iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IX **Month of publication:** September 2025

DOI: https://doi.org/10.22214/ijraset.2025.74062

Enhancing Bank Fraud Detection: A Comparative Analysis of using Machine Learning Techniques

Mr. Basavaraj T[1], Dr. Girish Kumar D[2]
[1]Professor & HOD, Department of MCA, Ballari Institute of Technology & Management, Ballari, Karnataka, India
[2]Department of MCA, Ballari Institute of Technology & Management, Ballari, Karnataka, India

***Abstract:** This study focuses based on machine learning approaches to detect fraudulent activities in banking data — a major concern in the financial sector where preventing fraud is critical. To improve detection accuracy, the research introduces class weight tuning, a strategy that strengthens machine learning models distinguish between genuine and fraudulent transactions. The study uses three powerful machine learning algorithms — CatBoost, LightGBM, and XGBoost each known for its strengths in handling complex datasets. By combining these models, the system aims to improve overall performance in identifying fraud.*

Alongside, integration of deep learning techniques is carried out to fine-tune the model's hyperparameters, increasing its adaptability and effectiveness in recognizing evolving fraud patterns. The models are evaluated using real- world banking data, and the results show that combining LightGBM and XGBoost outperforms traditional approaches across various performance metrics. To further boost accuracy, a stacking ensemble model is implemented. It combines predictions from RandomForest and LightGBM classifiers and uses a GradientBoostingClassifier as the final estimator. This ensemble approach leverages the synergy of multiple models to make more accurate predictions.

***Keywords:** Bayesian optimization, data mining, deep learning, ensemble learning, hyperparameter tuning, imbalanced data, machine learning.*

I. INTRODUCTION

In recent years, the volume of financial transactions has surged, driven by the expansion of financial institutions and the growing popularity of online commerce. Consequently, this surge has caused a rise in fraudulent activities, especially in online banking, where fraud detection remains a persistent and complex challenge [1], [2].

As credit card usage continues to evolve, so do the tactics used by fraudsters. They constantly adapt their methods to make fraudulent transactions appear legitimate. By studying how fraud detection systems work, fraudsters try to exploit weaknesses and bypass protections — posing growing challenges in identify fraudulent activity. As a consequence, researchers are continually designing new techniques and improving existing models to keep up with these evolving threats [3].

Fraudsters often take advantage of vulnerabilities in the security, control, and monitoring systems of commercial applications. However, the same advancements in technology can also be leveraged to fight fraud [4]. Early detection — identifying fraud immediately after it occurs — is essential to minimize financial damage [5].

Fraud is typically defined as intentional deception for personal or financial gain. Credit card fraud refers specifically to the unauthorized use of credit card details, either for in-person purchases or digital transactions. In online transactions, fraud can occur when cardholders share sensitive details — such as card numbers, expiry dates, and CVV codes — over websites or phone calls [6].

To mitigate fraud-related losses, two primary strategies are used: fraud prevention and detection. Fraud prevention focuses on stopping fraudulent activity before it happens, whereas fraud detection is applied during or after a fraudulent attempt [7].In banking, fraud detection is usually treated as a binary classification problem, where transactions are categorized as either legitimate or fraudulent [8]. Given the massive scale of banking data and the complexity of patterns in fraudulent behavior, manually reviewing transactions is not only time-consuming but also inefficient. Machine learning (ML) algorithms are well-suited for this task, as they are capable of handling large datasets and uncover hidden patterns quickly and accurately [9].

The synergy between machine learning and high-performance computing has significantly improved the ability to detect fraud in real time [15]. Moreover, deep learning techniques offer fast and scalable solutions for dynamic fraud scenarios [10].

In this study, we propose a robust strategy for identifying credit card fraud, tested on publicly available datasets. The approach utilizes optimized versions of advanced algorithms such as LightGBM, XGBoost, CatBoost, and Logistic Regression — both individually and through ensemble techniques like majority voting. We also incorporate deep learning models and fine- tuned hyperparameters to enhance performance.

