www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

Adaptive Multi-Model Approach for Detecting Illicit Payment Anomalies

Vadde Varun Tej Reddy, varuntejreddy999@gmail.com

Abstract: Because hackers posing as cardholders pose a threat to economic establishments, recognizing fraudulent credit score card transactions is a first-rate mission. Numerous resampling techniques—consisting of oversampling, undersampling, and SMOTE—are used to handle the elegance imbalance inherent in fraud detection using datasets such as EU statistics and Sparkov statistics: Ensemble studying makes use of several algorithms to improve accuracy and resilience, therefore improving type performance. To maximise version education and prediction, the paper shows an ensemble-based framework along with state-of-the-art resampling methods. Comprehensive examination of several classification fashions suggests the better overall performance of a Stacking Classifier, which efficiently mixes several base models to gain progressed accuracy, precision, recall, and F1 score throughout all methodologies. This approach has brilliant promise to significantly enhance fraud detection structures, consequently ensuring correct identification of fake transactions and reducing false positives. The suggested architecture emphasises the need of ensemble approaches and statistics balancing strategies in handling the complexity of monetary fraud detection.

"Index Terms - *Fintech, credit card fraud detection, ensemble learning, machine learning, simulated dataset, real-world data set".*

I. INTRODUCTION

In the age of digital payments, "credit card fraud (CCF)" detection is a major difficulty since it entails the discovery of irregularities in credit card transactions. Visa and mastercard by themselves accounted for more than 2.183 million cardholders in 2020, highlighting the scope of this problem [1]. According to reviews, there were about 1.4 million occurrences of identity theft in the same year; 393,207 of these cases were linked especially to credit card fraud [2]. "Comparatively to $23.97 billion in 2017—a 19.3% boom"—the financial losses linked with illegal credit card use were astounding, "total $28.6 billion in 2020. As cited in the Nilson file of 2022 [3]", those losses are expected to attain $408 billion by the quilt of the following decade. Notwithstanding tasks by financial institutions and banks, the steady increase in those numbers shows how urgently robust credit card fraud detection systems are needed.

A wide spectrum of methods has been developed to combat credit card abuse, mostly falling within statistical methods and machine learning-based solutions [2]. Identifying fraudulent transactions statistically means spotting anomalies in a dataset. For this aim statistical tools including normal distribution analysis, cluster-based methods, and box-and- whisker graphs have been applied. But the complexity of credit card transaction data has driven growing dependence on machine learning methods, which provide more flexibility and precision. Specifically made to analyse past data and forecast fraudulent transactions are machine learning classifiers. Common methods used in CCF detection are "neural networks, support vector machines, decision trees, and regression models" [3], [4], [5]. Although various methods have shown success to one of a kind degrees, their efficacy usually depends on the quality and features of the training set.

Entire learning approaches have been developed to improve detection capacity. Multiple base classifiers are sought to be combined in ensemble learning to produce a better, more resilient meta-classifier. One such method, bagging, creates many samples with replacement from the training data to separately train classifiers using aggregation methods including voting to obtain final predictions. Another ensemble technique, boosting creates classifiers one model after another, spreading prediction mistakes from one to the next to raise general performance. "Among them are XGBoost [6]", Gradient Boosting, and AdaBoost.

1/3 ensemble method combining several classifiers to produce a high-performance meta-classifier is stacking, sometimes known as generalisation. Combining the strengths of several models has shown promise as a way of handling the complexity of credit card fraud detection [7].

II. RELATED WORK

Index in Cosmos
Mar 2025, Volume 15, ISSUE 1
UGC Approved Journal

Financial organisations have always struggled with credit card fraud detection since the amount of transactions and the expertise of thieves keep rising. Many studies have looked at how statistical methods and machine learning might assist to lessen the dangers connected to faux transactions. Those techniques seek to minimise false positives and false negatives while but increasing the accuracy and dependability of fraud detection systems.

Varmedja et al. [10] examined how nicely machine learning techniques detected credit card fraud. Their work underlined the need of using methods such oversampling, undersampling, and "synthetic Minority Oversampling technique (SMOTE)" to manage imbalanced datasets—a typical feature of fraud detection chores. The results underlined how better generalising ensemble learning techniques as Random forest and Gradient Boosting on unseen data helped them to outperform single models. In a similar vein, Raj and Portia [11] investigated numerous fraud detection methods and found machine learning classifiers to be the most likely instruments for anomaly in transaction data detection. They underlined that the flexibility of machine learning techniques qualifies them for changing fraud trends.

