Fraud Detection in Financial Transactions: A Comparative Study of Machine Learning Models with Ensemble Voting

Boddu Krishna Chaitanya Sravanthi[1], Sai Tejaswini Keerthi[2], Vempada Latha[3], Guddati Vijaya Lakshmi[4], Ch.V.V. Satyanarayana[5] and Kosanam Vennela[6]
{chaithanyaboddu456@gmail.com[1], saitejaswini.keerthi@gmail.com[2], vempadalatha@gmail.com[3], gud.vijaya@gmail.com[4], csn@aditya.ac.in[5], kosanamsrinu12@gmail.com[6]}

Department of BCA Data Science, Aditya Degree & PG College, Kakinada (Autonomous), Andhra Pradesh, India[1]
Department of B.Sc. Data Science, Aditya Degree College, Tuni, Andhra Pradesh, India[2]
Department of Data Science, Aditya Degree College, Gajuwaka, Andhra Pradesh, India[3]
Associate Professor, Department of Data Science, Aditya Degree and PG College, Kakinada, Andhra Pradesh, India[4, 5]
Department of BCA, Aditya Degree & PG College, Gopalapatnam, Andhra Pradesh, India[6]

Abstract. Real-time fraud detection in financial transactions presents great importance for the stability of financial systems. The investigators proposed a machine-learning-based model to classify fraudulent activities in financial transactions using a dataset with 6.3 million rows. The methodology involves extensive data preparation, including removal of irrelevant columns, encoding of categorical variables, scaling of the data, and adaptation of the imbalances presented within the response classes using the Synthetic Minority Over-sampling Technique (SMOTE). Various machine-learning models, such as Random Forest, Gradient Boosting, Logistic Regression, and Support Vector Machine (SVM), are used to detect fraud. A voting ensemble is used to enhance the predictive quality and robustness. After model evaluation on proper metrics outlines such as the model-comparison precision and appropriateness, this verifies a good real-time fraud detection system. Results to date suggest that the system has increased the detection rate of fraudulent transactions significantly, making it an impressive contender for real-time fraud examination within the context of finance.

Keywords: Real-time fraud detection, machine learning, financial transactions, Synthetic Minority Over-sampling Technique (SMOTE), ensemble learning, Random Forest, Gradient Boosting, Support Vector Machine (SVM).

1 Introduction

Organizations and online payment systems are increasingly concerned about fraud in digital transactions. Traditional rule-based detection methods often fall short, as they struggle to capture complex patterns and adapt to new fraud techniques. This limitation can result in delayed detection or overlooked fraudulent activity, leading to financial losses.

Advances in machine learning (ML) are transforming fraud detection by providing more robust and scalable approaches. By analyzing diverse data such as transaction amounts, user behavior, and account details, ML algorithms can detect patterns that indicate suspicious

ICITSM-Part II 2025, April 28-29, Tiruchengode, India

DOI 10.4108/eai.28-4-2025.2358048

activity. Techniques including ensemble learning, anomaly detection, and supervised models have further improved the effectiveness of fraud detection systems.

Despite this progress, it is challenging to handle imbalanced data which is common in fraud detection, since fraudulent transactions are rare compared to accepted ones. This imbalance may lead to incorrect pre- dictions and hence reduces the models' performances. To make the model more effective, ensemble techniques along with over-sampling technologies such as the Synthetic Minority Over-sampling Technique (SMOTE) are used.

In this study, we propose a machine learning algorithm-based efficient fraud detection system that involves the integration of different existing models such as Random Forest, Support Vector Machine (SVM), Gradient Boosting and Logistic Regression. In order to improve the accuracy, an ensemble learning method is adopted to evaluate and combine these models. An additional enhancement to address imbalanced datasets is added to the system for accurate fraud recognition. We take the traditional evaluation metrics such as precision, recall, F 1 and demonstrate the performance of the model to determine fraud signals embedded in real financial transactions. The objective of this project is to establish an efficient and scalable technique for fraud detection in financial systems.

