Proceedings of the 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT-2024)
IEEE Xplore Part Number: CFP24CV1-ART; ISBN: 979-8-3503-2753-3

Robust Hybrid Machine Learning Model for Financial Fraud Detection in Credit Card Transactions

1ST DINGARI JAHNAVI
Department of Computer Science and Engineering, Amrita School of Computing, Chennai
jahnavidingari04@gmail.com

2ND MONA A
Department of Computer Science and Engineering, Amrita School of Computing, Chennai
monaananth07@gmail.com

3RD SANDEEP PULATA
Department of Computer Science and Engineering, Amrita School of Computing, Chennai
pulatasandeep@gmail.com

4TH SASANK SAMI
Department of Computer Science and Engineering, Amrita School of Computing, Chennai
sasanksami21@gmail.com

5TH BHARADWAJ VAKAMULLU
Department of Computer Science and Engineering, Amrita School of Computing, Chennai
bharadwaj2193@gmail.com

6TH BHARATHI MOHAN G
Professor, Department of Computer Science and Engineering, Amrita School of Computing, Chennai
g_bharathimohan@ch.amrita.edu

2024 2nd International Conference on Intelligent Data Communication Technologies and Internet of Things (IDCIoT) | 979-8-3503-2753-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/IDCIOT59759.2024.10467340

***Abstract*— Financial fraud is a rising problem that affects both organizations and people, necessitating cutting-edge solutions to lessen its effects. The majority of machine learning models used now in the field of fraud detection include Logistic Regression (LR), Decision Tree (DT), and Random Forest (RF). While these traditional models frequently lack sensitivity, have trouble figuring out complex fraud patterns, and are rigid in their ability to adjust to new threats. To overcome them, this research work provides a significant advancement by combining Decision Trees and Logistic Regression into a hybrid model, boasting an impressive accuracy of 98.1%. The proposed methodology not only improves the system's ability to detect fraud accurately but also makes it more flexible to the changing fraud strategies. Additionally, a thorough comparison analysis highlights the approach's undeniable benefits. In a nutshell, this work provides a method for detecting financial fraud using a hybrid model that expertly strikes a compromise between sensitivity and accuracy. In addition to improving fraud detection, this innovation also strengthens the security of financial systems.**

Keywords*— Financial fraud, Comparison analysis, Hybrid model, Contemporary world, Fraudulent transactions, Flexibility.

I. INTRODUCTION

Financial fraud has become a rising concern, endangering both individuals and organizations while threatening the stability and security of the financial sector. The development of cutting-edge solutions for the detection and prevention of fraudulent activities has become necessary as fraudsters have altered their strategies in a world with growing digital connectedness.

Modern techniques for detecting financial fraud mostly rely on individual machine learning models like Logistic Regression, Decision Trees, and Random Forests. Although these models have demonstrated some effectiveness, they are unable to offer a complete answer. They frequently experience difficulty coping with the complexity of fraud patterns, lack the sensitivity necessary to spot new fraudulent strategies, and show little flexibility. Additionally, class imbalances in datasets make the work more difficult by favouring the dominant class in the results and raising the possibility of false negatives. As a result of fraudsters taking advantage of these restrictions, financial institutions and organizations continue to sustain enormous losses. These conventional methods also have trouble with datasets that have an uneven distribution of classes because they frequently give priority to the majority class, missing potential fraud in the minority class.

The proposed approach introduces a hybrid model that successfully overcomes the drawbacks of traditional approaches, marking a significant progress in the field of financial fraud detection. The main innovation lies in the novel combination of Logistic Regression and Decision Trees, resulting in a Hybrid Model that considerably improves fraud detection accuracy, sensitivity to new fraud techniques, and flexibility in a dynamic environment. The problem of class imbalance is addressed using cutting-edge methods, which lowers the possibility of expensive false negatives. In the field of financial fraud detection, where missing even a single fraudulent transaction can result in large financial losses, this technique strikes a critical balance between accuracy and sensitivity.