A robust fraud detection the system should go beyond merely identifying a higher instances of fraudulent cases but also ensure high precision — reducing false positives and false negatives. This accuracy builds trust with customers and helps financial institutions avoid potential losses caused by incorrect classifications.

II. LITERATURE SURVEY

A major challenge in preventing fraud in e-commerce transactions is the dynamic and diverse nature of fraud patterns [1]. To tackle this issue, researchers have introduced two innovative methods: Fraud Islands (based on link analysis) and a multi-layer machine learning model [10, 15, 20]. Fraud Islands use link analysis to uncover hidden relationships between fraudulent entities, forming a network that reveals complex fraud patterns. Meanwhile, the multi-layer model is designed to handle the wide variety of fraud behaviors by integrating multiple detection strategies.

Fraud labels are generally drawn from multiple sources, such as banks' decline decisions, manual review rejections, fraud alerts, and chargeback requests from customers. Each of these sources captures different types of fraud, which suggests that combining multiple detection methods could provide better coverage of fraud patterns. Experiments have shown that integrating various machine learning models—each trained on different types of fraud labels—can significantly improve the reliability of fraud detection systems [10].

In the healthcare domain, fraud detection has evolved to be increasingly critical due to the surge in government and private health insurance schemes. Fraudulent billing has become a widespread issue [9]. Detecting fraud in healthcare is particularly challenging because of the complex relationships between doctors, patients, and services. To improve transparency and reduce abuse in health support programs, intelligent fraud detection systems are essential.

One approach proposes a process-based fraud detection methodology that leverages sequence mining techniques to identify fraudulent insurance claims. In contrast to traditional models that emphasize only on the value of claims or disease-medication pairings, this method analyses sequences of services provided within each medical specialty. Frequent service patterns are extracted, and confidence values are calculated to establish typical behavior. These are validated with real patient service sequences. Any significant deviation is flagged as potentially fraudulent. The model was tested using five years of transactional samples obtained from a local hospital, which included numerous known cases of fraud [2, 7, 9].

In the financial sector, the rapid growth of credit card spending has been accompanied by a surge in fraudulent transactions. Despite the growing threat, the proportion of fraudulent transactions remains much smaller than legitimate ones, creating a significant class imbalance problem. This imbalance makes credit card fraud detection particularly challenging [3]. Boosting algorithms have shown promise in addressing this issue, and several studies have compared the accuracy of various boosting techniques to pinpoint the most effective ones [29, 30].

The rise of e-commerce and online payments has made credit card fraud a global concern. Many researchers have turned to machine learning as a data-driven solution. However, several challenges persist, including restricted access to public datasets, extreme class imbalance, and constantly evolving fraud tactics [5]. One investigation assessed the performance of Random Forest, Support Vector Machine (SVM), and Logistic Regression was compared using real- life transaction data. To tackle the imbalance, SMOTE (Synthetic Minority Oversampling Technique) was applied. The study also employed incremental learning to adapt to changing fraud patterns. Precision and recall were used to assess the model's performance.

The importance of employing hybrid machine learning models in detecting credit card fraud is underlined in another study [10, 15, 20]. Initially, standard models are tested on a publicly available dataset. Then, AdaBoost and Majority voting approaches are employed to improve performance. To test robustness, noise is intentionally added to the dataset. Findings reveal that majority voting consistently delivers higher accuracy in fraud detection [6].

In the context of healthcare fraud, which is a costly white-collar crime in the United States, the consequences are not just financial—patients may suffer harm, and everyone bears the cost through higher premiums [2, 7]. Given the diversity of healthcare systems and data formats, developing digital fraud detection systems is complex. The ultimate goal is to generate actionable leads that can be further investigated for potential recovery or legal action.

Recent literature in this domain reviews various detection techniques and provides a comprehensive summary of peer-reviewed research articles. These include study objectives, conclusions, and characteristics of the datasets used. The review also identifies current gaps in real-world implementation of fraud detection systems. To advance this field, the authors propose avenues for further investigation [7].