2 Related Work

SB krishna Adusumilli [1] investigated machine learning (ML) techniques application for the enhancement of banking system fraud detection. To deal with the class imbalance, it evaluates techniques like ensemble methods, SVM, neural networks and decision trees over a SMOTE-enriched set. The study addresses the high performance of neural networks, which accomplished a high accuracy together with a good precision and recall. However, the work is not without limitations, the most prominent of them being the computational complexity of more advanced models, which limits the applicability of such methods to real-time scenarios. The contributors pay special attention to the role of the ML in the fight against fraud and acknowledge the existence of the challenges which include unequal samples, feature designing, privacy issues, contributing to the development of strong AI-decided solutions in financing.

A Singla and H Jangir [2] examined machine learning and predictive analysis methods for identifying fraud in real- time bank transactions. The study contrasts traditional rule- based approaches with advanced methods such as anomaly detection and contribution analysis, leveraging algorithms like decision trees, regression, and neural networks. By analyzing streaming financial data, the research demonstrates the ability of predictive analytics to provide timely insights and reduce false positives. Despite these advancements, the paper notes that challenges such as adapting to changing fraud patterns and ensuring data privacy remain. The findings underscore the transformative potential of integrating predictive models with machine learning to enhance fraud detection and support informed business decisions in financial domains.

RAL Transactions M Ladeira [3] has proposed a Fraud Detection System (FDS) to minimize false positives in the analysis of big volume financial transactions under real time constraint. The proposed method integrates the unsupervised outlier detection steps and the VA in order

to find the suspicious transactions efficiently. Through a real-world dataset from a Brazilian bank consisting of more than 30 million transactions per day, the system creates a model tailored to customers' historical behaviour and uses methods, including PCA and RFE, for feature selection. Performance of algorithms like Isolation Forest and One-Class SVM in detecting anomalies was proven to be satisfactory. Nevertheless, issues such as dataset imbalance and the computational cost for online processing, are still important challenges. It stresses the necessity of involving human's expertise and employing visual aids to enhance the accuracy of fraud detection and adaptability of the system.

RT Potla [4] overcame the limitations of rule-based systems in fraud detection by using real-time machine learning based solutions. The goal is to achieve higher accuracy in the detection of fraud and lower false positive rates, while keeping near-real time analysis on large sets of transaction data. To detect anomalies, the research applies unsupervised learning techniques such as autoencoders and supervised classifications such as Random Forests and Gradient Boosting Machines. Experimental results show the superior performance of our framework in terms of detection accuracy, false positive rates and scalability. Nevertheless, issues in system latency, data confidentiality and model interpretability still need to be addressed

T Amarasinghe [5] examined a range of anomaly and machine learning methods for identifying bank transaction fraud. The objective is to identify effective approaches among supervised methods like Bayesian Networks, Recurrent Neural Networks (RNNs), and Support Vector Machines (SVMs), as well as unsupervised methods like clustering and anomaly detection. The study highlights the strengths and limitations of each technique, emphasizing the need for hybrid approaches to address imbalanced datasets and improve model performance. The limitations include reliance on labeled data, computational cost, and interpretability challenges.

E Pan [6] focused on using machine learning to detect fraudulent transactions, addressing the growing complexity and volume of fraudulent activities. The objective is to utilize machine learning's pattern recognition and real-time processing capabilities to enhance fraud prevention strategies. Techniques such as decision trees, random forests, and neural networks are discussed, with practical case studies demonstrating improved detection accuracy and reduced false positives. Challenges include data quality, model interpretability, and high implementation costs, limiting widespread adoption

R Sharma and A Sharma [7] explores the application of machine learning and deep learning techniques to enhance fraud detection in digital finance. The authors focus on com- paring Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), using a dataset of transactional data. Their methodology includes data cleaning, model training with supervised and unsupervised approaches, and evaluating performance metrics like accuracy, sensitivity, specificity, and AUC. The RNN model outperformed CNN, achieving a 95.8% accuracy. While demonstrating robustness in identifying fraudulent transactions, the study identifies limitations such as high computational power demands and ethical concerns surrounding data privacy and model transparency.