In order to evaluate the effectiveness of several machine learning algorithms in the context of financial fraud detection, the approach conducts a thorough comparison analysis of the methods. The Null Model, Logistic Regression, Post Lasso Logistic Regression, Decision Tree, Random Forest, and K-Nearest Neighbours (KNN) are all included in the analysis. The approach guarantees a robust evaluation of these models by using a 5-fold cross-validation. It evaluates and trains these models in each fold to learn more about how well they work. For both, In Sample (IS) and Out of Sample (OOS) datasets, critical metrics like accuracy, sensitivity, specificity, and the geometric mean (G-mean) are determined. The IS findings show how well each model matches the training data, while the OOS results offer important details about their ability to generalize to new data. These performance measurements for each model in both IS and OOS configurations are gathered by the code.
In conclusion, this distinctive approach addresses the crucial problem of financial fraud by presenting a ground-breaking method that greatly improves the precision, sensitivity, and adaptability of fraud detection systems.

II. Literature Review

Financial fraud poses a significant threat to organizations and individuals, necessitating advanced solutions for effective mitigation. Samuel, Bethy and Otasowie focused on an extensive comparative analysis of techniques for detecting credit card fraud, evaluating their performance, strengths, and limitations in the face of concept drift [5]. The study examines machine learning methods, highlighting the difficulty caused by idea drift a term that describes variations in the underlying data distribution over time. Mohamed Fati and Saleh Alfaiz addressed All KNN-CatBoost, outperforms previous models, achieving high AUC, Recall, and F1-Score values [8]. Discussed credit card fraud in relation to the COVID-19 pandemic, emphasizing the growing reliance on internet resources. Using a two-stage evaluation process and a real-world European cardholder dataset. Sagadevan and Hassain Malim focused on preventing credit card fraud by using data mining and machine learning to find real and fake transactions by figuring out data patterns preventing credit card fraud by using data mining and machine learning to find real and fake transactions by figuring out data patterns [10]. After preprocessing the dataset, the study uses Bayesian network classifiers for supervised classification, with an accuracy of over 95%. Nguyen, Tahir and Abdelrazek presented a extensive research on deep learning techniques for credit card fraud detection and evaluation of how well they perform in comparison to different machine learning algorithms on three distinct financial datasets [14].

Bineet Kumar Jha, Sivasankari G and Venugopal K R I challenged to analyze financial crimes linked to fraudulent activities when conventional data mining techniques are unable to fully address them. In the retail industry, fraud is detected and prevented by using big data analytics to find unusual patterns. A variety of predictive analytics tools are used to handle large amounts of data and their patterns [15]. Applied big data analytics to spot odd trends and stop retail fraud. Singh Yadav and Marpe Sora identified frauds employing different text mining methods and safeguard, the investments of the public, financial regulators and auditors benefit from this investigation [16]. The study highlights the role that active models play in protecting public investments and how crucial they are in identifying financial reporting fraud. Thennakoon, Bhagyani, Premadasa and Mihiranga focused four primary fraud occurrences in real-world transactions. Each fraud is handled by a number of machine learning models, and evaluation determines which approach works best [17]. Examined credit card fraud incidents and use a number of machine learning models to handle different fraud types. In order to effectively prevent fraud in real-world transactions, the study highlights the significance of real-time credit card fraud detection and suggests a novel technique to handle skewed data distribution. Pranali Pawar described a reliable technique for data mining that finds suspicious behavior in healthcare providers in order to detect health insurance fraud [18]. The study draws attention to the growing concern over health insurance fraud and abuse as well as the application of data mining more especially, supervised and unsupervised learning techniques in the identification of false claims. Leena Shibu presented an examination of the methods currently employed in social media fraud detection with the goal of offering a thorough analysis of the various methods for spotting social media frauds [20]. Broadened the use of modern methods for detecting social media fraud and emphasized the value of watching user behaviour to identify and stop unwanted activity. The reach of social media is reviewed, and the growing frequency of fraud and its financial ramifications are acknowledged.

this paper suggested hybrid model, which combines logistic regression and decision trees, overcomes the drawbacks of conventional models by providing Fraud identification, which is greatly improved by achieving 98.1% detection accuracy. By Enhancing adaptability, the hybrid technique guarantees long-term efficacy by adjusting to changing fraud tactics. Sensitivity and accuracy are balanced, the model finds a critical middle ground between correctly identifying fraudulent activity and recognizing real transactions. The study makes a substantial contribution to the field of financial fraud detection by putting forth a fresh and useful hybrid model that expands on prior findings and resolves important shortcomings. Through the combined use of Decision Trees and Logistic Regression, the model opens the door to a more flexible and resilient method of defending financial systems and people against the ever-present risk of fraud.