Additionally investigated as a possible credit card fraud detection fix is deep learning. in order to raise detection accuracy, “Vimal and Vimal” [12] suggested a population-based optimal and condensed fuzzy deep belief network by combining feature selection and dimensionality reduction approaches, their approach proved strong in opposition to very unbalanced datasets. Combining fuzzy logic with neural networks, Razooqi et al. [13] created a hybrid system for fraud detection that demonstrated higher accuracy and interpretability than conventional machine learning methods. These research highlight the increased interest in using hybrid approaches and deep learning to address problems with false transaction identification.

Additionally used to improve fraud detection are visualising methods. Lokanan [14] investigated how visual aids might be used to spot illicit trends in cash laundering and credit card transactions. This method provides an easy strategy to examine big data units and helps researchers to understand complicated data interactions and anomalies. While it is not a stand-on my own repair, visualisation adds remarkable value to other detecting methods.

Another creative approach in credit card fraud detection has become graph-based techniques. Lebichot et al. [15] offered a semi-supervised system designed to identify fraud using graph-based models. Representing transactions as nodes and their connections as edges, the algorithm found unusual trends suggestive of fraudulent activity. Common in real-world fraud detection situations, the semi-supervised man or woman of this method addressed the lack of labelled data.

Because of their scalability and versatility, machine learning methods still predominate in credit card fraud detection. Decision trees, "support Vector machine (SVM)", and "k-Nearest Neighbours (okay-NN)" among other machine learning classifiers were compared in Awoyemi et al. [16]. Their results underlined that ensemble techniques—especially bagging and boosting algorithms—delivery exceptional performance. Through pooling the predictions of several classifiers, ensemble learning improves generalisation and lowers the probability of overfitting, hence enhancing the detection accuracy.

Using hybrid models has showed promise in tackling these difficulties. Combining statistical methods with machine learning models is a whole fraud detection strategy. Preprocessing steps like clustering and density-based algorithms, for example, can assist to find questionable transactions—which are subsequently fed into machine learning classifiers for extra investigation—by means of traditional outlier identification approaches. Using the capabilities of both techniques, this layered strategy guarantees thorough coverage of fraudulent trends.

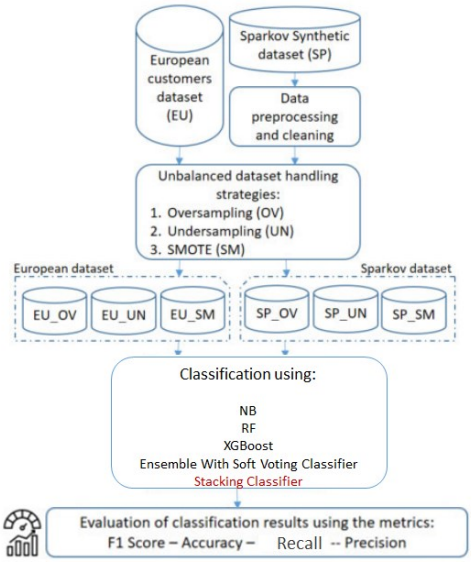
Although statistical approaches and machine learning have made great progress in fraud detection, in this field "explainable artificial intelligence (XAI)" is becoming more and more crucial. Transparency in decision-making and regulatory criteria need for the creation of interpretable models capable of offering clear justifications for their projections. In financial programs especially, where false positives could cause client discontent and false negatives might cause major financial losses, this is very important.

III. MATERIALS AND METHODS

Leveraging a mix of improved records sampling, function choice, and device getting to know techniques, the proposed machine seeks to improve credit card fraud detection. The dataset incorporates “EU facts and Sparkov information”, in an effort to be addressed elegance imbalance via “OverSampling, UnderSampling, and SMOTE” records sampling methods. PCA decomposition will be utilized in function selection to lower dimensionality and raise version overall

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

performance. To reflect different patterns in the data, numerous "machine learning models—Random forest [19] (RF), Naive Bayes [18] (NB), and XGBoost [20] (XGB)"—may be developed and assessed. Furthermore used could be ensemble techniques to increase accuracy and robustness: a soft voting Classifier integrating Random forest, Naive Bayes, and XGBoost and a Stacking Classifier coupled with LightGBM using a Bagging Classifier with Random forest and decision Tree. Combining these methods seeks to create a very powerful and efficient fraud detecting mechanism.



