RESEARCH ARTICLE

RSP Science Hub

International Research Journal on Advanced Science Hub
2582-4376
www.rspsciencehub.com
Vol. 06, Issue 06 June

Check for updates

http://dx.doi.org/10.47392/IRJASH.2024.020

Enhancing Credit Card Security with Machine Learning Fraud Detection

Pallavi

Computer Science and Engineering, Vidya Vihar Institute of Technology, India.

Email ID: *pallavijoshi800@gmail.com*

Article history

Received: 13 May 2024
Accepted: 20 May 2024
Published: 05 June 2024

Keywords:
Credit Card Fraud, Machine Learning Models, Random Forest, Oversampling Techniques, Performance Evaluation

Abstract

Lastly, evaluating machine learning models in the context of credit card fraud detection and categorization can yield important insights into their performance across diverse settings. After looking at F-score, recall, accuracy, and precision metrics, it's evident that Random Forest consistently outperforms other models, showing how well it handles class imbalances. Random Forest can continue to perform well even in balanced datasets by utilizing oversampling strategies to achieve class balance. This makes it an even more effective model. Because of its adaptability and reliability, the model is thus ideal for application in actual fraud detection systems. The consistent performance of ensemble, Logistic Regression, and Gradient Boosting approaches in fraud detection tasks demonstrates the necessity of utilizing a variety of machine learning algorithms and oversampling tactics to increase classification performance. The effectiveness of Random Forest in minimizing class differences and the significance of a balanced training dataset are both highlighted by these results. In sum, this study's results will aid in the development of more reliable machine learning models for fraud detection, which in turn will have practical applications in domains such as finance. Future research could look into other optimization tactics and ensemble approaches to see whether they help the model perform better in real-world scenarios.

1. Introduction

The issue of credit card fraud (Figure 1) has become a global concern in the financial transactions domain, posing significant challenges for financial institutions and consumers alike. A commensurate increase in the susceptibility to fraudulent activities has resulted from the widespread use of electronic payments and online transactions. Often, traditional rule-based fraud detection algorithms are not very good at identifying complex and dynamic fraud patterns [1] – [5]. Consequently, there exists an increasing need for sophisticated methodologies, such as machine learning, to proficiently identify and alleviate instances of credit card fraud. Machine learning (ML) methodologies present a potentially effective strategy for addressing credit card fraud through analysing massive volumes of financial data in search of questionable patterns. Using these methods, financial institutions like banks can detect fraud more accurately, reduce the number of false positives, and react quickly to emerging fraud patterns. Because of its incredible learning and adaptability, machine learning makes it easier to detect credit card fraud [6-10]. Machine learning algorithms can constantly search through financial records for signs of fraud. Since they can adapt their models in real-time according to input, they are also better at detecting fraud schemes that were previously unseen. Credit card fraud detection has

made use of a wide variety of supervised, unsupervised, and semi-supervised machine learning algorithms. Train supervised learning algorithms like logistic regression, decision trees, random forests, and support vector machines using labelled datasets that contain both valid and fraudulent transactions.

