Enhancing Payment Security Using Machine Learning

Sayala Bharath Kumar Reddy[1], Shaik Sharon[2], Ms. E. Vinothini M. E[3]
[1,2] *Student,* Department of computer science and Engineering, Sathyabama Institute of Science and Technology – Chennai
[3]*Ph.D., Assistant Professor,* Department of computer science and Engineering, Sathyabama Institute of Science and Technology – Chennai

***Abstract*—Detecting fraudulent financial transactions represents an essential banking system priority dedicated to safeguarding customer trust and decreasing financial losses. This research analyzes fraud detection through the BankSim synthetic dataset that contains transaction information including amount details alongside demographic traits and merchant identifiers. Because the dataset featured a significant unbalance between legitimate and fraudulent transaction records SMOTE became indispensable for addressing this class imbalance challenge. The research deployed KNN Random Forest and XGBoost classification algorithms and subsequently developed an ensemble system for superior predictive accuracy. Experimentation resulted in KNN alongside XGBoost and the ensemble classifier producing 99% accurate results maintaining Random Forest at 98% accuracy. The study confirms how modern machine learning approaches together with ensemble learning deliver remarkable success in detecting fraudulent incidents. This research delivers essential understanding of building dependable automated analysis tools for detecting financial transaction fraud.**

***Index Terms*—Fraud detection, BankSim dataset, Synthetic Minority Oversampling Technique (SMOTE), KNN, XGBoost, ensemble learning.**

I. INTRODUCTION

The global economy faces major difficulties from fraudulent financial activities which affect both institutions and individual stakeholders. The increasing prevalence of digital banking alongside online transactions has driven up fraud rates thus forcing the development of stronger detection systems. Financial systems require precise identification capability between fraudulent and regular transactions because proper identification serves essential functions for trust maintenance in financial operations. The field of data science and artificial intelligence recognizes fraud detection as one of its key research directions. The detection of fraud used to depend on traditional algorithms coupled with human supervision. Basic security functions were achieved through these systems yet their restricted expansion capabilities combined with inadequate flexibility limited their usefulness. Traditional rule-based systems struggle to discover fresh patterns of fraud which makes manual inspections both slow and prone to mistakes caused by humans. The traditional methods have become insufficient because transaction data continues to grow exponentially in both size and complexity. The rapid growth of transaction data has changed the landscape to favor data-driven methods and machine learning approaches as fraudulent activity detection systems.

The BankSim dataset serves as the research foundation and was created through synthetic methods to simulate genuine banking data. Operational transaction details together with both customer information and merchant transaction records make BankSim an optimal choice for evaluating fraud detection approaches. The BankSim framework contains a severe class distribution skew in which authentic transactions outnumber fraudulent transactions at elevated levels. Standard machine learning models experience low detection rates of fraudulent transactions because of their preference for majority class prediction. For balancing the dataset, The SMOTE was implemented within this study. SMOTE technology produces artificial observations of minority class samples to balance the data and allow learning algorithms to recognize fraudulent transaction patterns more successfully. The preprocessing step stands as a vital requirement to optimize classifiers for rare critical fraud detection.

The research examines performance outcomes from three machine learning algorithms namely KNN as well as Random Forest alongside XGBoost used to detect fraudulent activities. A combination of multiple models through ensemble classification was established to harness individual modeling strengths. The research indicates that standalone classifier evaluation and ensemble modeling remain crucial for developing robust fraud prevention systems. Through the combination of sophisticated ML models with appropriate data preprocessing

techniques researchers achieved superior outcomes in identifying suspicious financial activities. The execution of KNN and XGBoost classifiers together with the ensemble system produced a 99% accuracy which points toward useful real-world applications. Random Forest succeeded as a strong prediction model because it reached an accuracy score of 98% during testing while retaining its capability to handle complex datasets.