P Shukla et al. [8] evaluates six machine learning models (Naive Bayes, Neural Network, Decision Tree, Support Vector Machine, Logistic Regression, and Random Forest) for financial fraud detection. Random Forest emerged as the most effective model, achieving

96.1% accuracy and high stability across different datasets. The study utilized preprocessed data and tested various algorithms for optimal results, emphasizing the importance of ensemble methods and real-time fraud detection. Challenges included addressing imbalanced datasets and enhancing predictive accuracy through ensemble and pipelining strategies.

GJ Priya and S Saradha [9] emphasizes the role of machine learning in combating fraud across sectors, especially in real- time applications. The authors highlight the importance of structured lifecycle approaches involving monitoring, learning, detecting, and preventing fraud. Algorithms such as Random Forest, SVM, and hybrid models are discussed, with Random Forest being noted for its balance of sensitivity and accuracy. The paper also advocates for a centralized global fraud detection framework, enabling shared learning across organizations to counter fraud more effectively.

G Manoharan et al. [10] explored the use of machine learning for real-time fraud detection in financial transactions. The study employs models like decision trees, support vector machines, and neural networks to detect patterns and anomalies in transactional data. Using large datasets, the methods demonstrated improved fraud detection rates and reduced false positives, highlighting their potential for enhancing financial security. However, challenges like data quality, model interpretability, and privacy compliance remain obstacles to implementation.

Here are the limitations specifically for Real-time Financial Transaction Fraud Detection Using Machine Learning based on the previously reviewed publications:

- As fraudulent transactions are uncommon in comparison to genuine ones, datasets are heavily biased, which affects how well machine learning models work.
- Fraudulent behaviors evolve rapidly, making it challenging for static models to remain effective without frequent retraining.
- Models like Random Forest and Neural Networks can overfit the training data, especially when noisy data or imbalanced classes are involved, reducing their generalizability to new transactions.
- Using sensitive customer data, such as location, device in- formation, and transaction history, poses ethical concerns and regulatory challenges around data protection.
- Fraud patterns and detection requirements vary significantly across industries and regions, limiting the transferability of models trained on specific datasets.

3 Proposed Methodology

3.1 Data Collection

This data set is taken from Kaggle, which contains 6,362,620 records to simulate financial transaction and with 11 attributes, such as the type of transaction, amount, new and old balance of the origin and destination and flag information of fraud. It is also labelled with both is Fraud (which is the fraud transactions) and is Flagged Fraud (which would be fraud

transactions that are to be flagged) which makes it good as a supervised fraud detection problem.

3.2 Data Preprocessing

Data Preprocessing is one of the essential steps in a machine learning project where this process converts raw data to a clean data frame that a model can be fit to yield more accurate results. Preprocessing becomes even more critical for identifying fraud in financial transactions, as data needs cleaning (to remove noise), dealing with imbalanced distribution of the datasets and encoding that allows the model to understand patterns of fraudulent activities correctly. Fig 1 shows Implementation flow chart.

3.2.1 Dropping Irrelevant Columns

It is essential to eliminate features that do not enhance the estimated performance of the model by eliminating unnecessary columns. User IDs and other non-informative columns should be removed when financial fraud is detected. As a result, the model becomes less complex, there is less chance of overfitting, and training computations are improved.

3.2.2 Encoding Categorical Variables

Categorical variables, such as transaction type and user or account identifiers, need to be encoded into numerical values for machine learning algorithms to process them effectively. Techniques such as one-hot encoding or label encoding are commonly used to transform these categorical features into a format that models can understand, improving the accuracy of predictions.

3.2.3 Normalization

Normalization aims to standardize numeric features to the same scale so that features with larger values do not overshadow the learning. In transaction history datasets, values such as transaction amount and balances may have very different orders of magnitude. By performing, e.g. Min-Max scaling or Z-score standardization to the numerical features, all of them are weighted in the same way into the model, which increases the fraud detection performance of our model.

