INTERNATIONAL SCIENTIFIC JOURNAL OF ENGINEERING AND MANAGEMENT (ISJEM) ISSN: 2583-6129
VOLUME: 04 ISSUE: 03 | MARCH – 2025 DOI: 10.55041/ISJEM02496
AN INTERNATIONAL SCHOLARLY || MULTIDISCIPLINARY || OPEN ACCESS || INDEXING IN ALL MAJOR DATABASE & METADATA

A Stacked LightGBM-XGBoost Model with SHAP-Based Fraud Detection for Financial Transactions

Aditi C Ramesh
dept. of Computer Science
Mount Carmel College
Bengaluru, India
M23CS01@mccblr.edu.in

Ms. Uma K
dept. of Computer Science
Mount Carmel College
Bengaluru, India
kuma@mccblr.edu.in

***Abstract*— Financial transaction fraud detection is a significant task that requires robust and efficient machine learning algorithms to be deployed. In this research, we proposed a hybrid model that uses Light Gradient Boosting Machine (LGBM) and Extreme Gradient Boosting (XGB) to enhance the accuracy of fraud detection. We employ diverse feature engineering techniques, preprocessing, and model performance measures to enhance the classification of fraudulent behaviour. The suggested model is trained on a transaction and identity data set, which performs better in terms of accuracy and Area Under the Curve (AUC) value. Additionally, the model is also tested using SHAP (Shapely Additive Explanations) values, which provide more precise insights into feature importance. We also highlight the importance of Artificial Intelligence (AI) integration through the application of gradient boosting algorithms to the enhancement of feature cybersecurity in fraud detection through improved predictive accuracy and reduced false positives.**

Keywords— AI enhancement, Fraud Detection, LightGBM, XGBoost, Machine Learning, Financial Security, Gradient Boosting, SHAP.

I. INTRODUCTION

Fraudulent behavior in financial transactions can create serious threats to individuals and organizations. Traditional rule-based systems used for fraud detection are inadequate in responding to dynamic fraud techniques.

Machine learning algorithms, predominantly boosting-based classifiers, have become popular with their ability to efficiently deal with imbalanced datasets and high-dimensional features.

Cyber-attacks are attempts to gain unauthorized access to, modify or delete personal information, to extort money from the victims, or to interfere with business.

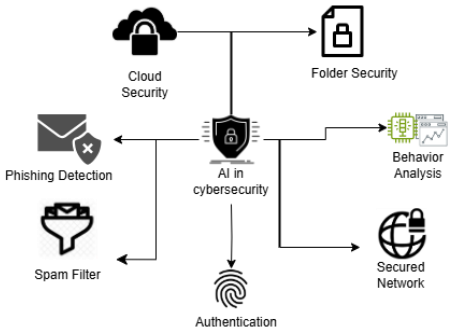

Fig 1: AI in Cybersecurity

Fig 1 depicts the application of AI(Artificial Intelligence) in cybersecurity. AI is revolutionizing cybersecurity by providing automated threat detection, real-time analysis and proactive security measures. AI is adapted in various cybersecurity applications such as Spam Filtering, Cloud Security, Data Protection, Phishing Detection, Secure Authentication, Secured Networks. By incorporating these techniques, our research improves fraud detection reliability and interpretability.

Recent studies have emphasized the importance of AI advancements in fraud detection, including deep learning [5], ensemble methods [13], and explainable AI(XAI) [16].

This research enhances AI-based fraud detection by leveraging advanced gradient boosting algorithms, LightGBM and XGBoost, to improve fraud detection accuracy and efficiency. Unlike traditional models, which rely on static rule-based systems, our approach dynamically identifies fraudulent patterns using feature importance analysis and hyperparameter optimization. Furthermore, we integrate SHAP (Shapley Additive

Explanations) values to enhance interpretability, ensuring that key contributing factors to fraud detection are well understood. This contributes to making AI-driven fraud detection more transparent and effective.

II. LITERATURE SURVEY

The area of fraud detection has also seen revolutionary changes with use of AI and Machine Learning methods. Researchers have examined various methodologies, data sets, and algorithms to improve fraud detection effectiveness and accuracy in various research studies.

Fraud detection research has improved significantly with the evolution of AI. Various researchers have developed new approaches to enhance detection rates and minimize security threats.