III. Methodology

The approach is characterized by a well-organized architecture created to handle the particular difficulties at hand.

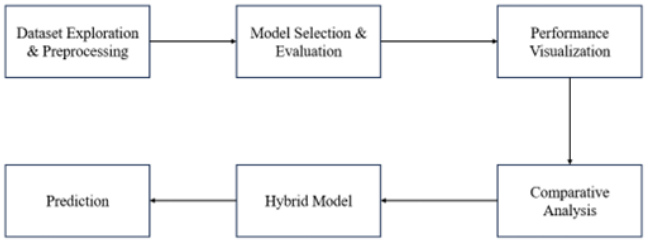

Fig.1: Block Diagram

The model architecture, as seen in Fig. 1, represents an organized methodology made up of six essential phases, each of which is crucial to determining the project's final result. Dataset exploration, preprocessing, model selection and evaluation, performance visualization, comparative analysis, building a hybrid model, and prediction are all included in these discrete stages. Each step contributes significantly to the creation and improvement of the model's overall effectiveness, which results in a novel and all-encompassing approach to combating financial fraud via the integration of hybrid models.

The section that follows provides a detailed explanation of each step in the architecture.

A. Dataset

An effective and "existing" dataset that was carefully prepared and analyzed is used to train the model. We thought the dataset, which was made public via the "kaggle" website, was the best. Both fraudulent and non-fraudulent transactions are included in the "fraudTrain.csv" dataset, which has undergone extensive analysis for a wide range of factors. The 'fraudtrain.csv' dataset includes important features that are necessary for the identification of fraud, including 'Trans_date_trans_time,' 'amt,"merchant,' and 'category.' Less crucial features including "first" & "last," "trans_num," "unix_time," "merch_lat," and "merch_long" are present in the dataset, despite the modest relevance of "cc_num," "gender," "Job," and "dob." The goal variable for binary classification—which is essential for detecting fraudulent transactions is called "is_fraud." The format of this dataset facilitates thorough analysis and modeling with the goal of identifying and reducing financial fraud.

B. Preprocessing.

To enhance the model's performance, efficient preprocessing has been applied. In the early preprocessing stages, the approach computes transaction amount and category statistics using the 'is_fraud' label. This sampling strategy was employed to balance the dataset and account for the inherent rarity of fraudulent transactions. The training dataset is developed with randomization and consistency in mind. Cleaning up the data by removing specific category columns that aren't required for model training is an additional preprocessing step.

Finally, the complete training dataset is encoded using one-hot encoding, which converts category variables into binary columns that are suitable for machine learning. Although the technique doesn't explicitly split the data into training and testing groups, it does prepare the feature matrix 'X' and target vector 'y' for machine learning.

C. Model Selection and Evaluation.

In order to conduct a comprehensive analysis of fraud detection, particular binary classification specifications call for customized classification algorithms designed to precisely identify fraudulent transactions. Machine learning models that showed less constraints and produced the best results in this field of study were chosen at random during the model selection procedure. The method, which uses K-Fold Splitting (kf) to evaluate robust models, is shown in Fig. 2 and proceeds methodically from the dataset (X, y). Several machine learning models are used in this procedure, where the Null Model is used as the standard for all further assessments. Because of its interpretability and ability to shed light on the relationship between the predictor variables and the chance of fraud, logistic regression is the first model of choice. By using regularization and feature selection, the Post Lasso Logistic Model improves performance and increases the accuracy of fraud detection. While Random Forests efficiently handle high-dimensional data by utilizing many decision trees, decision trees provide transparency in decision-making and insight into fraudulent elements. The KNN model detects trends in fraudulent transactions by comparing attribute features that are close to one other. To ensure a thorough and in-depth understanding of each model's efficacy in fraud detection, an evaluation method that is both in- and out-of-sample is used to examine each model. Performance measures are then employed to measure each model's performance.