"Fig.1 Proposed Architecture"

This method identifies fraudulent transactions the use of datasets—"EU and Sparkov". We first preprocess and sanitize the facts. "Oversampling, undersampling, and SMOTE" strategies are utilized to deal with unbalanced dataset issues. "NB, RF, XGB, Ensemble with soft voting Classifier, and Stacking Classifier" all are utilized in classification. "F1 score, accuracy, recall, and precision" measures assist in measuring version overall performance.

i) Dataset Collection:

Using labelled fraud signs for evaluation, the european and Sparkov datasets encompass transaction statistics with time, amount, and anonymised information needed to pick out fraudulent transactions via device gaining knowledge of. Comprising 284,807 transactions with 31 traits, the ecu statistics [8] dataset used for credit score card fraud detection is along with a intention variable "elegance" that denotes fraudulent transactions (1) or valid transactions (0), these comprise transaction details such as time, transaction quantities, and 28 anonymised numerical features (V1 to V28). Except for the "class" column, all the trends inside the dataset are non-forestall; lacking values are not present. The facts offers a wealthy basis for spotting tendencies and abnormalities in economic transactions.

	Time	V1	V2	V3	V4	V5	V6	V7	V8
0	0.0	-1.359807	-0.072781	2.536347	1.378155	-0.338321	0.462388	0.239599	0.098698
1	0.0	1.191857	0.266151	0.166480	0.448154	0.060018	-0.082361	-0.078803	0.085102
2	1.0	-1.358354	-1.340163	1.773209	0.379780	-0.503198	1.800499	0.791461	0.247676
3	1.0	-0.966272	-0.185226	1.792993	-0.863291	-0.010309	1.247203	0.237609	0.377436
4	2.0	-1.158233	0.877737	1.548718	0.403034	-0.407193	0.095921	0.592941	-0.270533

"Fig.2 Dataset Collection Table – European"

With 1,296,675 devices and 7 columns—"transaction details which include transaction date and time ("trans_date_trans_time")", "transaction amount ("amt")", and geographical records including ZIP code ("zip"), and "metropolis population ("city_pop")" the Sparkov dataset [9] buyer facts including "date of start ("dob")" and the objective variable "is_fraud," where 1 represents fraudulent transactions and 0 represents honest transactions, further comprises the dataset. With numeric and precise statistics forms, all columns that are non-null provide a robust dataset for fraud detection examine.

	Unnamed: 0	trans_date_trans_time	cc_num	merchant	category	amt
0	0	2019-01-01 00:00:18	2703186189652095	fraud_Rippin, Kub and Mann	misc_net	4.97
1	1	2019-01-01 00:00:44	630423337322	fraud_Heller, Gutmann and Zieme	grocery_pos	107.23
2	2	2019-01-01 00:00:51	38859492057661	fraud_Lind-Buckridge	entertainment	220.11
3	3	2019-01-01 00:01:16	3534093764340240	fraud_Kutch, Hermiston and Farrell	gas_transport	45.00
4	4	2019-01-01 00:03:06	375534208663984	fraud_Keeling-Crist	misc_pos	41.96

"Fig.3 Dataset Collection Table – Sparkov"

ii) Pre-Processing:

We will move over essential pre-processing ranges including "data processing, data visualization, PCA decomposition-based totally feature selection, and data sampling methods".

a) Data Processing: Raw data for machine learning must first be equipped via statistics processing. It

Index in Cosmos
Mar 2025, Volume 15, ISSUE 1
UGC Approved Journal

contains records kind conversion, managing lacking values, and replica removal from the dataset. Particularly for algorithms sensitive to scale, such as neural networks, transaction facts must be normalised or standardised in credit score card fraud detection. Other than that, unnecessary functions should be removed and class features should desire encoding. Properly handled facts ensures fashions' ability to detect fraudulent transactions and analyze trends.

b) Data Visualization: Preprocessing depends on an awareness of the distribution and interactions among features, which data visualisation facilitates. Heatmaps, scatter plots, and histograms among other tools expose trends, relationships, and dataset anomalies. Visualising the distribution of genuine against fraudulent transactions as well as the correlation between features like transaction amounts and time helps fraud detection to spot trends and anomalies. Visualisation also guides next preprocessing actions like resampling or feature engineering and aids in evaluation of class imbalance.