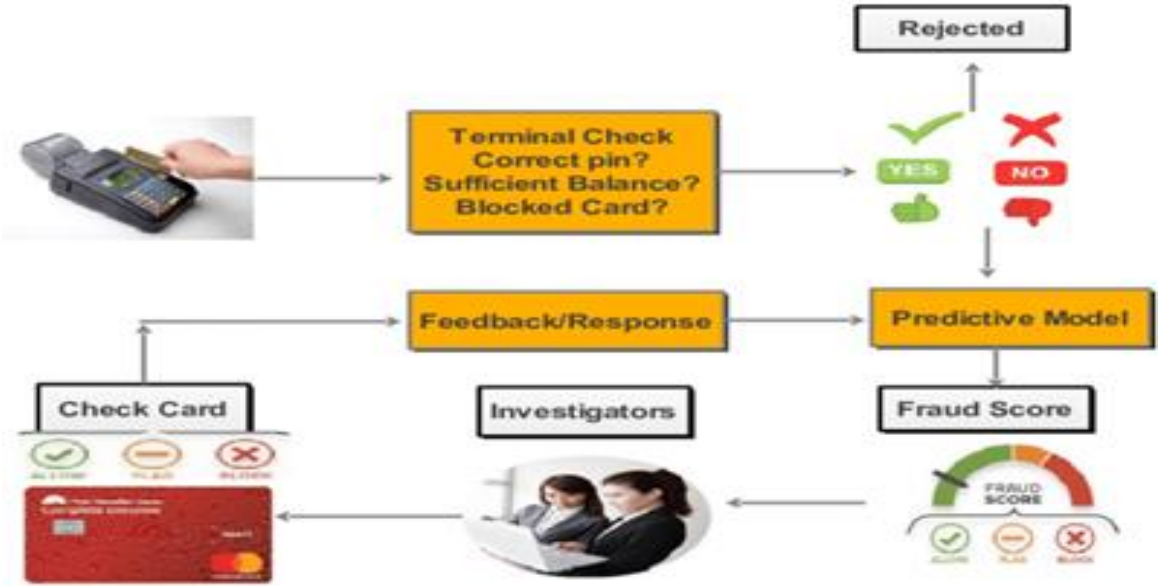

Figure 1 Credit Card Fraud Detection

In order to identify if future transactions are legitimate or fraudulent, this system learns from patterns in the training dataset. When there is a lack of labelled data, unsupervised learning algorithms are great for identifying fraudulent transactions. Among these approaches are clustering algorithms like K-means clustering and anomaly detection methods like exclusion forests and auto encoders. When applied to transactional data, this technique reveals irregularities that deviate significantly from the norm. Hybridizing supervised and unsupervised learning techniques is the name of the game when it comes to computational strategies. It completes its mission in this way. Just how? That is, by merging a smaller labeled dataset with a bigger one. This approach does double duty: it streamlines ML model training while faithfully portraying the complex nature of fraud.the numbers 6–10. Credit card fraud detection relies heavily on feature engineering, a component of which is the selection of appropriate machine learning algorithms. The user's actions, the type of merchant, the time and location of the transaction, and the total amount could all be indicators of fraudulent activity. Many procedures, such as feature selection, dimensionality reduction, and data pre-treatment methods, are involved in making machine learning models perform better. These methods might help us whittle down the irrelevant information and get down to brass tacks. To sum up, combating fraudulent financial transaction activity requires a data-centric and proactive approach, and machine learning algorithms provide just that. Banks' digital fraud detection systems might benefit from more complex algorithms, continuous learning, and careful feature engineering to improve accuracy and performance. Businesses and consumers alike can rest easy knowing that this strategy has their backs.to be located on pages [11–14].

2. Literature Review

Salekshahrezaee 2023 as well as coworkers have discovered this to be accurate. This study compares Principal Component Analysis (PCA) with Convolutional Autoencoder (CAE) and examines the feature extraction performance of ensemble classifiers such as XGBoost, Random Forest, CatBoost, and LightGBM with the purpose of detecting credit card fraud. Some of the data sampling methods that we tested were Is Tomek, Random Undersampling (RUS), and SMOTE. Both the area under the curve (AUC) and the F1 score are important performance indicators. The findings demonstrate that the optimal strategy for identifying credit card fraud is to combine RUS with CAE [15].

Prabhakaran 2023 et al. With the goal of identifying and categorizing credit card fraud, this study introduces the OCSODL-CCFD approach, a feature selection strategy based on oppositional cat swarm optimization that is deep learning-based. It uses a novel OCSO-based feature selection algorithm to pick the optimal subset of characteristics. Familiar frameworks for fraud classification include the bidirectional gated recurrent unit (BiGRU) and the chaotic krill herd algorithm (CKHA). By utilizing CKHA, the hyperparameters of BiGRU are fine-tuned. Multiple simulations have proven that OCSODL-CCFD is the best approach. On a broad variety of evaluation metrics, its performance outperforms rival models [16]. Salekshahrezaee 2023 et al. Using the credit card fraud ensemble classifier datasets from XGBoost, Random Forest, LightGBM, and CatBoost, this study compares the two preprocessing methods. We examine how Principal Component Analysis (PCA) and Convolutional Autoencoder (CAE) extract features and draw comparisons between the two. Specifically, we evaluate RUS, Is Tomek, and SMOTE's ability to retrieve datasets with a high concentration of minority populations. Area The F1 score and area under the curve (AUC) are two metrics that evaluate how well a classification system performs. The findings indicate that a combination of the RUS and CAE approaches is the most effective approach to detect credit card fraud [17]. Prabhakaran 2023 et al. The OCSODL-CCFD approach is detailed in this research; it integrates a convolutional neural network (CCFD) model with an innovative feature selection mechanism based on op-positional cat swarm optimization. Credit card fraud detection and classification is the primary focus of the OCSODL-CCFD method. The OCSODL-CCFD approach creates a new feature selection method based on OCSO for optimal feature subset selection. We also use the BiGRU framework to classify credit card frauds and the chaotic krill herd algorithm (CKHA) to tweak the model's hyperparameters. It took a lot of simulation tests to prove that the OCSODL-CCFD model was better. When compared side by side, the OCSODL-CCFD model performed better across the board in the exhaustive evaluation [18]. Mniai 2022 et al. The OCSODL-CCFD approach is detailed in this research; it integrates a convolutional neural network (CCFD) model with an innovative feature selection mechanism based on op-positional cat swarm optimization. Credit card fraud detection and classification is the primary focus of the OCSODL-CCFD method. The OCSODL-CCFD approach creates a new feature selection method based on OCSO for optimal feature subset selection. We also use the BiGRU framework to classify credit card frauds and the chaotic krill herd algorithm (CKHA) to tweak the model's hyperparameters. It took a lot of simulation tests to prove that the OCSODL-CCFD model was better. When compared side by side, the OCSODL-CCFD model performed better across the board in the exhaustive evaluation [3].

Table 1 Literature Summary

Author /Year	Method	Results	Ref
Singh/ 2022	Hybridization of firefly algorithm and support vector machine for credit card fraud detection.	FFSVM method outperforms non-optimization machine learning techniques in fraud detection.	[3]
Sasikala/2022	Credit card fraud detection using SVM with hyper parameter optimization.	SVM with hyper parameter optimization enhances credit card fraud detection accuracy.	[4]
Zhang/ 2022	Anomaly detection using Isolation Forest improves credit card fraud detection.	Isolation Forest and OCSVM significantly enhance credit card fraud detection.	[19]
Plakandaras/ 2022	Automated Just-Add-Data system enhances credit card fraud detection efficiency.	Just-Add-Data system efficiently detects credit card fraud in transactions.	[20]
Kochhar/2021	Various classifiers that are logistic regression, naive Bayes, AdaBoost, and voting classifiers applied to imbalanced dataset for credit card fraud detection.	Multiple classifiers tested for credit card fraud detection performance analysis.	[21]