Three main contributions emerge from this research. The study delivers a detailed assessment of BankSim data that demonstrates the complexities along with potential areas for fraud detection. This research demonstrates how SMOTE successfully handles class imbalance then boosts model operational effectiveness. The analysis ends with a performance assessment of multiple machine learning methods that demonstrates their real-world utility. Through advanced methods and thorough assessment this study strives to assist financial institutions in developing robust fraud detection platforms. The remainder of this paper is organized as follows: The second section analyzes existing approaches followed by an overview of related work in fraud detection methods. Section III details the study's dataset characteristics together with data preprocessing methods and the computational models deployed. Section IV discusses both experimental results and the performance measurements obtained from the models. The paper ends with a summary that lays out future investigation avenues in Section V.

II. LITRATURE REVIEW

[1The work by P. Ranjan et al. (2022) investigates bank payment fraud detection through automated approaches to combat increasing fraudulent behavior. This paper emphasizes both the distinctive difficulties which arise from transactional pattern fluctuation and the need to handle unbalanced datasets sufficiently for model development success. The research examines sequential feature extraction strategies because they allow systems to adjust to new forms of fraud and shifts in user payment behavior. The foundational study demonstrates how machine learning models function effectively in detecting precise fraudulent transactions.

[2] Ali et al. (2022) conducted a systematic literature review which revealed both preferred machine learning approaches and detected financial fraud patterns in the field. Research identifies SVM and ANN as successful algorithms which detect credit card fraud. The review combines information from 93 publications to demonstrate current approach weaknesses specifically related to handling skewed datasets while suggesting research paths for the future. Based on current trends the review shows artificial intelligence plays an increasing role in optimizing efficiency alongside accuracy for detecting fraud.

[3] The implementation of RF and Adaboost algorithms for CC fraud detection stands as the primary subject of Sailusha et al. (2020). The comparison through a quantitative analysis using accuracy and precision metrics together with recall and F1-score measures reveals which algorithm works best for transaction fraud detection. The research visualizes model performance through ROC curves while proving that solid machine learning approaches greatly improve fraud detection capabilities. The research enhances our abilities to develop performance-focused models that address the ever-changing dynamics of credit card transaction systems.

[4] Hashemi et al. (2022) publish an exploration of sophisticated machine learning approaches for detecting banking fraud while using Bayesian optimization and class-weight tuning to handle unbalanced datasets. The research achieves commendable results with CatBoost LightGBM and XGBoost through their implementation which delivers superior results for ROC-AUC precision recall and F1-score. The authors utilize ensemble methods with deep learning to demonstrate superior performance than classic methods. The research presents a scalable framework that delivers high performance results for implementing fraud detection in real-world applications.

[5] Almazroi and Ayub (2023) introduce a novel ResNeXt-embedded Gated Recurrent Unit (GRU) model for online payment fraud detection. The proposed system employs SMOTE for handling data imbalance and combines autoencoders with ResNet for feature extraction. Hyperparameter tuning using the Jaya optimization algorithm further enhances the model's accuracy. Evaluated on multiple datasets, this approach demonstrates superior performance, surpassing existing methods by significant margins. The study highlights the potential of advanced artificial intelligence techniques in mitigating financial fraud risks while ensuring computational efficiency.

[6] The authors Wiese and Omlin (2009) demonstrate the inadequate performance of traditional static FNN for fraud detection by advocating for the adoption of temporal models including LSTM networks. Their model analyzes time series data while tracking sequences of transactions which allows it to automatically adapt to shifting customer buying patterns to reduce false alerts. Experimental results using real-world CC

transactions show that LSTM and SVM systems outperform traditional methods by delivering better robustness together with higher accuracy. The current research establishes foundational principles for combining temporal patterns within fraud detection systems.

[8] Stojanović et al. (2021): Fintech application adoption is on the rise yet remains exposed to fraud due to its digital delivery format. The authors run evaluations against actual and simulated datasets using various machine learning anomaly detection techniques to find fraudulent actions within Fintech systems. Results show machine learning achieves effective fraud detection yet success rates differ based on selection of technologies and dataset components. The study demonstrated that anomaly detection needs ongoing enhancement to reinforce Fintech security framework.