3.2.4 Handling Imbalanced Dataset using SMOTE

Recognizing that there are significantly more fraudulent trans- actions than genuine ones in the dataset, it results in an imbalance that makes fraud detection extremely difficult. Biased models that more often predict the majority class result from this imbalance. This is addressed with the Synthetic Minority Over-sampling Technique (SMOTE), which creates fraudulent samples of the minority class (fraudulent transactions). In order to create fraudulent instances, SMOTE combines within the minority class sample and its closest neighbors. The following is the formula to create a fraudulent sample:

$$Synthetic\ Sample\ =\ Sample_i\ +\ \lambda\ (Sample_k\ -\ Sample_i) \qquad (1)$$

where λ is a random value between 0 and 1, and Sample_i and Sample_k are the original minority class sample and its nearest neighbor, respectively.

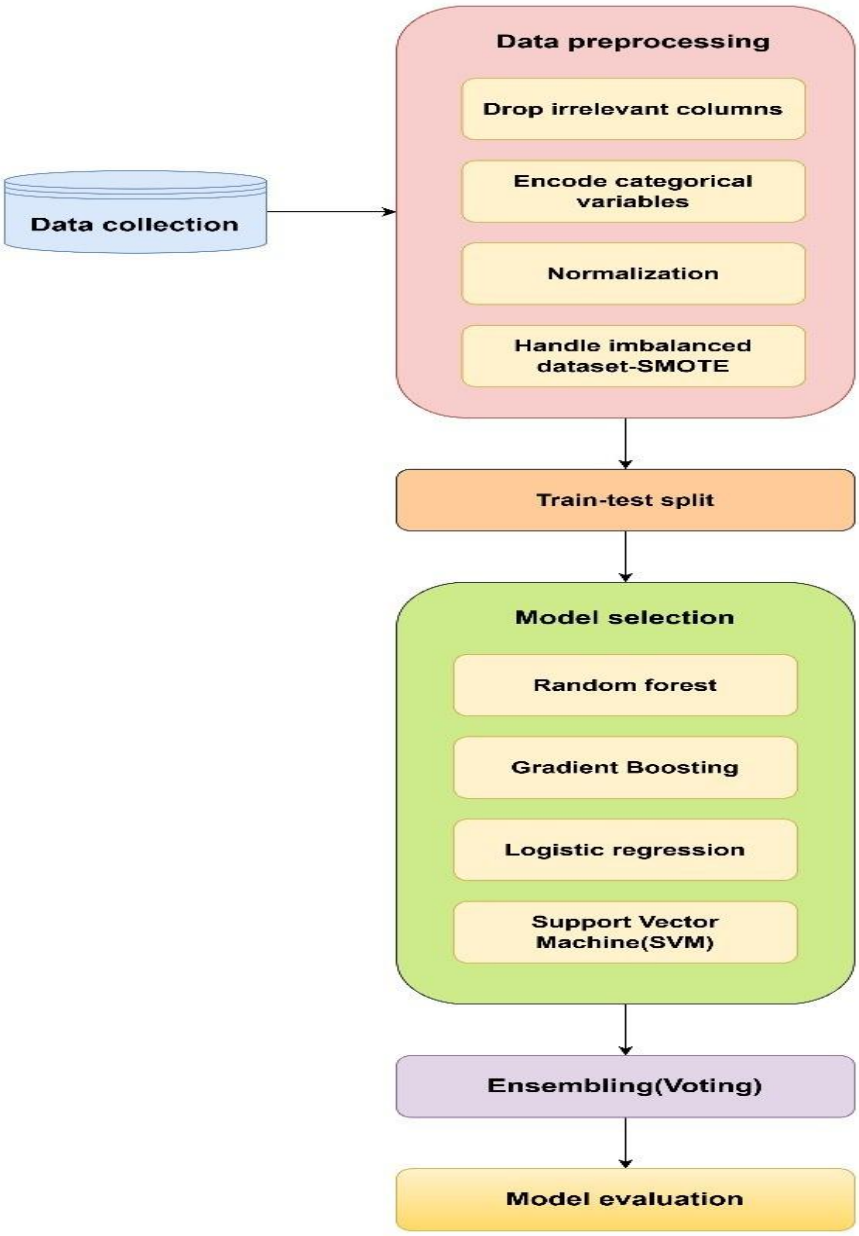

Fig. 1. Implementation flow chart.