2.1 Research Gap

The use of machine learning for the purpose of detecting credit card fraud is fraught with difficulties. Dealing with skewed datasets when fraudulent transactions are in the minority should be your top priority. Traditional algorithms may face difficulties in the presence of class imbalance, which could lead to inaccurate predictions. The dynamic nature of fraud also calls for continuous fine-tuning of machine learning algorithms. Accurately identifying emerging fraud tactics is critical. Establishing confidence and complying with regulatory standards both necessitate that models be interpretable and explainable. Furthermore, models must be able to generalize well to different datasets and fraud scenarios. It is critical to have reliable systems for transfer learning. More importantly, there is a great deal of concern about the possibility of malicious assaults on machine learning models. Research into adversarial robustness and the safety of models is highly important. In addition, getting accurate real-time fraud detection is still a huge challenge. Effective algorithms that can handle a high volume of transactions are in high demand. The only way to overcome these challenges is for experts in machine learning, cybersecurity, and finance to work together across disciplines. In order to tackle credit card theft more effectively, fraud detection systems based on machine learning can overcome these hurdles.

3. Research Methodology

Gathering data, namely a fictitious credit card transaction record covering 2019 and 2020, is the first step. In order to analyze consumer activity and prevent fraud, this log is vital. The data is then pre-processed to ensure its integrity by handling null values and merging the train and test sets. Data patterns can be better understood with the help of EDA's statistical and visual tools. Logistic regression, SVMs, gradient boosting, random forests, and ensemble systems are all part of machine learning. Binary classification tasks become more interpretable with the help of logistic regression. If you're looking to improve the accuracy of your predictions over time, gradient boosting is the way to go, and Support Vector Machines (SVMs) are great for classification and regression. Ensemble learning integrates numerous models to enhance prediction accuracy, making it applicable to numerous domains, whilst the random forest approach provides robustness against overfitting. Proposed Flowchart is shown in Figure 2.

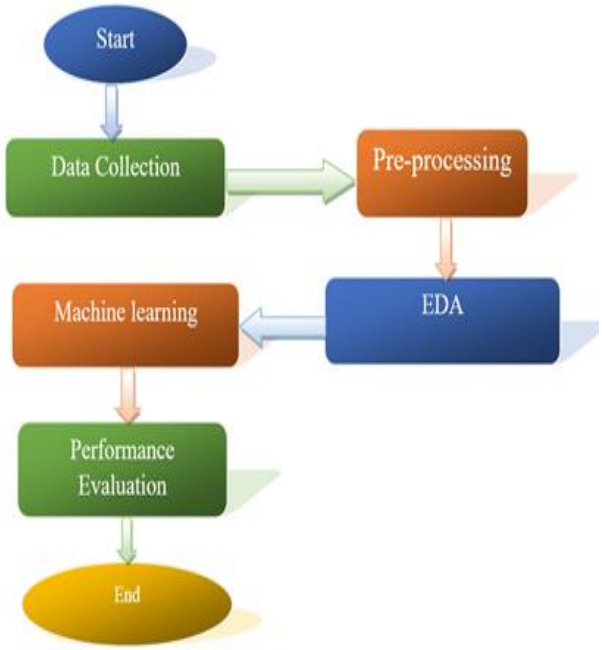

Figure 2 Proposed Flowchart

3.1 Data Collection

This study relied on data found at [22]. All the way from January 1, 2019, all the way up to December 31, 2020, this dataset has an imaginary record of credit card transactions. It deals with both legitimate and unethical business dealings. A thousand clients' purchases from 800 different stores are all part of this dataset. Each entry contains a plethora of information about the transaction, including the date and time, the merchant's name, the type of transaction, the amount, the cardholder's details (name, address, date of birth, and gender), the transaction number, the Unix time, and a flag that indicates there might have been fraud. This dataset contains a wealth of information regarding fraud, consumer habits, and enterprises. Even if it's virtual, it helps with building analytical methodologies and machine learning models to optimize business strategy and enhance transaction security.

3.2 Data Pre-processing

Data pre-processing involves performing several necessary procedures to ensure the dataset is free of errors and suitable for analysis. Making sure data is

accurate starts with finding and fixing duplicate or null values. Using a mixed train/test dataset ensures that preparation procedures are consistent. Enhancing the dataset's readability and performance follows the removal of unnecessary columns. To make sure the scales are consistent, normalize the numerical variables. After that, separate the numerical and category columns for analysis. By laying the groundwork for future study through the enhancement of datasets, the aforementioned strategy makes model construction and insight extraction more feasible. In order to take class imbalance a step further, we also quantify the frequencies of each class in the original dataset. Following the implementation of data balancing processes, such as down sampling, the following step is to reevaluate the class frequencies in the downsampled dataset. To ensure that all classes have an equal opportunity to improve the modeling's accuracy, we next determine what percentage of the downsampled dataset goes to each. Your dataset will be ready for detailed analysis and trustworthy model training after these pre-processing steps.

3.3 EDA

To better understand data properties, spot trends, and isolate outliers, exploratory data analysis (EDA) use visual and statistical tools. A few important processes include applying descriptive statistics to summarize the dataset, creating a data distribution visualization, and examining the correlations between variables using tools like scatter plots, correlation analysis, and heatmap visualization. By illuminating the dataset's patterns, structures, and possible problems, EDA allows for more reliable decision-making. It prepares the way for more advanced analysis or modeling by laying the framework for more data exploration and hypothesis testing.