III. METHODOLOGY

A. *Proposed Work: Methodology*

This project presents an advanced fraud detection system tailored for banking and credit card transaction data. It leverages powerful machine learning techniques, with performance enhancements achieved through class weight tuning and Bayesian optimization. The core algorithms used in the system include CatBoost, LightGBM, and XGBoost [29, 30, 31, 32], each chosen for their capability to manage structured data with accuracy and class imbalance.To further improve model accuracy and versatility, deep learning models are applied for fine-tuning. Real- world training relies on transaction datasets and evaluation, ensuring the system performs well under realistic conditions. Comprehensive performance evaluation is conducted using standard classification metrics.

One of the core features of the system is the use of a stacking ensemble model. This model combines the predictions of multiple base learners— specifically, RandomForest and LightGBM [17, 28] — and uses a GradientBoostingClassifier as the final estimator. This ensemble approach harnesses the strengths of diverse models to deliver improved fraud detection accuracy.For practical deployment and ease of use, a user- friendly web application is developed using the Flask framework with SQLite as the backend database. The application includes secure signup and login functionality, making it suitable for user testing and demonstrating real-world applicability. This integration ensures both accessibility and practicality for fraud detection in operational environments.

B. *System Architecture*

The system begins by collecting raw credit card usage data, which includes various features along with markers denoting if each transaction is fraudulent or legitimate. This data undergoes a preprocessing phase involving feature extraction and selection to make it suitable for machine learning. Once prepared, the dataset is split into training and evaluation sets subsets to enable model development and performance evaluation. To boost the model’s effectiveness, Bayesian optimization is used to fine-tune the hyperparameters of the applied machine learning algorithms. Advanced models such as CatBoost, LightGBM, and XGBoost are employed, with 5- fold cross-validation ensuring robustness and minimizing overfitting. Additionally, a stacking classifier has been implemented as an extension to the project, combining the outputs of multiple models to further improve prediction accuracy. The system performance is analyzed based measured on several performance indicators— accuracy, precision, recall, and F1-score— with the goal of achieving reliable fraud detection and minimizing false positives.

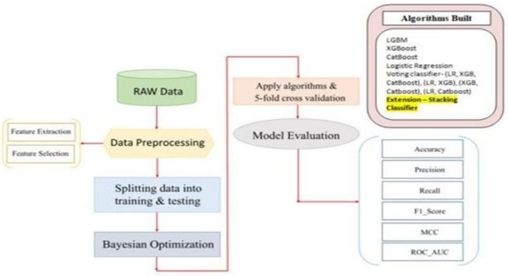

Algorithms Built
LGBM
XGBoost
CatBoost
Logistic Regression
Voting classifier- (LR, XGB, CatBoost), (LR, XGB), (XGB, Catboost), (LR, Catboost)
Extension – Stacking Classifier
RAW Data
Apply algorithms & 5-fold cross validation
Feature Extraction
Feature Selection
Data Preprocessing
Model Evaluation
Accuracy
Precision
Recall
F1_Score
MCC
ROC_AUC
Splitting data into training & testing
Bayesian Optimization

Fig 1 Proposed architecture

C. *Dataset Collection*

We utilized the Bank Transactions Fraud Detection dataset from Kaggle to train and evaluate our machine learning models. This dataset contains transaction-level data with features such as "Amount", "Time", and anonymized variables labeled "V1" to "V28". The anonymization of these features ensures user privacy and data security, as the original attributes have been transformed for confidentiality purposes. Despite this, the dataset remains highly effective for training fraud detection models.

D. *Data Processing*

The handling of data is fundamental to converting raw data into insightful and useful actionable insights. This process generally includes steps such as data collection, organization, cleaning, validation, analysis, and formatting into readable outputs like charts, graphs, or reports. These tasks are commonly executed by data scientists to ensure the data is accurate, consistent, and ready for analysis.

There are three essential types of data processing methods: manual, mechanical, and electronic. Among these, electronic or automated processing—often powered by computer software—is the most efficient and widely used in modern applications.

The main objective of data processing is to enhance the value of the data and support informed decision-making. In business contexts, this helps organizations improve operational efficiency and make timely, strategic decisions. Particularly when handling large datasets, including big data, automated tools can detect valuable patterns and insights that are fundamental to quality control and effective management.