3.3 Train-test-split

The dataset is categorized into two parts: a training set and a testing set. This division helps ensure that the model can effectively generalize to new data. The training set is used to train the model, allowing it to learn patterns associated with both fraudulent and legitimate transactions. The testing set, which remains separate from the training data, is then used to evaluate the model's performance and its ability to classify unseen transactions correctly. By testing the model on data, it has not encountered before, this approach minimizes the risk of overfitting and provides a clearer picture of how well the model can identify fraud in real-world applications.

3.4 Model Selection

The selection of appropriate machine learning models is crucial for achieving high accuracy in fraud detection, as different models may perform better based on the nature of the dataset and the problem at hand. For this project, several models are chosen for evaluation based on their ability to handle complex relationships within the data and their effectiveness in detecting fraud in real-time financial transactions.

- Random Forest: Several decision trees are built using the Random Forest ensemble learning technique, which then aggregates the output to increase prediction accuracy. The following is the Random Forest prediction formula for classification:

$$\hat{y} = majority\ voting\ of\ (\hat{y}1, \hat{y}2, \ldots, \hat{y}n) \quad (2)$$

  where $\hat{y}i$ represents the predictions of each tree, and the final prediction $\hat{y}$ is the majority vote among them.

- Gradient Boosting: Gradient Boosting develops trees one after the other, fixing the errors of the one prior to it. In gradient boosting, each model's update rule is:

$$fm + 1(x) = fm(x) + \eta \cdot \delta m(x) \quad (3)$$

  where $fm(x)$ is the prediction at step m, $\delta m(x)$is the residual of the previous model, and η is the learning rate?

- Logistic Regression: The logistic function is used in logistic regression to describe the likelihood of a binary outcome. The model is defined as:

$$P(y = 1|X) = \frac{1}{1+e^{-(\beta 0+\beta 1x1+\ldots+\beta nxn)}} \quad (4)$$

  where $P(y = 1|X)$ is the probability of fraud, β_0 is the intercept, and $\beta_1, \ldots, \beta_n$ are the coefficients of the features $x_1, \ldots, x_n$.

- Support Vector Machine (SVM): Support Vector Machine aims to find the hyperplane that best separates the classes. The decision rule for SVM is:

$$f(x) = sign(\langle w, x \rangle + b) \quad (5)$$

where $\langle w, x \rangle + b = 0$ represents the hyperplane, w is the weight vector, x is the input feature vector, and b is the bias term.

3.5 Ensembling

Voting is used in an ensemble method to increase the robustness and accuracy of fraud detection. Several foundation models, including Random Forest, Gradient Boosting, Logistic Regression, and Support Vector Machine (SVM), are combined in this method. Every model submits a prediction, and the majority vote of all the models determines the final prediction. When it comes to binary categorization (fraud vs. non-fraud), the class that most models predict is selected as the final choice. The individual predictions are combined using the majority vote method as follows:

$$\hat{y}_{final} = argmax(\sum_{i=1}^{n} \hat{y}_i) \quad (6)$$

where $\hat{y}_i$ is the prediction from the i-th base model, and n is the number of models? The final prediction $\hat{y}_{final}$ is the class with the highest number of votes. By combining the strengths of multiple models and reduce the chances of single-model bias, the voting-based ensemble approach to overall detection accuracy including imbalanced data such as fraud detection.

3.6 Model Evaluation

Model evaluation is important when assessing the performance of the fraud detection system. The goal is to measure how well the model can detect fraudulent transactions, and minimize the number of false positives and false negatives. The evaluation metrics chosen for this work are Accuracy, Precision, Recall, and F1 Score, for a reason that they provide a complete view of the model performance in accuracy during the prediction, trustworthiness, and the proportion of false positive to false negative.