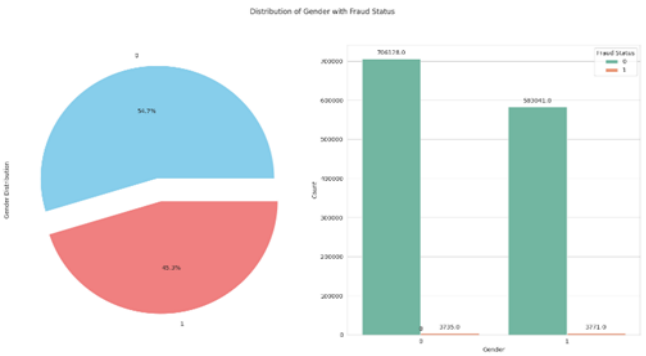

Figure 3 Count Plot of Distribution of Gender with Fraud Status

Gender distribution and fraud status are shown in Figure 3. A total of 65.3% of the pie slices are marked as 1, while 34.7% are marked as 0. The bar graph shows the total number of fraud cases for men and women specifically.

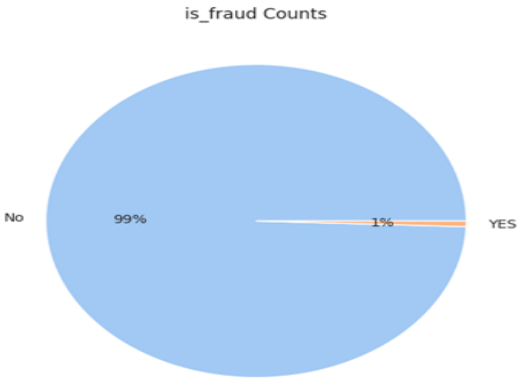

Figure 4 Pie Chart of is Fraud Count

To better understand data properties (Figure 4), spot trends, and isolate outliers, exploratory data analysis (EDA) use visual and statistical tools. A few important processes include applying descriptive statistics to summarize the dataset, creating a data distribution visualization, and examining the correlations between variables using tools like scatter plots, correlation analysis, and heatmap visualization. By illuminating the dataset's patterns, structures, and possible problems, EDA allows for more reliable decision-making. It prepares the way for more advanced analysis or modeling by laying the framework for more data exploration and hypothesis testing.

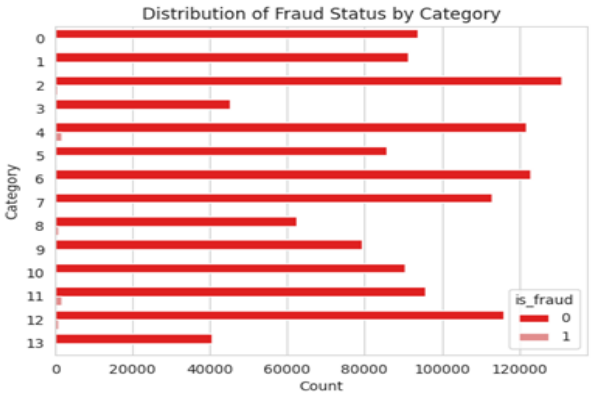

Figure 5 Count Plot of Distribution of Fraud Status by Category

An infographic titled "Distribution of Fraud Status by Category" (Figure 5) shows the overall count of fraud and non-fraud instances across various

categories. The red bars indicate instances of fraud, while the gray bars reflect non-fraudulent incidents.

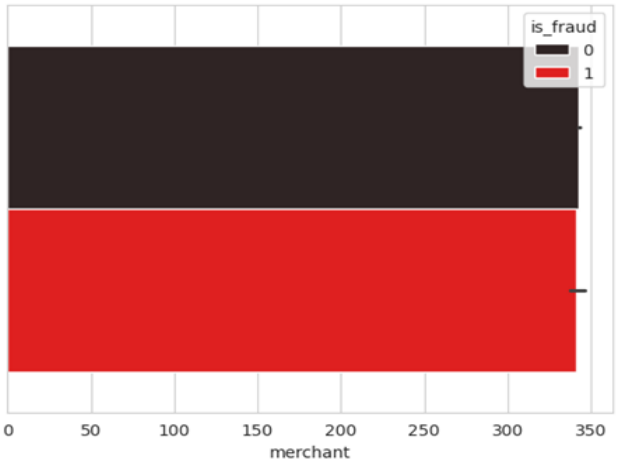

Figure 6 Graph Plot Between is Fraud and Merchant

The (figure 6) shows a bar graph that shows how merchants can detect fraud. On the one hand, we have "merchant," while on the other, we have "is_fraud." If there is no fraud, the bars will be black, and if there is, they will be red. Importantly, the red bar significantly extends beyond the 300 line on the x-axis compared to the black bar, indicating that there are more fraudulent cases than non-fraudulent ones. Quickly assess the level of fraudulent activity among the merchants represented with this visualization.