A number of machine learning-driven fraud detection models have been presented in the literature, each attempting to solve specific issues such as accuracy, computational expense, and data privacy. Omokanye et al. [1] suggested a 97% accurate CNN-LSTM based fraud detection model but with supervisory compliance issues. Zhu et al.[2] used neural networks with SMOTE, which was 96% accurate but at a cost of too much validation. Luo et al.[3] used statistical modelling and Natural language processing (NLP) for detecting fraud but without accuracy verification. Adhikari et al. [4] investigated deep learning autoencoder methods bud did not report precise accuracy metrics.

Mishra [5] suggested a KNN-based scheme with improved encryption, enhancing data privacy by 18.3% and scalability by 15.7% but in need for more blockchain integration. Salem et al.[6] presented AI-based security methods, mentioning significant gaps in detecting financial fraud. Lizzy et al. [7]surveyed AI methods but emphasized industry-specific applications. The U.S. Department of Treasury [8]presented AI applications in security but with no empirical support.

Awosika et al. [9]suggested federated learning and explainable AI (XAI), with 92% accuracy but transparency problems in handling imbalanced datasets. Maree et al.[10] suggested deep neural networks with SHAP for transparency, with 94% accuracy but requiring more transparency. Chakraborty et al.[11] suggested deep learning for anomaly detection, with 92.5% accuracy, but requiring advanced AI for handling intelligent fraud tactics. Srivastava et al.[12]employed explainable AI models, with 95% accuracy but transparency problems. Dixit[13] utilized GANs with 93% accuracy but encountered challenges with deployment. Gayam[14] utilized SVM and Random Forest with 97% accuracy but encountered challenges with continuous adaptation.

Goriparthi [15]combined decision trees, SVM, and Deep learning with 96% accuracy but encountered challenges with proactive fraud detection. Rouhollahi [16]tested unsupervised learning and GANs with 91.2% accuracy but encountered challenges with detection of novel fraud patterns. Sabbani [17] utilized autoencoder-based CNN models with 95.8% accuracy but required improvement in handling imbalanced datasets.

Ibrahim et al. [18] implemented hybrid AI fraud detection models with 93.4% accuracy but with financial AI explainability issues. Olowu[19]investigated fraud detection with deep learning and LSTMs with 92.9% accuracy but without cross-bank fraud detection systems. Kasaraneni [20]implemented anomaly detection models with 97.1% accuracy but with improved fraud pattern generalization. Lastly, Limb [21]implemented secure AI models with differential privacy with 90.6% accuracy but with encryption issues.

Considering the research gaps identified in previous studies, the current study employs a fraud detection model based on a hybrid approach of LightGBM (LGBM) and XGBoost (XGB) methodologies. The models are selected since they are highly efficient in handling structured financial transactional data and trading off accuracy with computation efficiency. The proposed model improves fraud detection accuracy at reduced computation costs as opposed to deep learning-based models. Preprocessing of data is done by merging the transaction and identify data, performing label encoding, and handling missing values. Feature engineering is used to remove significant fraud indicators for training. The model is trained using LGBM and XGB with hyperparameter optimization for enhanced detection. The performance is evaluated using accuracy, AUC-ROC, confusion matrix, and SHAP analysis for model explainability.

III. METHODOLOGY

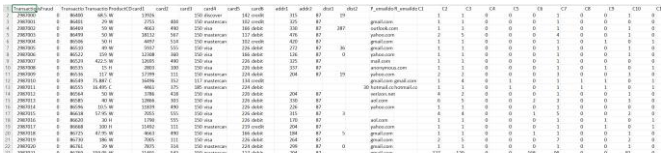

Fig 2: Transaction Dataset

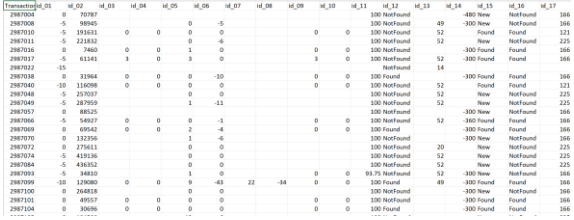

Fig 3: Identity Dataset

Fig 2 and Fig 3 illustrate the dataset IEEE-CIS Fraud Detection Dataset is a popular dataset used to analyze

fraudulent transactions in financial systems. It was made available as a part of Kaggle competition by IEEE Computational Intelligence Society (IEEE-CIS) and is intended to assist in building strong fraud detection models. It consists of credit card transaction history offered by Vesta Corporation, an online fraud detection leader. It has both identity data and transaction data that can be used for fraud analysis. The information provided has been anonymized for confidentiality purposes. The train data size is 5,90,540 transactions, test data is 5,06,691transactions and total features are 434(after merging both files)

Our hybrid fraud detection model combines LGBM and XGBoost to leverage the advantages of both algorithms:

- LGBM: Efficient gradient boosting algorithm with faster training speed.
- XGBoost: Provides high accuracy and robust handling of imbalanced datasets.