- Accuracy: Accuracy measures the overall correctness of the model, calculated as the ratio of correctly predicted transactions (both fraud and non-fraud) to the total number of transactions. It is expressed as:

$$\text{Accuracy} = \frac{\text{TP+TN}}{TP+TN+FP+FN} \quad (7)$$

  where TP (True Positive) represents the number of correctly identified frauds, TN (True Negative) represents the number of correctly identified non-frauds, FP (False Positive) is the number of non-fraud transactions incorrectly classified as fraud, and FN (False Negative) is the number of fraud transactions incorrectly classified as non-fraud. While accuracy gives a general sense of model performance, it may not be reliable in imbalanced datasets, where the number of non-fraudulent transactions vastly outnumbers fraudulent ones.

- Precision: Precision quantifies the accuracy of the fraud predictions. It measures the proportion of actual fraudulent transactions among all transactions predicted as fraud.

Precision for fraud detection is calculated as:

$$Precision = \frac{TP}{TP+FP} \quad (8)$$

A higher precision indicates fewer false positives, ensuring that the model is not incorrectly flagging non- fraudulent transactions as fraudulent.

- Recall: Recall measures the ability of the model to identify all fraudulent transactions. It calculates the proportion of actual frauds that were correctly identified by the model. Recall for fraud detection is given by:

$$Recall = \frac{TP}{TP+FN} \quad (9)$$

A higher recall indicates that the model successfully detects most fraudulent transactions, even at the cost of potentially higher false positives.

- F1 Score: F1 Score is the harmonic mean of Precision and Recall, providing a balanced measure between them. It is particularly useful in situations where there is an imbalanced class distribution. The F1 Score is calculated

$$F1\ Score = 2 \cdot \frac{Precision \cdot Recall}{Precision+Recall} \quad (10)$$

Since both false positives and false negatives are significant in fraud detection, a higher F1 Score indicates a better balance between precision and recall.

These evaluation metrics collectively provide a detailed assessment of the fraud detection system, ensuring that the model is capable of accurately identifying fraudulent transactions while minimizing errors.

4 Experimental Results and Analysis

About Dataset:

The kaggle dataset consists of 6.362.620 financial transaction records with 11 features that contain important information regarding each transaction. That include construction of the word “step” (transaction time in hours), “type” (the type of transaction, such as CASHOUT or TRANSFER), “amount”, the amount transferred, old and new balances of the origin and destination account (“oldbalanceOrg”, “newbalanceOrig”, “oldbalanceDest”, and “newbalanceDest”) and identification (e.g., “nameOrig” and “nameDest”). The ‘isFraud ‘column shows a flag for fraudulent transactions and ‘isFlaggedFraud ‘is a manual flag. This data set is perfect for training machine learning to detect and analyse frauds in financial transactions.

Results:

Table 1. Model Evaluation Results for Fraud Detection.

Model	Accuracy	Precision	Recall	F1 Score
Random Forest	0.920	0.91	0.92	0.91
Gradient Boosting	0.930	0.92	0.93	0.92
Logistic Regression	0.900	0.89	0.91	0.90
SVM	0.910	0.90	0.92	0.91
Voting Ensemble	0.970	0.96	0.97	0.96

The table 1 shows the results of testing different models for fraud prediction. You have the performance metrics for the individual models (Random Forest, Gradient Boosting, Logistic Regression, SVM, and the Voting Ensemble). The Voting Ensemble model is the best performing in terms of all the metrics \ (it\) has the highest accuracy and F1 Score.