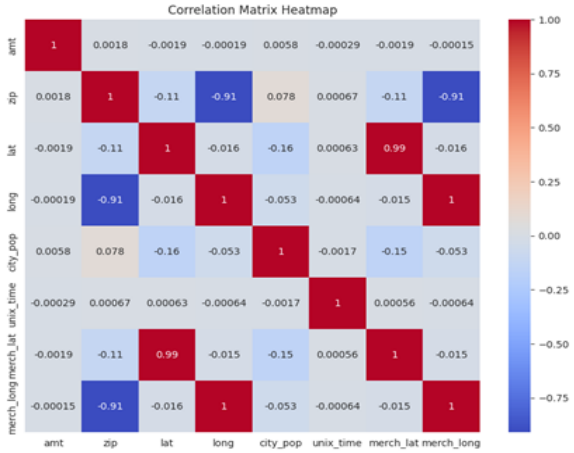

Figure 7 Correlation Heat map of Variables

The (figure 7) displays the correlation coefficients between pairs of variables using a color spectrum ranging from very red to very blue, resembling a correlation matrix heatmap. When dark blue is associated with a strong negative link, dark red is associated with a strong positive relationship. Included in this set are the following new variables: "amt," "zip," "lat," "long," "city_pop," "unix_time," "merch_lat," and "merch_long." A correlation coefficient of 1 shows a very positive correlation, -1 a significantly negative correlation, and 0 shows no linear association all on each cell. This heatmap can help you identify the relationships in the dataset and have a better understanding of how the variables are dependent on each other.

3.4 Machine Learning & Modeling

The goal of "machine learning" research in computer science is to train computers to learn from experience and make decisions and predictions autonomously through the use of computational algorithms and pattern recognition. This approach involves teaching models to recognize relationships and patterns in data, and then using those models to forecast or make decisions based on fresh data. Finding patterns in unlabeled data is the goal of unsupervised learning, as opposed to supervised learning's prediction-making using labeled data. A few examples of popular ML techniques are classification, dimensionality reduction, clustering, and regression. Many fields can benefit from machine learning's innovative solutions to long-standing problems; these include economics, healthcare, computer vision, recommendation systems, natural language processing (NLP), and computer vision.

3.4.1 Logistic Regression

One common supervised learning method for binary classification tasks is logistic regression. The procedure comprises considering one or more predictor factors in order to estimate the likelihood of a binary outcome. Applying a logistic curve to the dataset allows one to calculate the probability of an event occurring. Despite the model's intrinsic simplicity, it can only be beneficial if the independent variables have a linear connection with the dependent variable. Marketing, healthcare, and finance are just a few of the many industries that make use of it because of how efficient it is computationally and how easy it is to understand.

3.4.2 Support Vector Machine (SVM)

When it comes to regression and classification, the Support Vector Machine (SVM) approach is a trusted supervised learning option. Finding the hyperplane that optimizes the gap between classes in the feature space and best partitions them is the mechanism of operation. Because they employ a

range of kernel functions—including polynomial, radial basis functions (RBF), and linear—support vector machines (SVMs) can handle both linear and non-linear data rather easily. For multi-dimensional data, it excels, and it works well with datasets of moderate size. Several fields find support vector machines (SVMs) helpful, including bioinformatics, picture recognition, and text classification.

3.4.3 Gradient Boosting

As part of an ensemble learning strategy, Gradient Boosting builds a robust prediction model by progressively combining decision trees and other weak learners. The method is effective because it improves the overall accuracy of forecasts by fitting each subsequent model to the residual errors of the previous one. All three of these boosters have become famous for their exceptional adaptability and prediction accuracy. Anomaly detection, web search ranking, recommendation systems, and many more sectors make extensive use of them.

3.4.4 Random Forest

The Random Forest technique trains a huge number of decision trees, and then takes an average of their outputs to get the class mode or regression prediction. For ensemble learning, this approach works wonders. By repeatedly rebuilding the training set while disregarding all but a randomly chosen subset of tree attributes, it achieves randomization.The Random Forest method can handle high-dimensional datasets with ease, provides reliable feature relevance estimates, and is resistant to overfitting. Remote sensing, medicine, and finance are just a few of the many fields that regularly use classification and regression problems.

3.4.5 Ensemble Learning

Ensemble Learning is a method for computer-assisted learning that combines multiple models into a single, more accurate prediction model than would be possible with only one or two models. One way to improve generalization performance and reduce the likelihood of overfitting is to use a variety of models. It is common practice to build multiple models and then integrate their predictions using ensemble methods such as bagging, boosting, and stacking. Decision trees, neural networks, and support vector machines are just a few examples of the many basic learners that might benefit from ensemble techniques due to their adaptability. Real-world applications utilize them extensively in a variety of areas, including as e-commerce, healthcare, and finance.

4. Result & Discussion

When evaluating ML models, many popular metrics are recall, accuracy, precision, and the F-score. Simply said, "accuracy" is the ratio of correctly classified samples to total cases, and it's a way to gauge how reliable forecasts are. Precision, which focuses on the reliability of positive forecasts, is defined as the percentage of out of one hundred positive predictions that are actually correct. The sensitivity or recall of a model measures its ability to detect positive instances relative to the overall number of favorable examples. This demonstrates that the model is capable of detecting all positive instances. The F-score gives a fair evaluation of the model's accuracy since it takes into account both real and false positives. Here, we find the solution by summing the recall and precision harmonically.