"c) Feature Selection": A dimensionality reduction method called "principal component analysis (PCA)" enables one perceive the maximum crucial elements in a fixed. It orders the authentic features with the aid of variance and converts them into a set of linearly uncorried components. While keeping most of the data, PCA helps simplify the information. PCA is helpful in fraud detection for determining which factors most affect variance, thereby enabling the deletion of pointless or duplicated features and hence enhancement of model efficiency and performance.

d) Data Sampling: class imbalance in fraud detection datasets is addressed thru methods of data sampling. Whereas undersampling lowers the majority elegance instances to balance the dataset, oversampling will increase the quantity of minority elegance times. Via interpolating among cutting-edge statistics, SMOTE—synthetic Minority Over-sampling approach— generates artificial samples for the minority elegance. Those methods assure that machine mastering algorithms do no longer favour the bulk magnificence, therefore improving the potential of the model to stumble on fraudulent transactions by means of balanced datasets.

iii) Training & Testing:

Training and testing include the preparation of a data set for evaluating machine learning models. During training, the model acquires formulas and relationships within data through marked examples and internal parameters to reduce errors. The trained model is evaluated on new data during testing to determine its generalization and predictive accuracy. This procedure ensures that the model is durable and is able to create reliable predictions about new, unnoticed data, and therefore facilitates successful detection of fraudulent transactions.

iv) Algorithms:

"Random Forest": "Random Forest" [19] is a way of studying a document that generates numerous selection -making timber at some stage in the schooling segment and determines a class primarily based on the majority vote between those bushes. It will increase predictive accuracy and relieves excessive amount via averaging the effects from several trees. Research uses random forest because of its resistance in the processing of large data sets and its expertise in solving unbalanced classes, which is suitable for identifying fraudulent transactions characterized by complex and different patterns.

Naive Bayes: Naive Bayes is a chance classifier derived from Bayes' sentence, which represents that the residences are impartial at the magnificence label. It calculates the rear opportunity for every class and identifies the elegance with maximum chance. Research uses naive Bayes [18] for its simplicity and efficiency, especially beneficial for large data sets and situations where independence is a credible assumption, which makes it easier to classify fraud detection transactions.

In generalized notation we write:

$$"p(A,B|A) = p(A) * p(B|A) \qquad (1)"$$

The statement is: "Probability A and B, given to A, equal to the probability of multiplying probabilities B, conditional A." This is referred to as a conditional probability or more precisely, a common probability because the probability is evaluated on the basis of a previous event or status.

XGBoost: XGBOOST (Extreme Gradient Boosting) is a framework for increasing a gradient that constructs models gradually using decision -making trees, increasing performance through regularization and increasing methodologies. It is known for its exceptional accuracy, speed and efficiency. Research uses XGBOOST [20] to expand the detection of fraud with adept management of large data sets and complex interactions of elements and therefore increases the accuracy and download of prediction.

www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86

"$y\hat{}i=\sum k=1Kfk(xi)$ (2)"

"Where y^i denotes the final predicted value for the ith data point, K signifies the number of trees in the ensemble, and fk(xi) represents the prediction of the Kth tree for the ith data point".

Ensemble With Soft Voting Classifier (RF + NB + XGB): The soft voting classifier integrates various classifiers - Random Forest, Naive Bayes and XGBOOST - by average of their supposed probability for final classification. It takes advantage of each unique model to increase overall predictive accuracy. This project uses the file technique to develop a more resistant fraud detection system, effectively collects different formulas and minimizes the likelihood of incorrect diagnosis.

Stacking Classifier (Bagging Classifier with RF and DT with LightGBM): The stacking classifier merges different models, including RF, DT and LightGBM, to increase the predictive efficiency of synthesizing their outputs through meta. This method capitalizes the benefits of each model and alleviates distortion. The aim of the research is to improve the accuracy of fraud detection by consolidating predictions from multiple algorithms, resulting in a more reliable and general detection system.