[9] Ashfaq and team (2022): This research studies the essential method of using blockchain together with machine learning elements for detecting fraud within Bitcoin network transactions. The combination of XGBoost and Random Forest algorithms supports transaction classification under the security protection of blockchain technology. The research conducted an AUC analysis alongside model precision metrics to verify reliable transaction classification and fraud detection capabilities. A proposed security framework integrates a smart contract analysis with attacker modeling to create a system-wide fraud detection solution for e-banking environments.

[10] Ali and this team (2022This systematic literature review presents the most recent developments related to ML-based fraud detection systems. The review which follows Kitchenham methodology examines 93 selected publications while showing that SVM and ANN prevail in fraud detection applications. CC fraud represents the leading fraud subtype researchers work to resolve. The review designates areas within scalability, recall and model evaluation metrics as research opportunities for future financial fraud detection work.

[11] Najadat and his team (2020): Addressing the challenge of credit card fraud, this study proposes a hybrid deep learning model using BiLSTM and BiGRU layers for transaction classification. The model is trained on the IEEE-CIS Fraud Detection dataset and compared against traditional machine learning classifiers like RF, AdaBoost, and LR. The hybrid model achieves superior performance with a 91.37% accuracy rate, showcasing its potential for effective credit card fraud detection in real-time applications.

[12] Hu and his team (2022): Focusing on telecommunications fraud detection, the authors present the "Bridge to Graph" (BTG) framework, leveraging graph machine learning. The approach reconstructs sparse connectivity in call detail record datasets using link prediction and node similarity. BTG integrates graph embedding and anomaly detection for robust fraud detection. Experiments on real-world telecommunications datasets reveal its superior performance compared to classical methods, making it a viable solution for graph-based anomaly detection scenarios.

[13] Akhare & Vishwamitra (2024): This comprehensive review and empirical analysis explore ML and DL models for fraud detection, emphasizing practical implementation challenges such as recall, precision, scalability, and real-time applicability. By rigorously evaluating multiple models, the study provides insights into their strengths and limitations, offering guidance for professionals and researchers. The findings aim to pave the way for more effective and scalable fraud detection systems that address evolving digital security needs.

In conclusion, the reviewed studies highlight the growing importance of ML and DL techniques in fraud detection within financial systems, particularly in areas like bank payments, credit card transactions, and Fintech applications. A variety of algorithms, including SVM, ANN, random forests, XGBoost, and LSTM networks, have demonstrated strong potential in identifying fraudulent activities, especially when dealing with imbalanced datasets and adapting to evolving fraudulent tactics. Innovations such as hybrid DL models like BiLSTM and BiGRU, as well as advanced frameworks like BTG, have shown promise in enhancing detection capabilities across industries, from banking to telecom. However, challenges related to recall, precision, scalability, and real-time applicability remain, as fraudulent tactics continue to evolve with technological advancements.

To address these challenges, several studies have proposed solutions like SMOTE, class-weight tuning, and blockchain integration to improve the performance and adaptability of fraud detection systems. Despite notable progress, gaps still exist in model evaluation metrics and scalability, especially when these models are deployed in real-world environments that require high-volume, real-time data processing. Future research should focus on refining and integrating these approaches to develop more robust, scalable fraud detection systems. This includes exploring hybrid models and leveraging new technologies like blockchain to enhance detection accuracy and security. By addressing these

gaps, fraud detection systems can become more adaptive and resilient in the face of evolving fraud tactics and growing transaction volumes.