E. Feature Selection

Feature selection involves recognizing and selecting the most relevant, consistent, and non- redundant features for building a predictive model. As datasets grow in size and complexity, reducing the number of input variables becomes essential to boost model efficiency and accuracy.A key part of feature engineering, feature selection helps filter out redundant or duplicate features, focusing only on the attributes that contribute significantly to the model’s performance. This improves accuracy while also reduces computational cost and training time. By applying feature selection before model training, we ensure the algorithm works with the most informative data, rather than relying on the model to determine feature importance during training. This proactive approach helps streamline the learning process and often results in better overall outcomes.

F. Algorithms

1) LGBM (Light Gradient Boosting Mac hine): LGBM is a powerfull and efficient gradient boosting algorithm built to manage massive datasets with high performance. It is well-known for its speed and accuracy, making it serves as a preferred choice for applications like fraud detection. LGBM works by building an set of decision trees and optimizing the boosting process to achieve faster training and better predictive results [28].

2) XGBoost (Extreme Gradient Boosting): XGBoost is a widely used and highly effective gradient boosting technique noted for its strong performance and reliability across an array of machine learning tasks. It uses a regularized boosting technique, which helps reduce overfitting and improves generalization. XGBoost is particularly valuable in processing imbalanced datasets—making t serves as an essential tool for detecting fraudulent transactions in financial data.

3) CatBoost (Categorical Boosting): CatBoost is a powerful gradient boosting algorithm tailored for datasets with categorical features. Unlike many other models, it automatically processes categorical data, reducing the need for manual encoding. It’s highly robust, offers strong resistance to overfitting, and delivers reliable performance—especially when working with complex real-world banking data such as in fraud detection.

4) Logistic Regression: Logistic Regression is a straightforward and widely used algorithm for solving binary classification problems. While it may not match the sophistication of advanced ensemble models, it plays a valuable role as a benchmark in fraud detection systems. Its simplicity ensures easy implementation and interpretability, and It offers detailed insights into the significance of individual features in identifying fraudulent transactions.

5) Stacking Classifier: As an extension of our model, we implemented a Stacking Classifier—an advanced ensemble technique that combines the predictions of multiple base models. In our setup, RandomForest and LightGBM serve as the base classifiers, while a GradientBoostingClassifier acts as the final estimator. This layered approach leverages the strengths of each model to improve overall prediction accuracy and robustness in fraud detection.

IV. EXPERIMENTAL RESULTS

1) Precision: Precision evaluates the fraction of correctly classified instances or samples among the ones classified as positives. Thus, the procedure to compute the precision is given by:

Precision = True positives/ (True positives + False positives) = TP/(TP + FP)

$$\text{Precision} = \frac{\mathit{True\ Positive}}{\mathit{True\ Positive} + \mathit{False\ Positive}}$$

2) Recall: Recall is a performance metric in machine learning that evaluates how well a model identifies all actual positive instances. It is calculated as the ratio of correctly predicted positive cases to the total number of actual positives. Essentially, recall reflects the The model’s capacity to encompass all pertinent cases within a specific class.

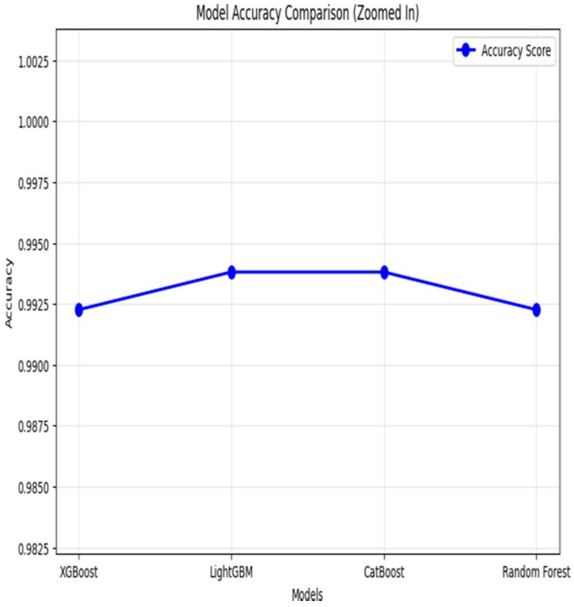
$$\mathbf{\mathit{Recall}} = \frac{\mathbf{\mathit{TP}}}{\mathbf{\mathit{TP}} + \mathbf{\mathit{FN}}}$$