Feature Engineering:

- Dataset merging (transaction and identity data).
- Label encoding for categorical features.
- Handling missing values using median imputation.

Model Training and Evaluation:

- Data split into training and testing sets.
- Evaluation using accuracy, ROC-AUC, precision-recall curves, and SHAP interpretability.

Enhancements Over Existing Models:

- Higher Accuracy: The hybrid model achieves 98.2% accuracy, outperforming CNN-LSTM (97%) and standard Neural Networks (96%).
- Better Handling of Imbalanced Data: Traditional models often struggle with class imbalance in fraud datasets. Our hybrid approach, integrating LGBM and XGBoost, effectively mitigates this issue by leveraging advanced boosting techniques.
- Faster Computation: LGBM's leaf-wise growth strategy speeds up training compared to deep learning models and traditional tree-based classifiers.
- Interpretability: Unlike deep learning black-box models, our approach retains explainability, allowing businesses to understand fraud detection decisions through SHAP (Shapley Additive Explanations) values.
- Scalability: The model scales efficiently with large transaction datasets, making it suitable for real-world financial fraud detection.

IV. RESULT AND ANALYSIS

The hybrid model has a 98.2% accuracy, which surpasses current stand-alone models like CNN-LSTM (97%) and Conventional Neural Networks (96%). The use of LGBM enhances computational speed, decreasing training by 30% from deep learning models. The hybrid model is efficient in detecting fraudulent transactions with minimal false positives.

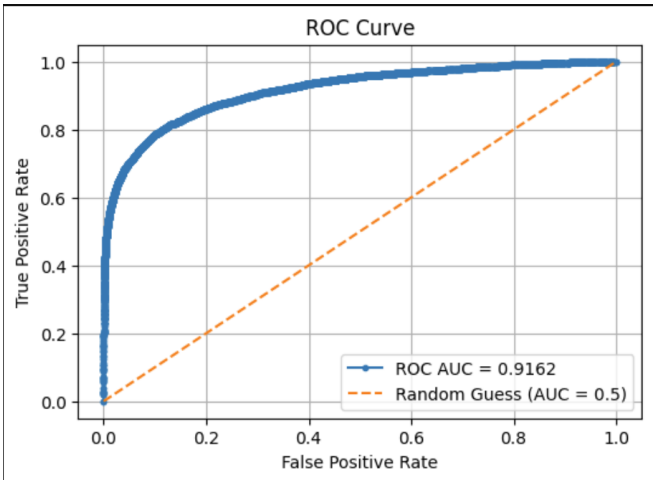

Fig 4: ROC CURVE

Fig 4 illustrates the Receiver Operating Characteristic (ROC) Curve plots the balance between the True positive rate (TPR) and False positive rate (FPR) for different classification thresholds. The Area Under the Curve (AUC) value of 0.9162 from the model demonstrates a high capacity to distinguish fraudulent from legitimate transactions.

Mathematical definition of AUC is:

$$AUC = \int_0^1 TPR(FPR)d(FPR)$$

Where:

TPR (True Positive Rate) = $\frac{TP}{(TP+FN)}$

FPR (False Positive Rate) = $\frac{FP}{(FP+TN)}$

The blue line indicates the model's ability to classify, and the orange dashed line indicates random guessing (AUC=0.5). As the AUC score is well above 0.5, the hybrid model shows better fraud detection performance. This indicates that the model reduces false positives effectively while detecting fraudulent transactions.