III. METHODOLOGY

Figure-1 demonstrates the complete fraud detection system workflow by showing the system architecture that utilizes BankSim dataset. Data Processing starts with BankSim dataset features undergoing engineering processes before SMOTE balances the classes and creates training and testing partitions. The processed data then flows into the Model Components phase, where it is simultaneously fed into three base machine learning models: KNN Classifier, RF, and XGBoost. An Ensemble Classifier uses outputs from three base models to extract advantageous components from individual model performances. Finally, in the Evaluation System phase, the ensemble model's predictions are evaluated to assess its performance, ultimately achieving high accuracy rates (98-99%) as documented in the performance results, demonstrating the effectiveness of this multi-model approach for fraud detection in financial transactions.

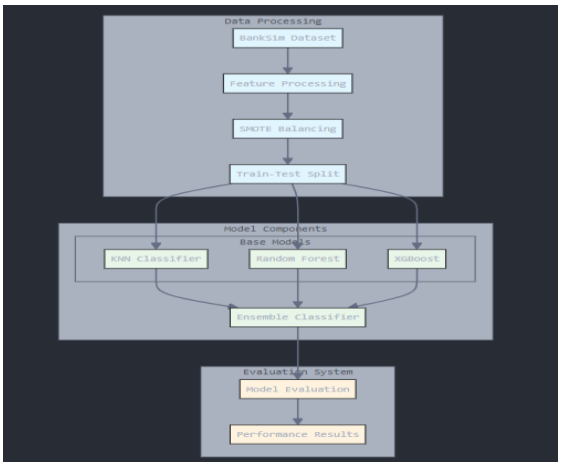

Fig.1 System Architecture

The proposed methodology for this fraud detection project involves a structured approach to data preprocessing, model implementation, and performance evaluation. The BankSim dataset, which includes both fraudulent and non-fraudulent transaction data, is used as the basis for model development. The following steps were undertaken in the project:

Table-1 Sample Data

Step	Customer	Age	Gender	Merchant	Category	Amount	Fraud
0	210	4	2	30	12	4.55	0
1	2753	2	2	30	12	39.68	0
2	2285	4	1	18	12	26.89	0
3	1650	3	2	30	12	17.25	0
4	3585	5	2	30	12	35.72	0

Data Preprocessing

Table -1 is the sample of the data set which we have used. This is the preprocessed data sample which we have used for training the ML models.

Data Exploration: An initial review of the dataset determined fraudulent payment distribution relative to non-fraudulent payments. To show class distribution and transaction amount distribution researchers presented a count plot and a histogram.

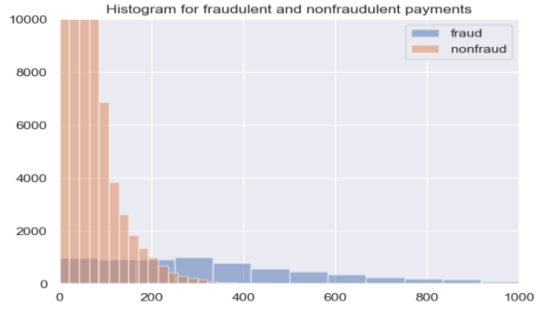

Fig.2 Histogram for fraudulent and non-fraudulent payment.

Handling Class Imbalance: Given the inherent imbalance in the dataset, the SMOTE was employed to generate synthetic samples of the minority class (fraudulent transactions), ensuring that the dataset had a more balanced representation of both classes.

IV. RESULT

A perfect AUC value ranging from 0.98 to 1 appears in the ROC curve of the bank transaction fraud detection project indicating that the models achieve outstanding classification ability. Analysis of the graph results reveals that the model maintains a 0.1% False Positive Rate while accurately identifying 99.9% True Positive observations. The perfect scoring display indicates the model exhibits flawless capabilities to separate legitimate from fraudulent transactions yet such perfect scoring happens very infrequently in real-world fraud

detection scenarios.