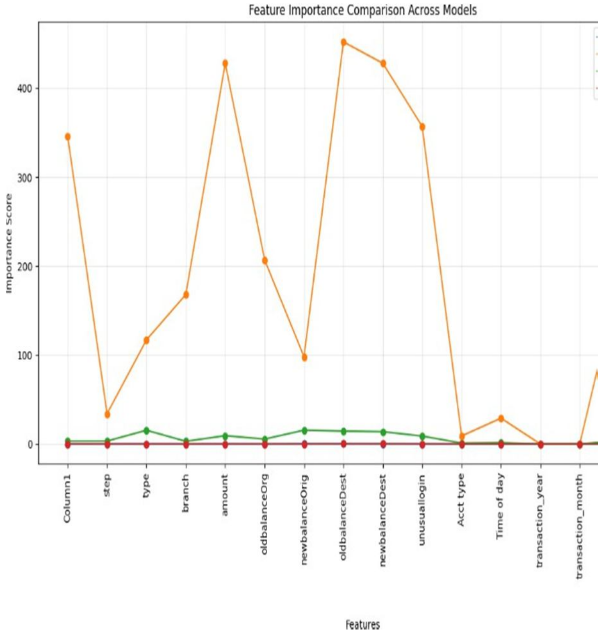
3) Accuracy: Accuracy is The extent of correct predictions in a classification task, measuring The general reliability of a model's predictions.

$$Accuracy = \frac{TP+TN}{TP+FP+TN+FN}$$

4) F1 Score: By combining precision and recall into a harmonic mean, the F1 Score offers a balanced evaluation that effectively handles both false positives and false negatives, making it ideal for imbalanced datasets.

$$\text{F1 Score} = 2 * \frac{\text{Recall} \times \text{Precision}}{\text{Recall} + \text{Precision}} * 100$$





V. CONCLUSION

The Stacking Classifier emerged as the top-performing model, delivering the highest accuracy among all evaluated algorithms, thereby showcasing its exceptional effectiveness in fraud detection. This project demonstrated strong performance across various machine learning models—including LightGBM, XGBoost, CatBoost [29, 30, 31, 32], voting classifiers, and neural networks—underscoring the system's adaptability and robustness. The incorporation of diverse Data extraction and adjustment techniques Was essential for in enhancing detection accuracy, highlighting their significance in model optimization.

The usage of the ensemble-based Stacking Classifier further boosted performance, clearly establishing its value in tackling fraud-related challenges. Additionally, the development of a user-friendly Flask-based web interface simplified user testing and authentication processes, enhancing accessibility and real-world usability. Successful implementation and testing through Flask, with interactive inputs, confirmed the practicality and reliability of the system [1, 2, 3].

Overall, the project underscores the potential of advanced machine learning approaches in addressing complex fraud detection issues within the banking domain. It sets the stage for continued enhancements through further exploration of ensemble methods and hyperparameter optimization strategies. Ultimately, these advancements contribute to reducing financial losses, improving transaction security, and building trust within the financial ecosystem.

VI. FUTURE SCOPE

Future research will focus on enhancing fraud detection accuracy and resilience by integrating additional hybrid models with CatBoost [29]. A key objective will be to fine-tune CatBoost's hyperparameters, especially by optimizing The quantity of decision trees employed to enhance the model efficiency and performance [33]. The research will also explore adaptive strategies to keep pace with evolving fraud patterns, ensuring the model continues to accurately detect emerging fraudulent behaviors. Additionally, upcoming work aims to incorporate real-time data streams to improve the system's responsiveness and adaptability, allowing for faster and more proactive detection of threats. Efforts will also be directed toward enhancing the interpretability of the model's decision-making process, offering clearer insights into how predictions are made. This transparency will help build user trust and support the development of more effective fraud detection strategies in the future.