IV. RESULTS AND DISCUSSION

Accuracy: The take a look at accuracy is its ability to distinguish among patients and healthful cases. If you need to evaluate the check accuracy, calculate the ratio of true positives and true negatives in all evaluated instances. This can be mathematically expressed as:

$$"Accuracy = \frac{\text{TP} + \text{TN}}{"\text{TP} + \text{FP} + \text{TN} + \text{FN}"}(3)"$$

"Precision": The "precision" quantifies the share of exactly identified fantastic instances or samples. The precision is decided by the formulation:

$$"Precision = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}}(4)"$$

Recall: The assessment of ML evaluates the potential of the model to pick out all suitable instances of the elegance. It shows the efficiency of the model when the class with the aid of contrasting exactly predicted nice observation with the entire wide variety of positives.

$$Recall = \frac{\text{TP}}{\text{TP} + \text{FN}}(5)$$

F1-Score: The accuracy of the machine learning model is evaluated using the F1 score. Integration of the accuracy of the model and metrics of evocation. The metric of accuracy quantifies the frequency of the real predictions made by using the model throughout the records record.

$$"F1\ Score = 2 * \frac{"Recall\ \text{X}\ Precision"}{"Recall + Precision"} * 100(6)"$$

Tables 1 to 6 compare the performance measure—F1-score, precision, recall, and accuracy—of every set of rules. Stacking Classifier automatically outperforms all other algorithms for all metrics. Tables provide a comparative analysis of the metrics for the opportunity techniques.

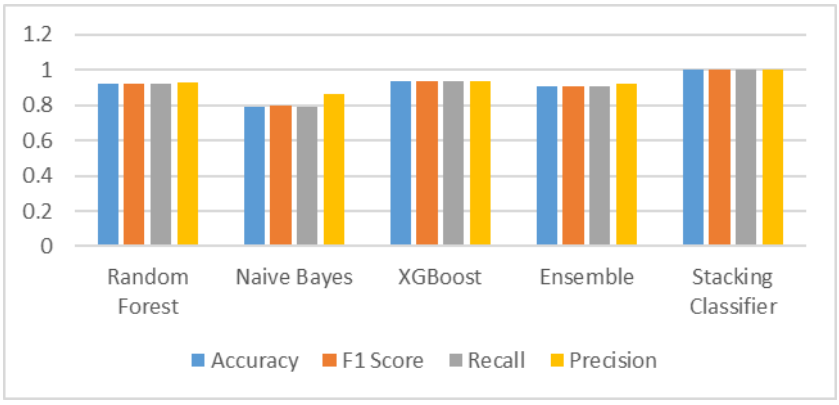
"Table.1 Performance Evaluation Metrics for OverSampling – European dataset"

Model	Accuracy	F1 Score	Recall	Precision
Random Forest	0.925	0.925	0.925	0.928
Naive Bayes	0.793	0.801	0.793	0.867
XGBoost	0.937	0.937	0.937	0.939
Ensemble	0.910	0.911	0.910	0.921
Stacking Classifier	**1.000**	**1.000**	**1.000**	**1.000**

"Graph.1 Comparison Graphs for OverSampling – European dataset"

Index in Cosmos
Mar 2025, Volume 15, ISSUE 1
UGC Approved Journal

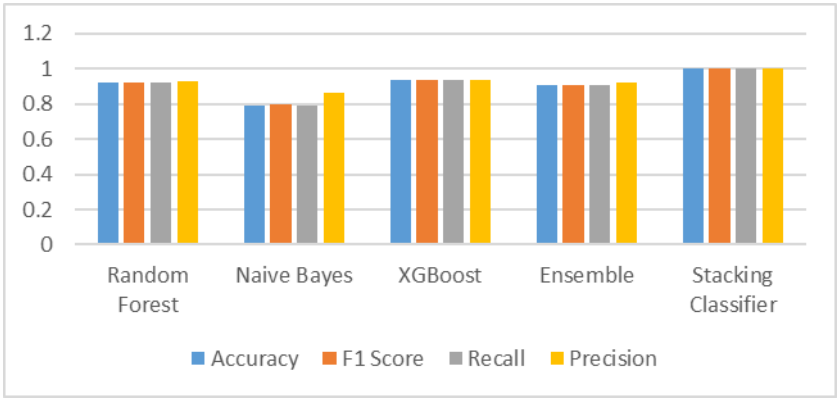
www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86