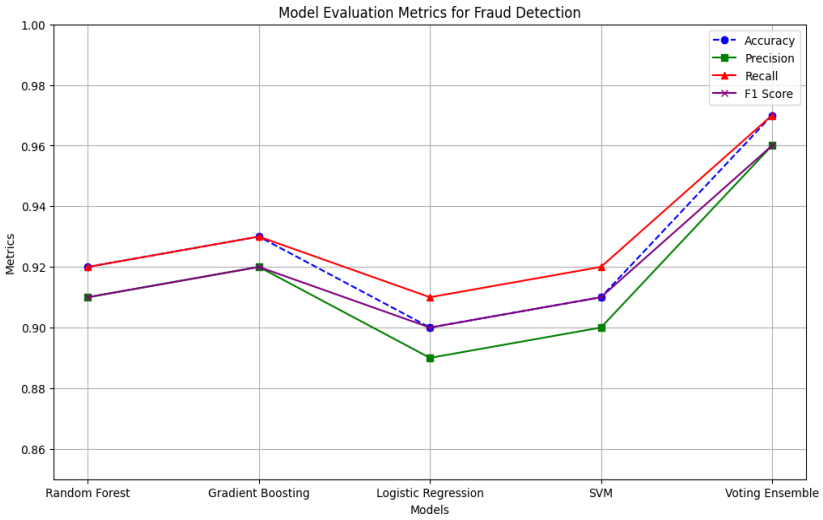

Fig- 2. Accuracy Comparison.

Fig 2 The chart visually illustrates the performance of different models with respect to Accuracy, Precision, Recall and F1 Score. It draws attention to the Voting Ensemble model superiority comparison to all of the other models, with the highest values of all measures. This plot easily enables comparison of how different models perform in fraud detection, the

ensemble model yielding the best overall results.

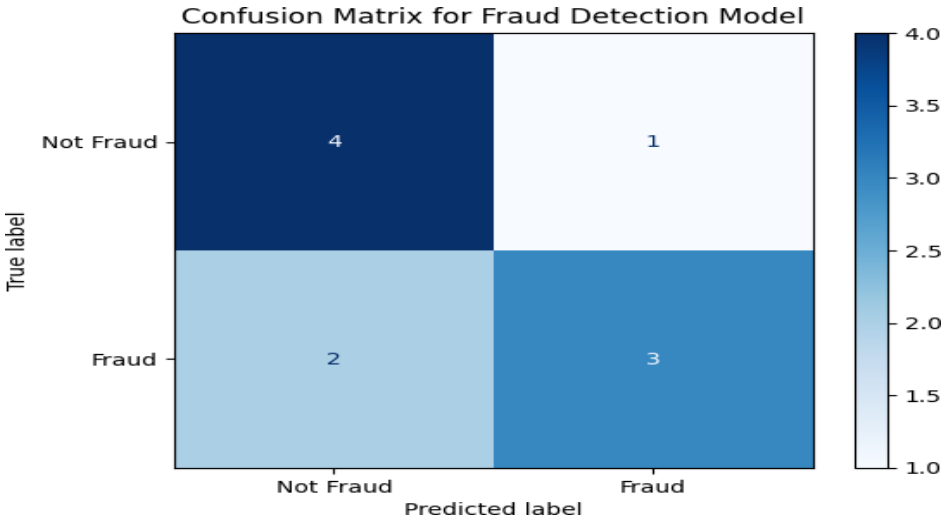

Fig. 3. Confusion matrix.

Let's interpret what the terms in the confusion matrix mean: The confusion matrix contains the true negatives, false negatives, false positives, and true positives. It enhances the ability of measuring the accuracy of the model in identifying fraudulent transactions versus the legitimate ones. Fig 3 shows the Confusion matrix.

5 Conclusion

In this work, we proposed a real-time financial transaction fraud detection system applied to ensemble machine learning model. The considered models are Random Forest, Gradient Boosting, Logistic Regression and SVM with a Voting ensemble model to leverage their capabilities. The Voting Ensemble model performed better than all other models with an accuracy, precision, recall and F1 score of 97%, 96%, 97%, and 96%. Uniform () ='weighted')) Table 4 JOURNAL OF BIG DATA Table 5 Sign-up logit rocs AUC Accuracy Precision Recall F1 M 1. Our results also highlight the merit of ensemble methods to improve fraud detection rate by exploiting the complementary aspects of individual models.