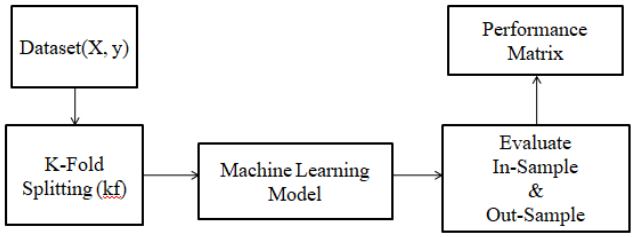

Fig.2: Model Assessment through K-fold cross Validation

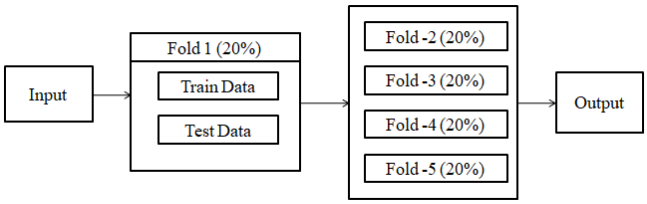

Fig.3: K- fold cross Validation Framework

This process depicted in Fig.3, illustrates the K-Fold Cross-Validation technique's iterative process. The procedure works by splitting the total dataset into five folds, each of which contains 20% of the data. To enable the model to be trained on one part of the fold and tested on another, each fold is further divided into training and test data. This procedure is done for each of the five folds, allowing for a thorough assessment of the model's performance while reducing the risk of biased model evaluation.

D. Evaluation

The thorough investigation of classification performance metrics contains important metrics for evaluating binary classification models. By precisely classifying genuine fraudulent transactions as fraudulent in fraud detection, the True Positives (TP) indicate exactly predicted events within the positive class. Correctly identifying genuine, non-fraudulent transactions, True Negatives (TN) precisely count the anticipated cases in the negative class. When legitimate, non-fraudulent transactions are mistakenly interpreted as fraudulent, this is known as a false positive (FP). The term False Negatives (FN) refers to occurrences when the model failed to correctly identify actual fraudulent transactions, indicating that the positive examples it predicted were incorrect. When taken as a whole, these metrics provide important information about how well a model determines which transactions are fraudulent and which are not.

Accuracy, sensitivity, specificity, and G-mean are among the classification performance indicators analyzed. The percentage of accurately identified cases both true positives and true negatives among all the instances is known as accuracy. Recall or True Positive Rate are other names for sensitivity, which quantifies a model's capacity to accurately detect positive instances, such as fraudulent transactions. Specificity gauges a model's capacity to accurately pinpoint unfavourable occurrences, such as transactions that aren't fraudulent. A balanced measurement that takes into account both sensitivity and specificity is offered by the geometric mean.

1. *Accuracy (Acc):*

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

2. *Sensitivity (Recall):*

$$Recall = \frac{TP}{(TP+FN)} \quad (2)$$

3. *Specificity:*

$$Specificity = \frac{TN}{(TN+FP)} \quad (3)$$

4. *G-mean (Geometric Mean):*

$$Geometric\ mean = \sqrt{Sensitivity \times Specificity} \quad (4)$$

E. Performance Visualization

Confusion Matrix:

The confusion matrices illustrated in Figure 4(a) & 4(b), provide a visual representation of the prediction accuracy of the model by distinguishing between true positives, false positives, true negatives, and false negatives. It provides a thorough understanding of how well the model performs in categorizing different scenarios.