4.1 Accuracy

An indication of how well the model is doing could be its accuracy, which is the percentage of times it gets predictions right out of all the possible events. For the purpose of evaluating the model's ability to identify and classify brain cancers, we examine its ability to differentiate between various types of brain cancer. The reliability and quality of medical image analysis have a direct correlation to the accuracy ratings.

$$Accuracy = \frac{(TP+TN)}{(TP+FP+TN+FN)} \quad (1)$$

4.2 Precision

Calculating the accuracy of positive predictions is one approach to assess their performance. Accuracy is the ratio of the number of positively predicted cases to the total expected number of positive cases. How well the model can identify individual brain tumors with minimal false positives is what we mean when we talk about "accuracy" in this context.

$$Precision = \frac{TP}{TP+FP} \quad (2)$$

4.3 Recall

A model's recall, sometimes called sensitivity, reveals how well it can identify each positive occurrence. Examining the ratio of correctly

identified positive cases to all positive occurrences, the statistic focuses on the sensitivity of the model. Memory enhancement has the dual benefit of reducing false positives and enhancing tumor detection sensitivity.

$$Recall = \frac{TP}{TP+FN} \quad (3)$$

4.4 F score

The F-score gives a complete evaluation of a model's performance since it considers both the true positives and false positives. Despite their seeming contradictions, it manages to establish a balance between accuracy and memorability. Particularly helpful for activities requiring accuracy and memorization, such as medical diagnosis, this evaluation offers a holistic perspective of a model's situational categorization abilities.

$$F - score = \frac{2}{\frac{1}{precision}+\frac{1}{recall}} \quad (4)$$

Table 2 Performance Evaluation of Machine Learning Models on Imbalance Data

Models	Accuracy	Precision	Recall	F score
Logistic Regression	84.98	84.98	84.98	84.98
SVM	64.83	64.83	64.83	64.83
Gradient Boosting	87.77	87.77	87.77	87.77
Random Forest	89.91	89.91	89.91	89.91
Ensemble	87.94	87.94	87.94	87.94

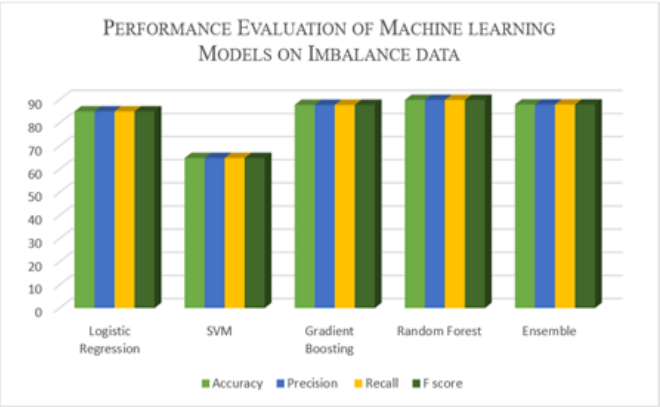

Figure 8 Performance Graph on Imbalanced Data

Table 2 shows how machine learning models fared when fed data that was skewed in one direction or the other. For each model, it gives information on the F-score, recall, accuracy, etc. Logistic Regression reliably meets or exceeds expectations across all measures (Figure 8). In every respect, SVM is superior to its rival models. All three methods—Ensemble, Random Forest, and Gradient Boosting—produce inferior results when compared side by side. These metrics show how well each model does at instance classification; Random Forest outperforms its rivals on imbalanced data.

Table 3 Machine Learning Model Performance Evaluation Oversampling (Training and Testing Data) For Class Balance

Models	Accuracy	Precision	Recall	F score
Logistic Regression	84.94	84.94	84.94	84.94
SVM	65.03	65.03	65.03	65.03
Gradient Boosting	87.77	87.77	87.77	87.77
Random Forest	89.84	89.84	89.84	89.84
Ensemble	87.97	87.97	87.97	87.97

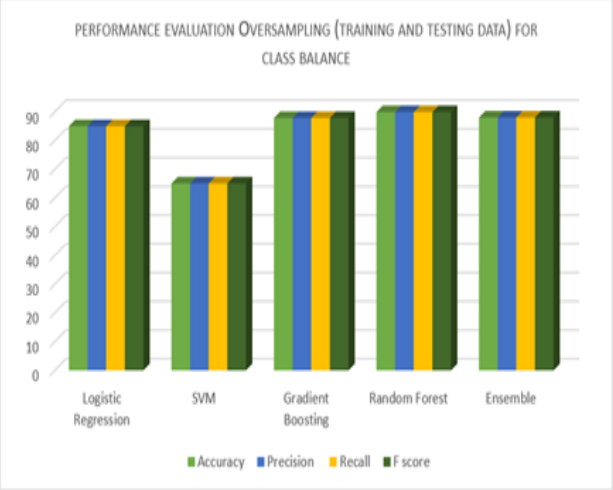

Figure 9 Performance Evaluation Graph Oversampling (Training and Testing Data) For Class Balance

Figure 9 and Table 3 show the results of evaluating machine learning models' performance after using oversampling approaches to ensure that the testing and training sets are balanced. For every model, the

table details their accuracy, precision, recall, and F-score. The performance of the ensemble, Gradient Boosting, and Logistic Regression approaches is consistent across all criteria. In comparison to other models, SVM performs poorly, however Random Forest outperforms them all. The results reveal that oversampling improves machine learning models' classification performance. Random Forest has the strongest overall performance, which indicates that it can handle class imbalances well.