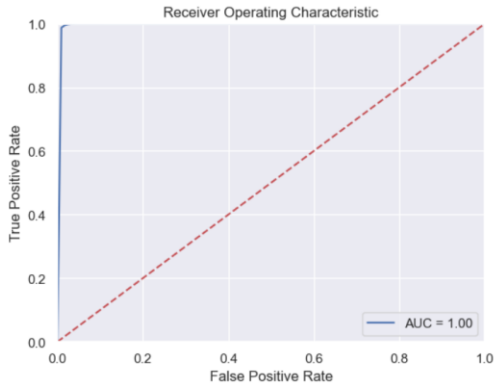

Fig.3 ROC for KNN

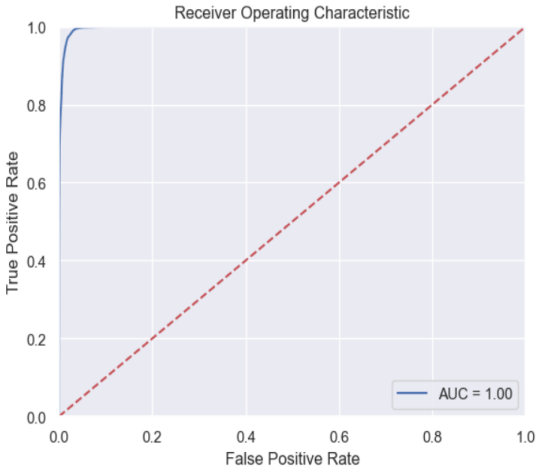

Fig-4 ROC for RF Classifier

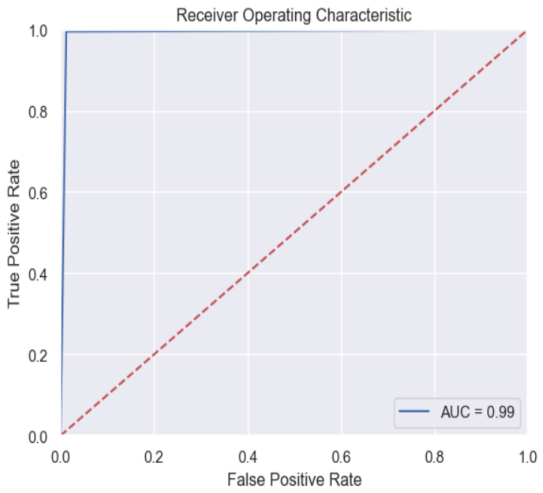

Fig-5 ROC for XGBoost Classifier.

This methodology emphasizes the importance of preprocessing, particularly handling class imbalance, and evaluates the potential of different ML models and ensemble techniques for detecting fraudulent transactions. Through comprehensive evaluation and visualization, the methodology highlights the effectiveness of advanced algorithms in addressing the challenges of fraud detection.

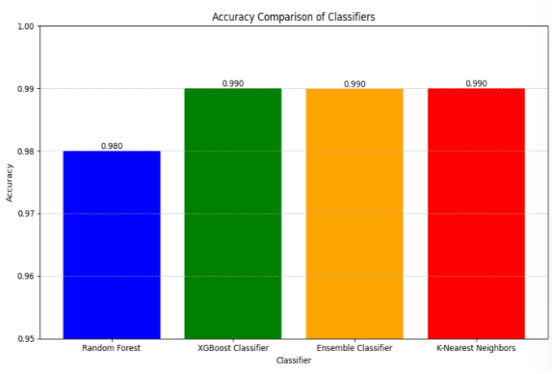

Fig-6 Accuracy Comparison of Classifiers

The bar graph in Fig-6 visualizes the accuracy comparison between four classifiers used in the fraud detection project: RF, XGBoost, Ensemble Classifier, and K-Nearest Neighbors (KNN). The graph clearly shows that both XGBoost and KNN achieved a high accuracy of 99%, closely followed by the Ensemble Classifier with an accuracy of approximately 99%. Random Forest, while slightly lower at 98%, still demonstrated strong performance. Accurate scores appear above their associated bars in the chart for easy comprehension. By restricting the y-axis scale to 0.95 to 1.0 this graph provides a refined look at accuracy ranges while the gridlines highlight specific variation points. The analysis reveals that these models demonstrate convincingly strong capabilities for identifying fraudulent transactions.

