algorithms like RF, DT, and KNN are known to help in training skewed data distribution; SVM and LR have been applied on small subset data for fraudlist identification.

Fraud datasets employed for the research purposes are typically considered as private and possess a high separation between the objects: many normal transactions, few fraudulent ones. Previous work in this area has applied techniques like SMOTE, undersampling methods, and cost-sensitive approaches, for adequate training of the models. Both classification and regression models in this project also use similar pre-processing techniques in order to balance classes of a dataset for better prediction of machine learning models. RF and DT approaches have been used earlier with success to handle imbalanced data; whereas, SVM and KNN are used to identify local fraud patterns.

The reuse of the five techniques involves the analysis of the results of the decision-making procedure on new imbalanced data sets and the comparison of the resulting accuracy. The project proposes the use of RF and DT for their applicability to large datasets, SVM due to precision in the small feature subsets KNN for proficiency in anomaly detection, and LR as a base model. Therefore, through comparing of these techniques, this project aims to find out which algorithms or what combined algorithms are the most efficient in detecting frauds in credit card transactions. Furthermore, it will be possible to learn from the outcomes of reusing these methods to veil over the solutions to some of the shortcomings; for instance, Scala SVM and the tendency of DT to over-fit. Finally, this paper's comprehensive evaluation of several methods will help improve the general understanding of fraud detection concepts and their real-world implementation.

Data Sources

The dataset was retrieved from an open-source website, Kaggle.com.

Dataset 1

- Size:284,807 rows, 31 columns
- Key Features: Anonymized features (V1 to V28), Time (contains the elapsed seconds between the first and other transactions of each attribute), Amount (amount of each transaction), and Class (contains binary variables where "1" is a case of fraudulent transaction, and "0" is not as case of fraudulent transaction).
- Relevance: Provides a balanced mix of features for fraud detection, making it ideal for evaluating machine learning models.

Dataset 2

- Size: 568,630 rows, 31 columns

- Key Features: Similar structure to Dataset 1, including ID, anonymized features, Amount, and Class.
- Relevance: Larger dataset size allows for testing model scalability and robustness.

Dataset 3

- Size: 150,000 rows, 32 columns
- Key Features: Includes Time, transaction-specific features (feat1 to feat28), Transaction_Amount, and IsFraud (fraud indicator).
- Relevance: Adds diversity to the data with slightly different feature representations and labeling, aiding model generalizability.

These datasets collectively provide sufficient scale, diversity, and relevant features to critically evaluate various machine learning techniques for fraud detection.

Identification of Machine Learning Methods

1. Random Forest: Random Forest is one of the group methods that uses multiple decision trees to get better estimation of the results as well as to avoid high variance. The technique works very well when dealing with the big data sets that are skewed like the ones used in credit card fraud detection. In detail, it offers feature important metrics, which are valuable for understanding which attributes define fraudulent transactions. Its noise tolerance and capability to handle large datasets make it suitable for this project.
2. Logistic Regression: As it has been mentioned earlier Logistic Regression provides a straightforward interpretable model for binary classification task which can serve as a baseline. It assists in the creation of basic understanding of patterns that exist in features and the possibility of fraud. Although it fails to detect elaborate structure it provides similarities in terms of easier implementation and greater performance in large sample size.
3. K-Nearest Neighbor: KNN is an instance of non-parametric algorithm which working is based on the comparison of transaction features to other examples. It is relatively easy to use and can find local anomalies that may be interesting for exploratory purposes. However, making optimization for KNN to fit the big data requirement ensures that the issue of computational complexity and imbalanced training data is solved.
4. Decision Tree: Decision Trees are easy to interpret models that mimic the normal decision-making process of an individual. They are efficient in the process of identifying decisive characteristics that separate fraudulent from real transactions. Nonetheless, such obvious over-fitting can be alleviated by using blurring techniques such as pruning or combining with other ensemble procedures, making them effective for examination from first perspectives and or features.
5. Support Vector Machine: SVM is a very powerful model if used for high dimensional data sets, it has good classification power. Both linear and RBF kernels are used to test it on simple and complicated patterns. Even though SVM requires great computational resources, this method stands as a strong approach to separative decision boundaries between fraud transactions and genuine ones.