"Table.2 Performance Evaluation Metrics for UnderSampling – European dataset"

Model	Accuracy	F1 Score	Recall	Precision
Random Forest	0.878	0.878	0.878	0.878
Naive Bayes	0.787	0.794	0.787	0.854
XGBoost	0.898	0.899	0.898	0.900
Ensemble	0.883	0.884	0.883	0.898
Stacking Classifier	**0.954**	**0.954**	**0.954**	**0.959**

"Graph.2 Comparison Graphs for UnderSampling – European dataset"

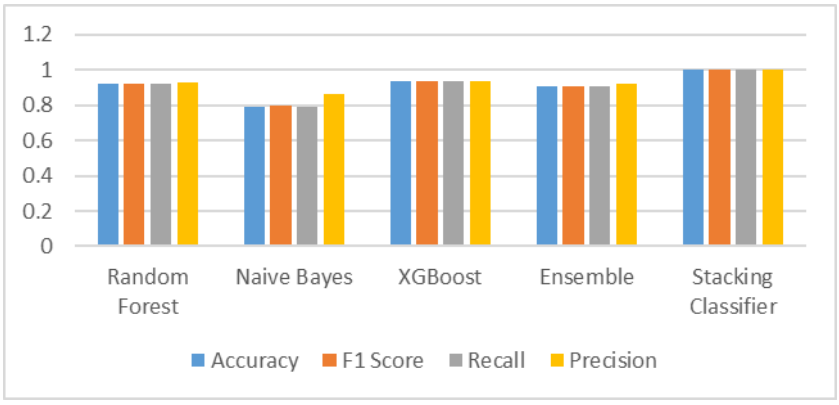


"Table.3 Performance Evaluation Metrics for SMOTE – European dataset"

Model	Accuracy	F1 Score	Recall	Precision
Random Forest	0.941	0.941	0.941	0.941
Naive Bayes	0.807	0.813	0.807	0.871
XGBoost	0.955	0.955	0.955	0.956
Ensemble	0.923	0.923	0.923	0.930
Stacking Classifier	**1.000**	**1.000**	**1.000**	**1.000**

"Graph.3 Comparison Graphs for SMOTE – European dataset"

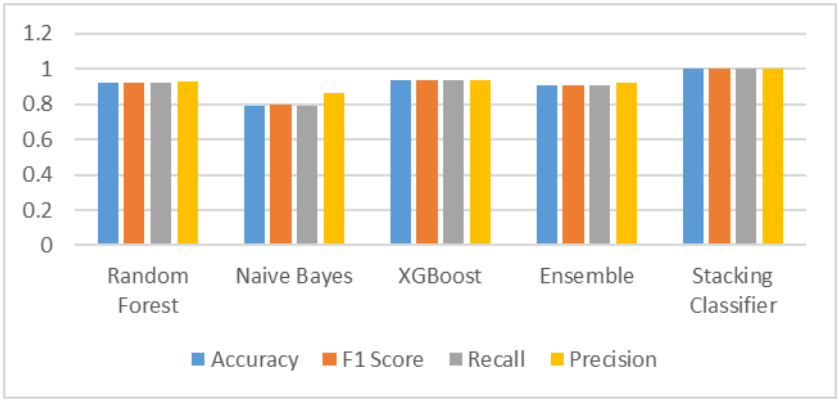
www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86



"Table.4 Performance Evaluation Metrics for OverSampling – Sparkov dataset"

Model	Accuracy	F1 Score	Recall	Precision
Random Forest	0.861	0.862	0.861	0.881
Naive Bayes	0.806	0.811	0.806	0.860
XGBoost	0.913	0.914	0.913	0.921
Ensemble	0.864	0.866	0.864	0.888
Stacking Classifier	**1.000**	**1.000**	**1.000**	**1.000**

"Graph.4 Comparison Graphs for OverSampling – Sparkov dataset"