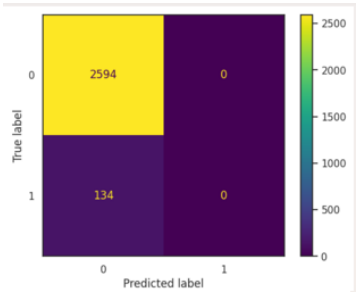

Fig.4(a): Confusion Matrices

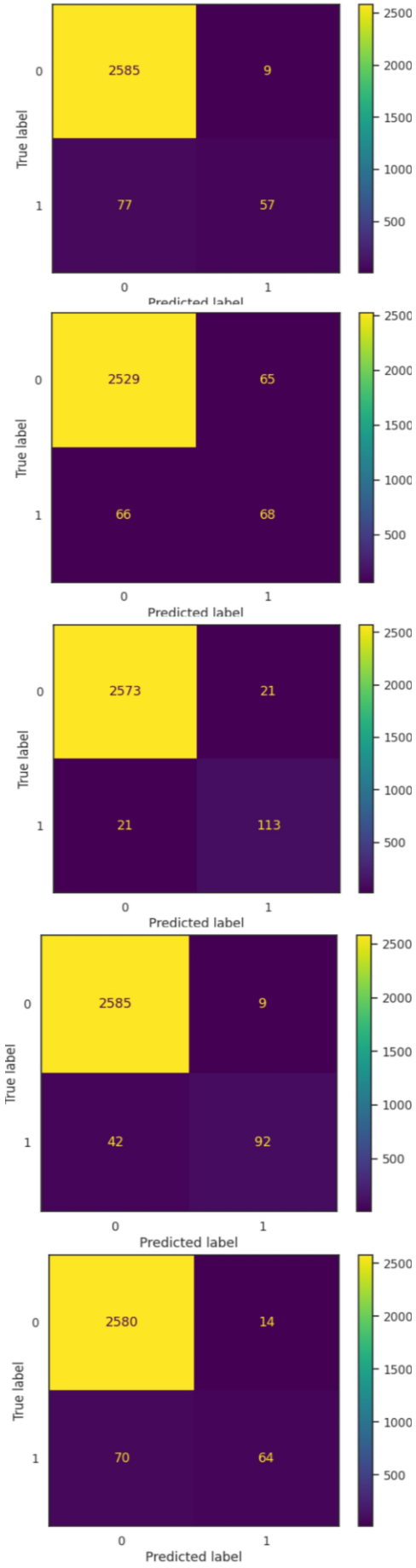

Fig.4(b): Confusion Matrices

Learning Curve:

The learning curve, which is shown in Fig. 5(a) & 5(b), shows how well the model performs in relation to the number of training samples. It evaluates how the accuracy of the model varies with the availability of fresh training data. It provides information on how the amount of the training data affects the model's performance by showcasing the convergence of the training and cross-validation scores.