Identification of Evaluation Methods

To evaluate the performance of the chosen machine learning techniques in detecting fraudulent credit card transactions, the following methods will be applied. Each method is selected for its relevance to specific challenges in classification tasks, particularly in the context of imbalanced datasets.

1. Accuracy: Accuracy calculates the percentage of the right labelled transactions with respect to the total number of observations. A major disadvantage of accuracy is that it affords a general assessment of model performance but does not represent the performance of minority classes in big data sets that present an imbalance.

2. Precision: Precision then measures the ratio of true positive values out of all positive values as predicted by the classifier. This is especially important in fraud detection since any errors mean more leads that would be investigated are from legitimate users.
3. Recall: Recall calculates the degree of true positives predictions in relation to all the real positives. To reduce incidences of financial losses, it is central for identifying all fraudulent transactions.
4. F1-Score: The F1-Score gets as the so called 'harmonic mean' of the Precision and the Recall, so it offers a good middle ground between both. It is very helpful when false classifications of either positive or negative are costly for the organization or the project.
5. Cohen's Kappa Score: Cohen's Kappa evaluates the concordance of a model's predictions to its results taking into consideration coincidences that were bound to happen by chance. It is very helpful for models that could be prone to overfitting the majority class.
6. Matrix of Correlation Coefficient (MCC): MCC measures the quality of the binary classification even in case of sparse class constellations and takes all the values of the confusion matrix into account. It is less subjective than Accuracy to give a review of the articles.
7. Matrix of Confusion: The Confusion Matrix is an eye-opener for model predictions giving detailed outputs of true positive, true negative, false positive, false negative. This visualization helps in the identification of certain types of errors.
8. ROC-AUC Score: The performance of the model can be calculated using the Receiver Operating Characteristic (ROC) which measures how well a model discriminates between two classes using the Area Under the Curve (AUC) summing up the overall results. It is especially useful for comparing tradeoffs of true positives against false positives, and so on.

Bibliography

[1] J. O. Awoyemi, A. O. Adetunmbi and S. A. Oluwadare, "Credit card fraud detection using machine learning techniques: A comparative analysis," 2017 International Conference on Computing Networking and Informatics (ICCNI), Lagos, Nigeria, 2017, pp. 1-9, doi: 10.1109/ICCNI.2017.8123782.

[2] F. N. Ogwueleka, "Data Mining Application in Credit Card Fraud Detection System", Journal of Engineering Science and Technology, vol. 6, no. 3, pp. 311-322, 2011.

[3] Bin Sulaiman, R., Schetinin, V. & Sant, P. Review of Machine Learning Approach on Credit Card Fraud Detection. Hum-Cent Intell Syst 2, 55–68 (2022). https://doi.org/10.1007/s44230-022-00004-0

[4] Sriram Sasank JVV, Sahith GR, Abhinav K, Belwal M. Credit card fraud detection using various classification and sampling techniques: a comparative study. In: IEEE, 2019. p. 1713–1718.

[5] Alam MN, Podder P, Bharati S, Mondal MRH. Effective machine learning approaches for credit card fraud detection. Cham: Springer; 2021.

[6] Itoo F, Meenakshi SS. Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection. Int J Inf Technol. 2020;13:1503–11. https://doi.org/10.1007/s41870-020-00430-y.

[7] H. Z. Alenzi and N. O. Aljehane, "Fraud Detection in Credit Cards using Logistic Regression," International Journal of Advanced Computer Science and Applications, vol. 11, (12), 2020.

[8] Gaikwad, J.R., Deshmane, A.B., Somavanshi, H.V., Patil, S.V. and Badgujar, R.A., 2014. Credit card fraud detection using decision tree induction algorithm. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 4(6), pp.2278-3075.