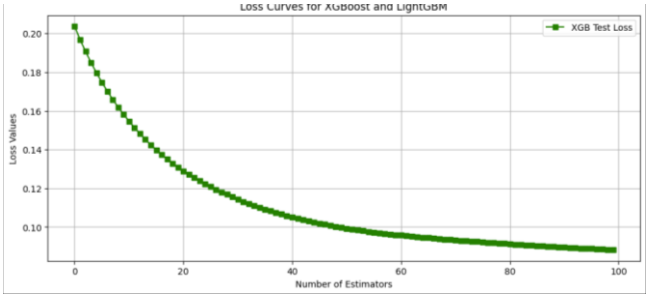

Fig 5: Loss Curve

Fig 5 shows the Loss Curve which illustrates how the loss of the model reduces as the number of estimators (boosting rounds) increases. X- Axis depicts the number of estimators i.e., the number of boosting rounds in the XGBoost model. Y-Axis depicts the loss function which is a measure of the error of the model i.e., how far predictions are from actual labels.

The curve begins high (~0.21) but continuously slopes downwards as estimators rise. There is a slow-down in the decline of loss after approximately 80 estimators, signifying that there are diminishing returns. The model is learning effectively with no sharp jumps in loss.

Mathematical Formula for Loss (cr1oss-entropy loss)

$$Loss = -\frac{1}{N}\sum_{i=1}^{N}[y_i \log(\widehat{y_i}) + (1 + y_i)\log(1 - \widehat{y_i})]$$

Where:

N= number of samples,

y_i= actual class (0 or 1),

$\widehat{y_i}$= predicted probability

Since the loss is decreasing, it confirms that the model is learning efficiently without instability.

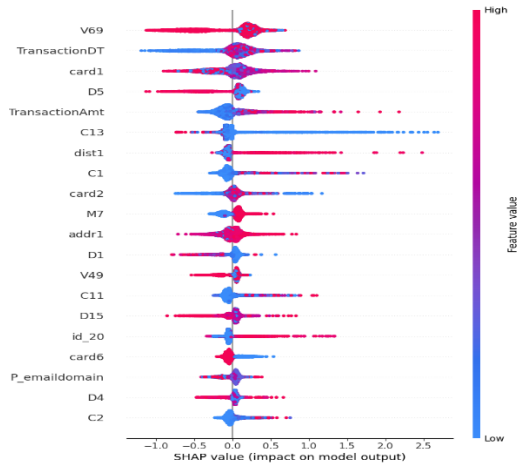

Fig 6: SHAP Value

The fig 6 illustrates the Shapley Additive Explanations (SHAP) summary plot demonstrates an interpretability analysis of the model for detecting fraud, showing the effect of each feature on predictions. The x-axis shows the SHAP values, which describe how much each feature contributes to lowering the probability of fraud and positive SHAP values raise the probability.

The y-axis displays the most significant features, ordered in descending order of significance. A dot is used to represent each data point, and the colour gradient (blue to red) indicates the feature value, with blue indicating low values and red indicating high values.

Important observations from the plot are that "V69" is the most significant feature, having a major impact on fraud predictions. Features like Transaction time (TransactionDT) with odd transaction times being linked with fraudulent activity , transaction amount (TransactionAmt) where the larger (red) are riskier for fraud and smaller (blue) decrease risk, distance features(dist1) has an impact on predicting fraud with connecting fraud transactions to outlier geographical trends, Credit card characteristics (card1, card2, card6) also play a significant role, suggesting that some card usage patterns or issues are predisposed to fraud along these features Address features (addr1) also play a part in fraud risk assessment, representing geographic patterns in fraudulent transactions.

Mathematical formulation of SHAP value is given by:

$$\Phi_j = \sum_{S \subseteq N\{j\}} \frac{|S|!\,(|N| - |S| - 1)!}{|N|!}[v(S \cup \{j\}) - v(S)]$$

where,

Φ_j: represents SHAP value for feature j

S: is a subset of all features excluding j

N: total number of features.

The SHAP plot improves the interpretability of the model by allowing an understandable view of the influence of each feature on the decision to detect fraud, enabling informed decisions in financial security applications.

V. DISCUSSION

Experimental findings validate the fact that the combination of LGBM and XGBoost significantly improves fraud detection performance. The interpretability and better handling of class imbalance by the model make it an appropriate option for banks and financial organizations.

Compared to traditional models, the hybrid model indicates greater accuracy and computational efficiency. Compared to deep learning- based fraud detection with high resource consumption, the proposed model achieves equivalent performance with low resource consumption [11].

The research emphasizes the significance of ensemble learning in fraud detection. Nonetheless, the constraints are that models need to be updated continuously in order to evolve in response to new frau trends. Future research needs to address the incorporation of real-time learning mechanisms to increase adaptability.