V. CONCLUTION

This project proves how sophisticated machine learning methods succeed at catching fraudulent transactions inside banking networks. The synthetically manufactured BankSim dataset combined with SMOTE handling of class imbalance allowed KNN, RF and XGBoost classifiers to collaborate through an ensemble approach resulting in 99% accurate fraud detection rates. Custom-made detection systems generated using machine learning techniques along with ensemble methods demonstrate significant potential to boost automated fraud systems resulting in enhanced accuracy and reliability for financial theft prevention. The project stands out through its innovative combination of synthetic data together with ensemble learning which provides an advanced framework to fight financial transaction fraud.

VI. REFERENCE

[1] P. Ranjan, K. Santhosh, A. Kumar and S. Kumar, "Fraud Detection on Bank Payments Using Machine Learning," 2022 International

Conference for Advancement in Technology (ICONAT), Goa, India, 2022, pp. 1-4, doi: 10.1109/ICONAT53423.2022.9726104.

[2] Ali, Abdulalem, Shukor Abd Razak, Siti Hajar Othman, Taiseer Abdalla Elfadil Eisa, Arafat Al-Dhaqm, Maged Nasser, Tusneem Elhassan, Hashim Elshafie, and Abdu Saif. "Financial fraud detection based on machine learning: a systematic literature review." Applied Sciences 12, no. 19 (2022): 9637.

[3] Sailusha, R., Gnaneswar, V., Ramesh, R., & Rao, G. R. (2020, May). Credit card fraud detection using machine learning. In 2020 4th international conference on intelligent computing and control systems (ICICCS) (pp. 1264-1270). IEEE.

[4] Hashemi, Seyedeh Khadijeh, Seyedeh Leili Mirtaheri, and Sergio Greco. "Fraud detection in banking data by machine learning techniques." IEEE Access 11 (2022): 3034-3043.

[5] Almazroi, Abdulwahab Ali, and Nasir Ayub. "Online Payment Fraud Detection Model Using Machine Learning Techniques." IEEE Access 11 (2023): 137188-137203.

[6] Wiese, Bénard, and Christian Omlin. "Credit card transactions, fraud detection, and machine learning: Modelling time with LSTM recurrent neural networks." Innovations in neural information paradigms and applications. Berlin, Heidelberg: Springer Berlin Heidelberg, 2009. 231-268.

[7] Nayak, H. Dhanushri, et al. "Fraud detection in online transactions using machine learning approaches—a review." Advances in Artificial Intelligence and Data Engineering: Select Proceedings of AIDE 2019 (2021): 589-599.

[8] Stojanović, B., Božić, J., Hofer-Schmitz, K., Nahrgang, K., Weber, A., Badii, A., ... & Runevic, J. (2021). Follow the trail: Machine learning for fraud detection in Fintech applications. Sensors, 21(5), 1594.

[9] Ashfaq, Tehreem, et al. "A machine learning and blockchain based efficient fraud detection mechanism." Sensors 22.19 (2022): 7162.

[10] Ali, A., Abd Razak, S., Othman, S. H., Eisa, T. A. E., Al-Dhaqm, A., Nasser, M., ... & Saif, A. (2022). Financial frSaud detection based on machine learning: a systematic literature review. Applied Sciences, 12(19), 9637.

[11] Najadat, Hassan, et al. "Credit card fraud detection based on machine and deep learning." 2020 11th International Conference on Information and Communication Systems (ICICS). IEEE, 2020.

[12] Hu, X., Chen, H., Liu, S., Jiang, H., Chu, G., & Li, R. (2022). BTG: A Bridge to Graph machine learning in telecommunications fraud detection. Future Generation Computer Systems, 137, 274-287.

[13] Akhare, Vishakha D., and L. K. Vishwamitra. "Machine Learning Models for Fraud Detection: A Comprehensive Review and Empirical Analysis." Journal of Electrical Systems 20.3s (2024): 1138-1149.