Table 4 Evaluation of Machine Learning Model Performance with Oversampling on Balanced Training and Testing Data

Models	Accuracy	Precision	Recall	F score
Logistic Regression	84.74	84.74	84.74	84.74
SVM	64.96	64.96	64.96	64.96
Gradient Boosting	87.77	87.77	87.77	87.77
Random Forest	90.00	90.00	90.00	90.00
Ensemble	88.07	88.07	88.07	88.07

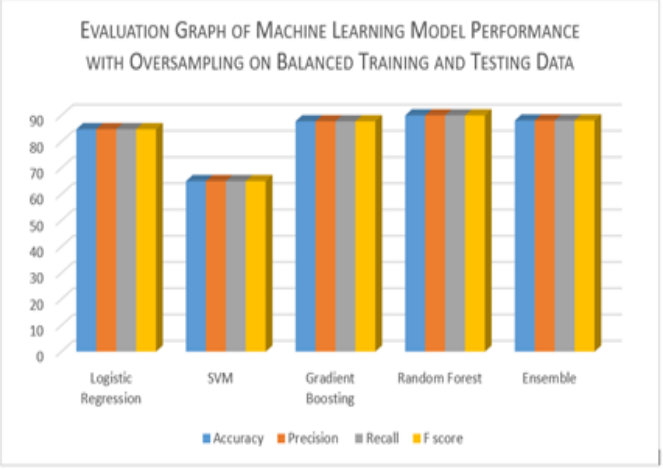

Figure 10 Machine Learning Model Performance with Oversampling on Balanced Training and Testing Data

As indicated in Table 4, we utilized oversampling methodologies to assess the machine learning model's performance, ensuring that the training and testing data sets were balanced. You may view the F-score, recall, accuracy, and precision for each model in the table. All metrics show that the ensemble, Gradient Boosting, and Logistic Regression methods perform similarly (Figure 10). Support Vector Machines (SVM) are not very good models. Random Forest continues to dominate all other metrics, demonstrating its ability to handle class imbalances effectively, even after taking oversampling into consideration. These results show that a balanced dataset for training and testing is necessary to improve the classification performance of machine learning models. Out of the three tables, Table 4, which shows the evaluation of machine learning model performance with balanced training and testing data and oversampling, appears to yield the best results. With maximum scores reaching 90.00, the table shows that Random Forest performs better than all other measures, including accuracy, precision, recall, and F-score. This indicates that, even when using oversampling strategies, the Random Forest model still performs better than other models when it comes to improving class inequality. Logistic Regression, Gradient Boosting, and Ensemble techniques consistently perform well across all measures, further supporting the efficiency of oversampling strategies in enhancing the classification performance of machine learning models. Results are shown in Figure 11.

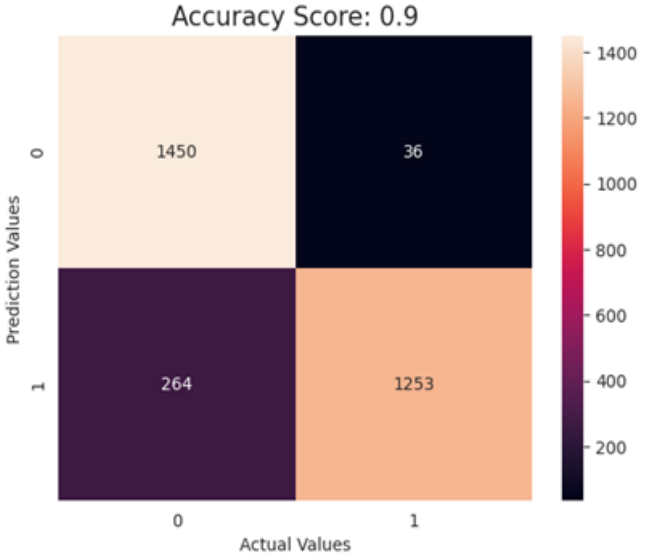

Figure 11 Result

The classification model is functioning as expected if the random forest confusion matrix shows that 90% of the predictions were right. Additionally, it displays the total number of TPs, FPs, and TRs; a score of 0.9 indicates that all three events occurred simultaneously.

Conclusion

In conclusion, there are a plethora of important lessons about how machine learning models work in different contexts to detect and classify credit card fraud. In a thorough review of accuracy,

precision, recall, and F-score criteria, Random Forest regularly beats rival models, proving that it is robust and effective in addressing class imbalances. Because it uses oversampling techniques to achieve class balance, Random Forest continues to perform exceptionally well even with balanced datasets. This exemplifies the model's adaptability and reliability, two qualities that make it an attractive candidate for practical application in fraud detection systems. If you want better classification results in fraud detection activities, you need to apply oversampling strategies and several machine learning approaches. Ensemble, Gradient Boosting, and Logistic Regression results demonstrate this is feasible. A balanced training dataset is crucial, and Random Forest is effective at eliminating class inequalities, according to the results. The study's overall conclusions provide useful information for developing more trustworthy machine learning models for fraud detection, which could have widespread practical applications in the financial sector. Additional research might investigate different optimization strategies and ensemble procedures to enhance the model's functionality in practical settings.

References

[1]. L. Moumeni, M. Saber, I. Slimani, I. Elfarissi, and Z. Bougroun, "Machine Learning for Credit Card Fraud Detection," *Lect. Notes Electr. Eng.*, vol. 745, no. 24, pp. 211–221, 2022, doi: 10.1007/978-981-33-6893-4_20.