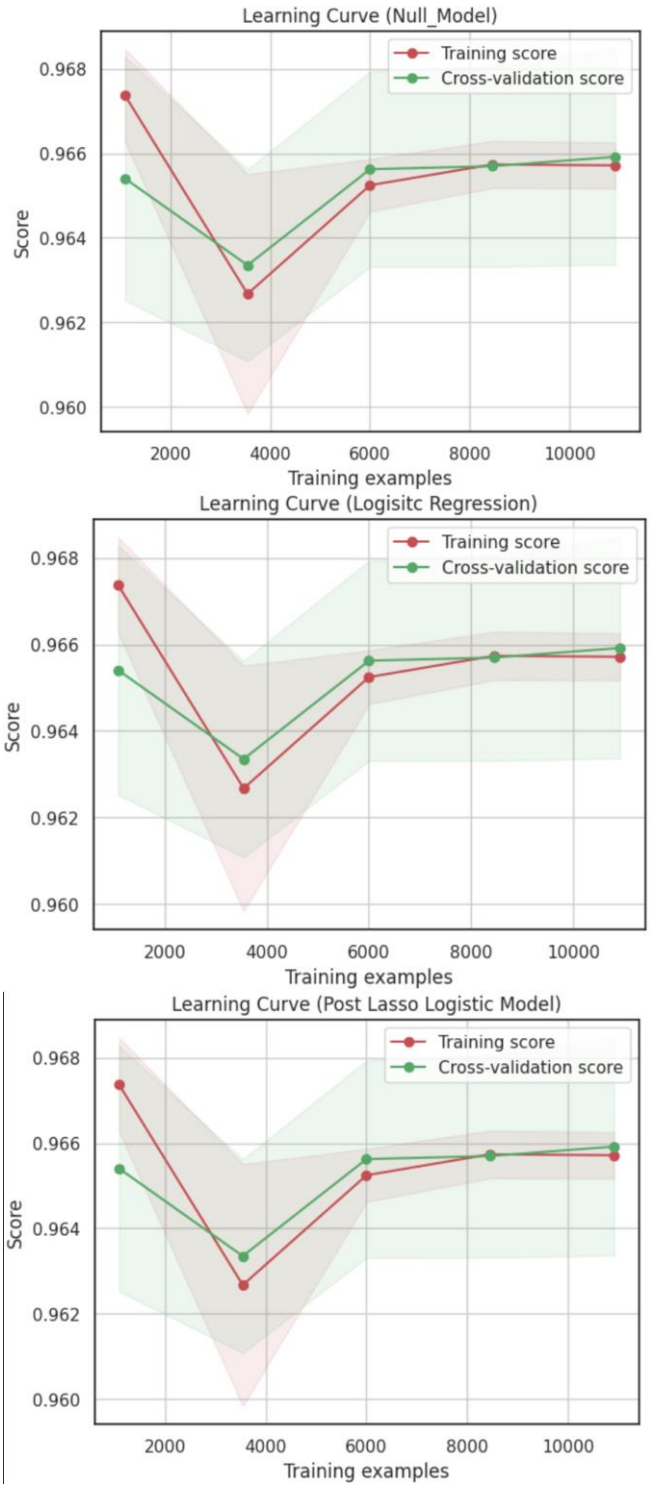

Fig.5(a): Learning Curves

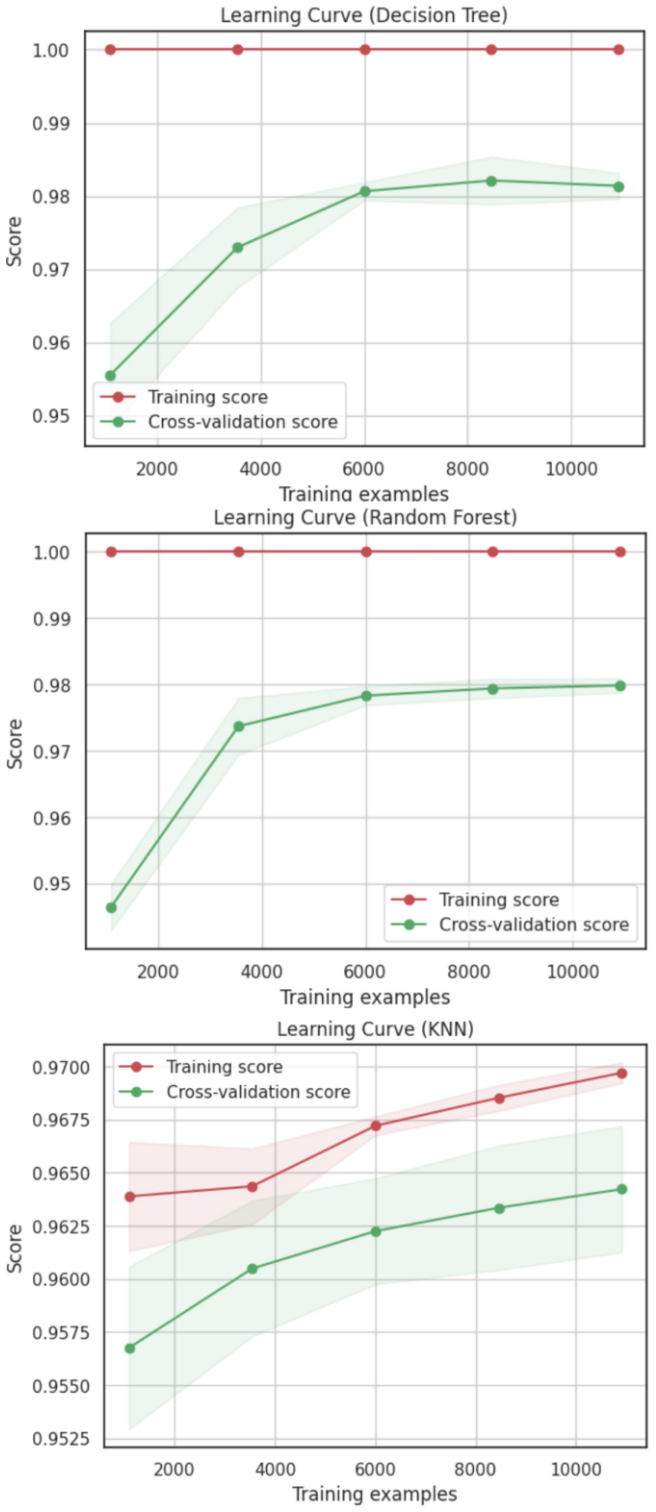

Fig.5(b): Learning Curves

F. Comparative Analysis

The detailed performance characteristics of several fraud detection methods are displayed in Table 1. Each model's G-mean, sensitivity, specificity, and accuracy values are listed in the table. In particular, the decision tree shows the maximum sensitivity and G-mean, but the logistic regression shows a compromise between specificity and accuracy.