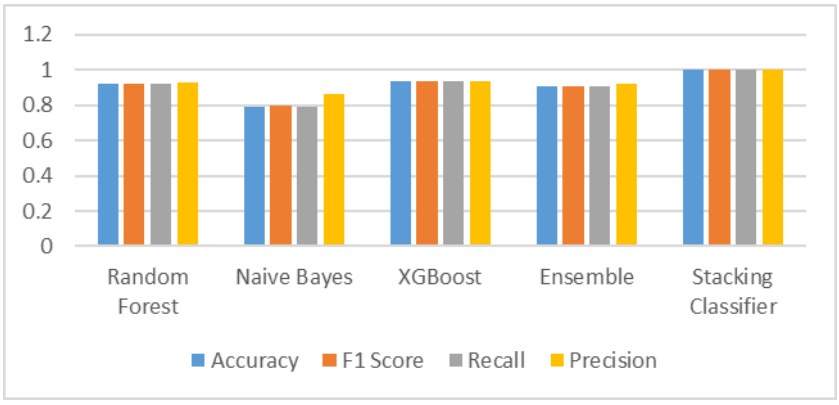


"Table.5 Performance Evaluation Metrics for UnderSampling – Sparkov dataset"

Model	Accuracy	F1 Score	Recall	Precision
Random Forest	0.861	0.862	0.861	0.884
Naive Bayes	0.843	0.845	0.843	0.867
XGBoost	0.911	0.911	0.911	0.919
Ensemble	0.865	0.866	0.865	0.888
Stacking Classifier	**0.995**	**0.995**	**0.995**	**0.995**

"Graph.5 Comparison Graphs for UnderSampling – Sparkov dataset"

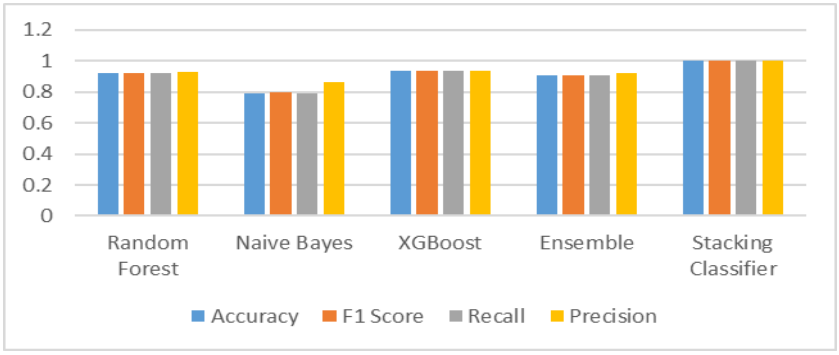
www.ijbar.org
ISSN 2249-3352 (P) 2278-0505 (E)
Cosmos Impact Factor-5.86



"Table.6 Performance Evaluation Metrics for SMOTE – Sparkov dataset"

Model	Accuracy	F1 Score	Recall	Precision
Random Forest	0.861	0.863	0.861	0.885
Naive Bayes	0.814	0.819	0.814	0.863
XGBoost	0.863	0.865	0.863	0.885
Ensemble	0.860	0.861	0.860	0.883
Stacking Classifier	**0.999**	**0.999**	**0.999**	**0.999**

"Graph.6 Comparison Graphs for SMOTE – Sparkov dataset"



In Graphs (1 to 6), accuracy is depicted in blue, F1-score in orange, recall in grey, and precision in mild yellow. Compared to the alternative fashions, the Stacking Classifier has greater overall performance across all standards, accomplishing the best values. The graphs above visually represent those findings.

V. CONCLUSION

Identification of fraudulent "credit card transactions" helps to prevent significant financial losses for organizations. Regardless of the persistent efforts of the financial parties, these losses permanently escalate and emphasize the urgent need for more efficient detection systems. File models inside the machine learning algorithms have shown a significant potential in solving this difficulty. File approaches, such a soft vote classifier and stacking classifier that use random forest, naive Bayes and XGBOOST show excellent efficiency in detecting fraudulent transactions. These fashions combine the benefits of various classifiers, growth "accuracy, precision, F1-score and recall" the detection of anomalies. The stacking classifier has shown exceptional accuracy, which makes it one of the most effective methods for detecting credit card fraud. Using these high -performance algorithms, financial institutions can significantly reduce the chance of fraud and strengthen the safety of digital transactions, thereby averting significant cash losses.