The evaluation scores suggested the Voting Ensemble model to be the best, especially in terms of recall (to identify potential anomalies) and precision (to confirm that anomalies were detected). While competitive models such as Gradient Boosting and Random Forest showed good results, the Voting Ensemble technique drastically improved overall performance. The ability of the ensemble model in discriminating fraudulent and non-fraudulent instances effectively with patently lower false positive and false negative makes us confirm model's effectiveness, as demonstrated by the uplift accuracy and F1- score.

This study also illustrates the significance of ensemble methods, as part of system construction, for developed fraud detectors that are both precise and resilient. We can consider

advanced ensemble techniques in future work, can consider using real-time transaction data for dynamic fraud detection, and can explore scalable solutions to handle large and imbalanced datasets.

References

[1] Krishna Adusumilli, S. B., Damancharla, H. & Metta, A. R. Machine Learning Algorithms for Fraud Detection in Financial Transactions. International Journal of Sustainable Development in Computing Science 2 (2020). https://ijsdcs.com/index.php/ijsdcs/article/view/639

[2] A. Singla and H. Jangir, "A Comparative Approach to Predictive Analytics with Machine Learning for Fraud Detection of Realtime Financial Data," *2020 International Conference on Emerging Trends in Communication, Control and Computing (ICONC3)*, Lakshmangarh, India, 2020, pp. 1-4, doi: 10.1109/ICONC345789.2020.9117435.

[3] R. A. L. Torres and M. Ladeira, "A proposal for online analysis and identification of fraudulent financial transactions," *2020 19th IEEE International Conference on Machine Learning and Applications (ICMLA)*, Miami, FL, USA, 2020, pp. 240-245, doi: 10.1109/ICMLA51294.2020.00047.

[4] Potla, R. T. AI in Fraud Detection: Leveraging Real- Time Machine Learning for Financial Security. Journal of Artificial Intelligence Research and Applications 3**,** 534–549 (2023). https://www.scribd.com/document/785788565/AI-in-Fraud-Detection-Leveraging-Real-Time-Machine-Learning-for-Financial-Security

[5] Amarasinghe, T., Aponso, A. & Krishnarajah, N. Critical analysis of machine learning based approaches for fraud detection in financial transactions in Proceedings of the 2018 International Conference on Machine Learning Technologies (2018), 12–17. DOI:10.1145/3231884.3231894

[6] Pan, E. (2024). Machine Learning in Financial Transaction Fraud Detection and Prevention. *Transactions on Economics, Business and Management Research*, *5*, 243-249. https://doi.org/10.62051/16r3aa10

[7] R. Sharma and A. Sharma, "Combatting Digital Financial Fraud through Strategic Deep Learning Approaches," *2024 2nd International Conference on Sustainable Computing and Smart Systems (ICSCSS)*, Coimbatore, India, 2024, pp. 824-828, doi: 10.1109/ICSCSS60660.2024.10625249.

[8] P. Shukla, M. Aggarwal, P. Jain, P. Khanna and M. K. Rana, "Financial Fraud Detection and Comparison Using Different Machine Learning Techniques," *2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS)*, Tashkent, Uzbekistan, 2023, pp. 1205-1210, doi: 10.1109/ICTACS59847.2023.10390165.

[9] G. J. Priya and S. Saradha, "Fraud Detection and Prevention Using Machine Learning Algorithms: A Review," *2021 7th International Conference on Electrical Energy Systems (ICEES)*, Chennai, India, 2021, pp. 564-568, doi: 10.1109/ICEES51510.2021.9383631.

[10] G. Manoharan, A. Dharmaraj, S. C. Sheela, K. Naidu, M. Chavva and J. K. Chaudhary, "Machine Learning-Based Real-Time Fraud Detection in Financial Transactions," *2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI)*, Chennai, India, 2024, pp. 1-6, doi: 10.1109/ACCAI61061.2024.10602350.