Table -1: Evaluation Metrics

Model	Accuracy	Sensitivity	Specificity	G-mean	Accuracy (%)
Null Model	0.944953	0.000000	1.000000	0.0000	94.495
Logistic	0.96459	0.446097	0.994731	0.66582	96.4597
Post Lasso	0.943121	0.407602	0.974332	0.63005	94.312
Decision Tree	0.979990	0.803890	0.990393	0.89210	97.9990
Random Forest	0.975592	0.621741	0.996131	0.78674	97.5592
KNN	0.96144	0.428071	0.992478	0.65072	96.1445

G. Building a Hybrid Model

Following a thorough analysis of numerous variables, the "Decision Tree" and "Logistic Regression" models were determined to be the most promising methods for detecting fraud. It is thought that combining the advantages of both models into a hybrid strategy will benefit from the interpretability of Logistic Regression and the ability of Decision Trees to identify complex decision boundaries, potentially improving overall fraud detection performance.

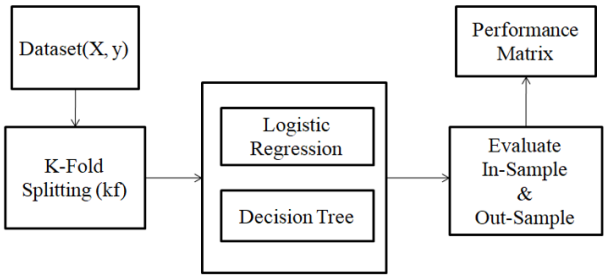

Fig.6: Hybrid Model Architecture

As shown in Fig. 6, the model evaluation procedure uses K-Fold cross-validation, applying the Decision Tree and Logistic Regression methods to the split dataset in turn. It generates an extensive performance matrix by assessing performance in both in-sample and out-of-sample circumstances. Accurate fraud detection and model comparison are made easier by this iterative procedure.

A strong performance is indicated by the high sensitivity, specificity, and G-mean of the hybrid model's out-of-sample assessment, as illustrated in Fig.7.

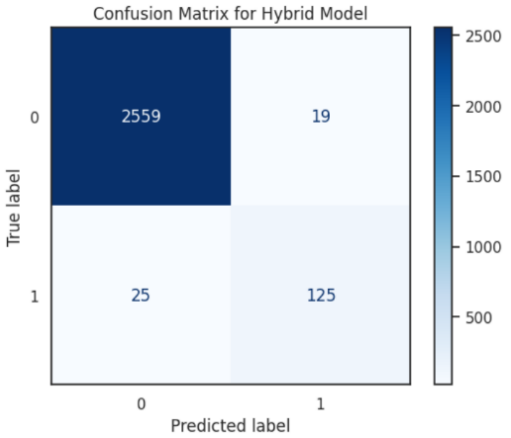

Fig.7: Accuracy Output

```
Out of Sample Evaluation for the Hybrid Model:
accuracy       0.981749
Sensitivity    0.825572
Specificity    0.990847
G-mean         0.904389
dtype: float64
```

Fig .8: Confusion Matrix for Hybrid model

H. Prediction

The approach makes predictions by combining Decision Trees and Logistic Regression into a hybrid model. Once every model has been trained using the entire dataset, predictions are produced for each class separately and then averaged for the positive class. Fraudulent (1) and non-fraudulent (0) transactions are classified by converting continuous forecasts into binary form and applying a 0.5 threshold. The fraudulent transactions that have been flagged are filtered systematically by the prediction model, which highlights transactions that are assigned a binary prediction of 1. For these identified incidents, information is shown that includes transaction amounts and other available details. Table-2 shows a visual representation of the process's output.

Table -2: Fraudulent Transactions

S.No.	Transaction ID	Amount
1)	12	329.8
2)	43	594.09
3)	82	903.55
4)	134	311.41
5)	143	846.52
6)	145	1088.85
7)	188	427.02
8)	207	776.84
9)	237	708.06
...	...	...

IV. Conclusion

The field of financial fraud detection has considerable obstacles when it comes to dealing with fraudulent strategies that are always changing. The dynamic nature and complexity of fraudulent patterns are typically beyond the capabilities of traditional machine learning models, such as Random Forests, Decision Trees, and Logistic Regression. This methodology's introduction of a hybrid model that combines Decision Trees and Logistic Regression is what makes it revolutionary. This new method not only reduces false negatives and tackles class imbalance, but it also greatly raises the accuracy of fraud detection. In contrast to alternative models, the hybrid approach exhibits robust overall performance, efficiently mitigating the detrimental effects of financial fraud on organizations. Finally, in order to tackle the increasingly pressing issues of financial fraud, this approach offers a sophisticated and all-encompassing solution that greatly improves the accuracy and versatility of fraud detection techniques.