[2]. R. Bin Sulaiman, V. Schetinin, and P. Sant, "Review of Machine Learning Approach on Credit Card Fraud Detection," Human-Centric Intell. Syst., vol. 2, no. 1–2, pp. 55–68, 2022, doi: 10.1007/s44230-022-00004-0.

[3]. A. Singh, A. Jain, and S. E. Biable, "Financial Fraud Detection Approach Based on Firefly Optimization Algorithm and Support Vector Machine," Appl. Comput. Intell. Soft Comput., vol. 2022, no. Cc, 2022, doi: 10.1155/2022/1468015.

[4]. G. Sasikala et al., "An Innovative Sensing Machine Learning Technique to Detect Credit Card Frauds in Wireless Communications," Wirel. Commun. Mob. Comput., vol. 2022, no. i, 2022, doi: 10.1155/2022/2439205.

[5]. Z. Faraji, "A Review of Machine Learning Applications for Credit Card Fraud Detection with A Case study," SEISENSE J. Manag., vol. 5, no. 1, pp. 49–59, 2022, doi: 10.33215/sjom.v5i1.770.

[6]. N. Uchhana, R. Ranjan, S. Sharma, D. Agrawal, and A. Punde, "Literature Review of Different Machine Learning Algorithms for Credit Card Fraud Detection," Int. J. Innov. Technol. Explor. Eng., vol. 10, no. 6, pp. 101–108, 2021, doi: 10.35940/ijitee.c8400.0410621.

[7]. A. Bansal and H. Garg, "An Efficient Techniques for Fraudulent detection in Credit Card Dataset: A Comprehensive study," IOP Conf. Ser. Mater. Sci. Eng., vol. 1116, no. 1, p. 012181, 2021, doi: 10.1088/1757-899x/1116/1/012181.

[8]. A. Mohari, J. Dowerah, K. Das, F. Koucher, and D. J. Bora, "Credit Card Fraud Detection Techniques: A Review," no. July, pp. 157–166, 2021, doi: 10.1007/978-981-16-1048-6_12.

[9]. A. Mehbodniya et al., "Financial Fraud Detection in Healthcare Using Machine Learning and Deep Learning Techniques," Secur. Commun. Networks, vol. 2021, 2021, doi: 10.1155/2021/9293877.

[10]. A., "Credit Card Fraud Detection using Machine Learning and Data Science," Int. J. Res. Appl. Sci. Eng. Technol., vol. 9, no. VII, pp. 3788–3792, 2021, doi: 10.22214/ijraset.2021.37200.

[11]. N. M. Mqadi, N. Naicker, and T. Adeliyi, "Solving Misclassification of the Credit Card Imbalance Problem Using near Miss," Math. Probl. Eng., vol. 2021, 2021, doi: 10.1155/2021/7194728.

[12]. V. Muthulakshmi, C. Saravanakumar, and A. Tamizhselvi, "An Efficient Machine Learning Model for Location Aware Credit Fraud and Risk Classification and Detection," 2021, doi: 10.4108/eai.16-5-2020.2304200.

[13]. I. Journal, E. Vol, I. Factor, and J. Homepage, "IJMIE13Jan21-NagAka," vol. 11, no. 01, pp. 108–112, 2021.

[14]. D. Prajapati, A. Tripathi, J. Mehta, K. Jhaveri, and V. Kelkar, "Credit Card Fraud Detection Using Machine Learning," 2021 7th IEEE Int. Conf. Adv. Comput. Commun. Control. ICAC3 2021, no. Iciccs, pp. 3–8, 2021, doi: 10.1109/ICAC353642.2021.9697227.

[15]. Z. Salekshahrezaee, J. L. Leevy, and T. M. Khoshgoftaar, "The effect of feature extraction and data sampling on credit card fraud detection," J. Big Data, vol. 10, no. 1, 2023, doi: 10.1186/s40537-023-00684-w.

[16]. N. Prabhakaran, "Oppositional Cat Swarm Optimization-Based Feature Selection Approach for Credit Card Fraud Detection," vol. 2023, no. Dl, 2023.

[17]. A. Mniai and K. Jebari, "Credit Card Fraud Detection by Improved SVDD," Lect. Notes Eng. Comput. Sci., vol. 2244, pp. 32–37, 2022.

[18]. E. F. Malik, K. W. Khaw, B. Belaton, W. P. Wong, and X. Chew, "Credit Card Fraud Detection Using a New Hybrid Machine Learning Architecture," Mathematics, vol. 10, no. 9, 2022, doi: 10.3390/math10091480.

[19]. Y. F. Zhang, H. L. Lu, H. F. Lin, X. C. Qiao, and H. Zheng, "The Optimized Anomaly Detection Models Based on an Approach of Dealing with Imbalanced Dataset for Credit Card Fraud Detection," Mob. Inf. Syst., vol. 2022, 2022, doi: 10.1155/2022/8027903.

[20]. V. Plakandaras, P. Gogas, T. Papadimitriou, and I. Tsamardinos, "Credit Card Fraud Detection with Automated Machine Learning Systems," Appl. Artif. Intell., vol. 36, no. 1, 2022, doi: 10.1080/08839514.2022.2086354.

[21]. H. Kochhar and Y. Chhabra, "A Novel Framework for Credit Card Fraud Detection," Turkish J. Comput. Math. Educ., vol. 12, no. 11, pp. 3189–3195, 2021.

[22]. "Credit Card Transactions Fraud Detection Dataset." https://www.kaggle.com/datasets/kartik2112/fraud-detection (accessed Apr. 10, 2024).