Future research should investigate the effects of multiplicative, variable and randomized factors during an authentication step to improve fraud detection robustness. In addition, it will be necessary to emphasize the explaining and interpretability of algorithms. Understanding and clarifying the decision -making processes of these models can bring a deep insight into their behavior, increase transparency and promote faith in their forecasts. This development will growth the

development of extra reliable and comprehensible fraud detection systems.

REFERENCES

[1] Z. Faraji, ''A review of machine learning applications for credit card fraud detection with a case study,'' SEISENSE J. Manage., vol. 5, no. 1, pp. 49–59, Feb. 2022.

[2] F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, ''Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms,'' IEEE Access, vol. 10, pp. 39700–39715, 2022.

[3] Nilson Report. Card Fraud Worldwide. Accessed: May 2023. [Online]. Available: https://nilsonreport.com/

[4] N. S. Alfaiz and S. M. Fati, ''Enhanced credit card fraud detection model using machine learning,'' Electronics, vol. 11, no. 4, p. 662, Feb. 2022.

[5] B. Arora and Sourabh, ''A review of credit card fraud detection techniques,'' Recent Innov. Comput., pp. 485–496, 2022.

[6] S.Srinidhi, K.Sowmya, and S.Karthika, ''Automatic credit fraud detection using ensemble model,'' in ICT Analysis and Applications. Springer, 2022, pp. 211–224.

[7] A. Alharbi, M. Alshammari, O. D. Okon, A. Alabrah, H. T. Rauf, H. Alyami, and T. Meraj, ''A novel text2IMG mechanism of credit card fraud detection: A deep learning approach,'' Electronics, vol. 11, no. 5, p. 756, Mar. 2022.

[8] Kaggle. (2022). European Cardholders Dataset. Accessed: May 2023. [Online]. Available: https://www.kaggle.com/datasets/mlgulb/creditcardfraud

[9] Sparkov Data Generation on Github, Sparkv simulator, 2020.

[10] D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, ''Credit card fraud detection–machine learning methods,'' in Proc. 18th Int. Symp. INFOTEH-JAHORINA (INFOTEH), Mar. 2019, pp. 1–5.

[11] S B. E. Raj and A A. Portia, ''Analysis on credit card fraud detection methods,'' in Proc. Int. Conf. Comput., Commun. Electr. Technol. (ICCCET), 2011, pp. 152–156.

[12] J. M. V and D. Vimal, ''Population based optimized and condensed fuzzy deep belief network for credit card fraudulent detection,'' Int. J. Adv. Comput. Sci. Appl., vol. 11, no. 9, 2020.

[13] T. Razooqi, P. Khurana, K. Raahemifar, and A. Abhari, ''Credit card fraud detection using fuzzy logic and neural network,'' in Proc. 19th Commun. Netw. Symp., 2016, pp. 1–5.

[14] M. E. Lokanan, ''Financial fraud detection: The use of visualization techniques in credit card fraud and money laundering domains,'' J. Money Laundering Control, vol. 26, no. 3, pp. 436–444, Apr. 2023.

[15] B. Lebichot, F. Braun, O. Caelen, and M. Saerens, ''A graph-based, semi supervised, credit card fraud detection system,'' in Proc. 5th Int. Workshop Complex Netw. Appl. (COMPLEX Network). Springer, 2017, pp. 721–733.

[16] J.O.Awoyemi, A.O.Adetunmbi, and S.A.Oluwadare, ''Credit card fraud detection using machine learning techniques: A comparative analysis,'' in Proc. Int. Conf. Comput. Netw. Informat. (ICCNI), Oct. 2017, pp. 1–9.

[17] I. Sohony, R. Pratap, and U. Nambiar, ''Ensemble learning for credit card fraud detection,'' in Proc. ACM India Joint Int. Conf. Data Sci. Manage. Data, Jan. 2018, pp. 289–294.

[18] K. M. Leung, ''Naive Bayesian classifier,'' Polytech. Univ. Dept. Comput. Sci./Finance Risk Eng., vol. 2007, pp. 123–156, Nov. 2007.

[19] A. Prinzie and D. Van den Poel, ''Random forests for multiclass classification: Random MultiNomial logit,'' Expert Syst. Appl., vol. 34, no. 3, pp. 1721–1732, Apr. 2008.

[20] T. Chen and C. Guestrin, ''XGBoost: A scalable tree boosting system,'' in Proc. 22nd ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, Aug. 2016, pp. 785–794.