V. References

[1] Markus Goldstein, Seiichi Uchida, "A Comparative Evaluation of Unsupervised Anomaly Detection Algorithms for Multivariate Data". Dongxiao Zhu, Wayne State University, April 19, 2016.

[2] Bharathi Mohan Gurusamy, Prasanna Kumar Rengarajan, Parthasarathy Srinivasan, "A hybrid approach for text summarization using semantic latent Dirichlet allocation and sentence concept mapping with transformer", Amrita Vishwa Vidyapeetham, Apr 3, 2023.

[3] Hangjun Zhou, Guang Sun, Sha Fu, Wangdong Jiang and Juan Xue, "A Scalable Approach for Fraud Detection in Online E-Commerce Transactions with Big Data Analytics", Tech Science Press, .179-192, 2019.

[4] G. Bharati Mohan ,R. Prasanna Kumar, "A COMPREHENSIVE SURVEY ON TOPIC MODELING IN TEXT SUMMARIZATION".

[5] Oluwadare Samuel Adebayo; Thompson Aderonke Favour-Bethy; Owolafe Otasowie; Orogun Adebola Okunola, "Comparative Review of Credit Card Fraud Detection using Machine Learning and Concept Drift Techniques", July 2023.

[6] Patrick McDaniel, "Big Data Analytics for Security". University of Texas at Dallas.

[7] Chereddy Spandana, Ippatapu Venkata Srisurya, S. Aasha Nandhini, R. Prasanna Kumar, G. Bharathi Mohan, Parathasarathy Srinivasan, "An Efficient Genetic Algorithm based Auto ML Approach for Classification and Regression", Amrita Vishwa Vidyapeetham,January 2023

[8] Noor Saleh Alfaiz, Suliman Mohamed Fati, "Enhanced Credit Card Fraud Detection Model Using Machine Learning", 21 February 2022.

[9] Sk. Kamaruddin, "Credit Card Fraud Detection using Big Data Analytics: Use of PSOAANN based One-Class Classification".

[10] Ong Shu Yee, Saravanan Sagadevan and Nurul Hashimah Ahamed Hassain Malim, "Credit Card Fraud Detection Using Machine Learning as Data Mining Technique". University Sains Malaysia.

[11] John O. Awoyemi, Adebayo O. Adetunmbi, Samuel A. Oluwadare, "Credit card fraud detection using Machine Learning Techniques".

[12] Abhinav Srivastava, Amlan Kundu, Shamik Sural, Senior Member, "Credit Card Fraud Detection Using Hidden Markov Model", MARCH 2008.

[13] GUANSONG PANG and CHUNHUA SHEN, "Deep Learning for Anomaly Detection: A Review".

[14] Thanh Thi Nguyen, Hammad Tahir, Mohamed Abdelrazek Ali Babar, "Deep Learning Methods for Credit Card Fraud Detection".

[15] Bineet Kumar Jha, Sivasankari G and Venugopal K R, "Fraud Detection and Prevention by using Big Data Analytics".

[16] Ajit Kr. Singh Yadav, Marpe Sora, "Fraud Detection in Financial Statements using Text Mining Methods".

[17] Anuruddha Thennakoon, Chee Bhagyani, Sasitha Premadasa, Shalitha Mihiranga, Nuwan Kuruwitaarachchi, "Real-time Credit Card Fraud Detection Using Machine Learning".

[18] Pranali Pawar, "Review on Data Mining Techniques for Fraud Detection in Health Insurance".

[19] G. Bharathi Mohan, R. Prasanna Kumar, Srinivasan Parathasarathy, S. Aravind, K. B. Hanish G. Pavithria , " Text Summarization for Big Data Analytics: A Comprehensive Review of GPT 2 and BERT Approaches ".

[20] Leena Shibu, Dr.Ajeet Chikkamannur , " A SURVEY OF FRAUD DETECTION TECHNIQUES IN SOCIAL MEDIA ". New Horizon College of Engineering, 4.(11): November, 2015.