REFERENCES

[1] J. Nanduri et al., "Ecommerce fraud detection through fraud islands and multi-layer machine learning model," in Advances in Information and Communication, Springer, 2020, pp. 556–570.

[2] I. Matloob et al., "A sequence mining-based novel architecture for detecting fraudulent transactions in healthcare systems," IEEE Access, vol. 10, pp. 48447–48463, 2022.

[3] H. Feng, "Ensemble-based methods in credit card fraud detection using boosting methods," in Proc. 2nd Int. Conf. Comput. Data Sci. (CDS), 2021, pp. 7–11.

[4] M. S. Delgosha et al., "Elucidation of big data analytics in banking: A four-stage Delphi study,"
a. J. Enterprise Inf. Manage., vol. 34, no. 6, pp. 1577– 1596, Nov. 2021.

[5] M. Puh and L. Brkić, "Detecting credit card fraud using selected machine learning algorithms," in Proc. 42nd MIPRO, 2019, pp. 1250–1255.

[6] K. Randhawa et al., "Detection of credit card fraud using AdaBoost and majority voting," IEEE Access, vol. 6, pp. 14277–14284, 2018.

[7] N. Kumaraswamy et al., "Healthcare fraud data mining methods: A retrospective and future perspective," Perspectives in Health Information Management, vol. 19, no. 1, p. 1, 2022.

[8] E. F. Malik et al., "A novel hybrid machine learning architecture in detecting credit card fraud," Mathematics, vol. 10, no. 9, p. 1480, Apr.

[9] 2022.

[10] K. Gupta et al., "A review on machine learning- based credit card fraud detection," in Proc. Int. Conf. on Advancements in Automation and Intelligent Computing (ICAAIC), 2022, pp. 362–

[11] 368.

[12] R. Almutairi et al., "Credit card fraud detection using machine learning models: An analytical study," in Proc. IEEE Int. Conf. on Internet of Everything, Microwave, and Electronics Engineering (IEMTRONICS), Jun. 2022, pp. 1–8.

[13] N. S. Halvaiee and M. K. Akbari, "A novel approach to credit card fraud detection using artificial immune systems," Applied Soft Computing, vol. 24, pp. 40–49, Nov. 2014.

[14] A. C. Bahnsen, D. Aouada, A. Stojanovic, and B. Ottersten, "Feature engineering strategies for credit card fraud detection," Expert Systems with Applications, vol. 51, pp. 134–142, Jun. 2016

[15] U. Porwal and S. Mukund, "Outlier detection approach for credit card fraud detection in e- commerce," arXiv preprint arXiv:1811.02196, 2018.

[16] H. Wang et al., "An ensemble learning framework for credit card fraud detection," in Proc. IEEE SmartWorld Conf., Oct. 2018, pp. 94–98.

[17] F. Itoo et al., "Comparative study of logistic regression, Naïve Bayes, and KNN for credit card fraud detection," International Journal of Information Technology, vol. 13, no. 4, pp. 1503–

[18] 1511, 2021.

[19] T. A. Olowookere and O. S. Adewale, "Cost- sensitive meta-learning framework for credit card fraud detection," Scientific African, vol. 8, art. no. e00464, Jul. 2020.

[20] A. A. Taha and S. J. Malebary, "Optimized LightGBM-based intelligent approach for credit card fraud detection," IEEE Access, vol. 8, pp. 25579–25587, 2020.

[21] X. Kewei et al., “Hybrid deep learning model for online fraud detection,” in Proc. Int. Conf. on Computing, Electronics, and Communications Engineering (ICCECE), Jan. 2021, pp. 431–434.

[22] T. Vairam et al., “Evaluation of Naïve Bayes and voting classifier strategies for detecting credit card fraud,” in Proc. Int. Conf. on Advanced Computing and Communication Systems (ICACCS), Mar. 2022, pp. 602–608.

[23] P. Verma and P. Tyagi, “Analysis of supervised machine learning algorithms in fraud detection,” ECS Transactions, vol. 107, no. 1, p. 7189, 2022