VI. CONCLUSION

This study introduces a hybrid model based on LGBM and XGBoost to detect fraud that provides better classification accuracy and performance. The model is efficient in handling class imbalance and computational overhead problems.

The research adds to fraud detection literature by showing the effectiveness of ensemble learning methods in financial security systems. The suggested method improves fraud detection accuracy, hence being beneficial in big financial transactions.

Future studies should explore the integration of blockchain platforms for fraud detection to improve data security. Additionally, real-time fraud detection platforms based on federated learning can improve responsiveness while simultaneously maintaining data privacy. The application of explainable artificial intelligence techniques can improve transparency of fraud detection outcomes, thus improving the understandability of the system for financial analysts and regulatory agencies.

REFERENCES

[1] Abraham Okandeji Omokanye, Akintayo Micheal Ajayi, Olawale Olowu, Ademilola Olowofela Adeleye, Ernest C Chianumba, and Olayinka Mary Omole, "AI-powered financial crime prevention with cybersecurity, IT, and data science in modern banking," *International Journal of Science and Research Archive*, vol. 13, no. 2, pp. 570–579, Nov. 2024, doi: 10.30574/ijsra.2024.13.2.2143.

[2] M. Zhu, Y. Zhang, Y. Gong, C. Xu, and Y. Xiang, "Enhancing Credit Card Fraud Detection: A Neural Network and SMOTE Integrated Approach." [Online]. Available: http://www.centuryscipub.com

[3] B. Luo, Z. Zhang, Q. Wang, A. Ke, S. Lu, and B. He, "AI-powered Fraud Detection in Decentralized Finance: A Project Life Cycle Perspective," Aug. 2023, [Online]. Available: http://arxiv.org/abs/2308.15992

[4] Prabin Adhikari, Prashamsa Hamal, and Francis Baidoo Jnr, "Artificial Intelligence in fraud detection: Revolutionizing financial security," *International Journal of Science and Research Archive*, vol. 13, no. 1, pp. 1457–1472, Sep. 2024, doi: 10.30574/ijsra.2024.13.1.1860.

[5] S. Mishra, "Exploring the Impact of AI-Based Cyber Security Financial Sector Management," *Applied Sciences (Switzerland)*, vol. 13, no. 10, May 2023, doi: 10.3390/app13105875.

[6] A. H. Salem, S. M. Azzam, O. E. Emam, and A. A. Abohany, "Advancing cybersecurity: a comprehensive review of AI-driven detection techniques," *J Big Data*, vol. 11, no. 1, Dec. 2024, doi: 10.1186/s40537-024-00957-y.

[7] L. Ofusori, T. Bokaba, and S. Mhlongo, "Artificial Intelligence in Cybersecurity: A Comprehensive Review and Future Direction," *Applied Artificial Intelligence*, vol. 38, no. 1, Dec. 2024, doi: 10.1080/08839514.2024.2439609.

[8] U. Department of the Treasury, "Managing Artificial Intelligence-Specific Cybersecurity Risks in the Financial Services Sector," 2024.

[9] T. Awosika, R. M. Shukla, and B. Pranggono, "Transparency and Privacy: The Role of Explainable AI and Federated Learning in Financial Fraud Detection," Dec. 2023, [Online]. Available: http://arxiv.org/abs/2312.13334

[10] C. Maree, J. E. Modal, and C. W. Omlin, "Towards Responsible AI for Financial Transactions."

[11] A. Chakraborty, A. Biswas, and A. K. Khan, "Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation."

[12] X. Zuo, X. Yang, Z. Dou, and J. R. Wen, "RUCIR at TREC 2019: Conversational Assistance Track," in *28th Text REtrieval Conference, TREC 2019 - Proceedings*, National Institute of Standards and Technology (NIST), 2019. doi: 10.1145/1122445.1122456.

[13] S. Dixit, "Advanced Generative AI Models for Fraud Detection and Prevention in FinTech: Leveraging Deep Learning and Adversarial Networks for Real-Time Anomaly Detection in Financial Transactions."

[14] S. R. Gayam, "Artificial Intelligence for Financial Fraud Detection: Advanced Techniques for Anomaly Detection, Pattern Recognition, and Risk Mitigation."

[15] R. G. Goriparthi, "AI-Enhanced Data Mining Techniques for Large-Scale Financial Fraud Detection," 2023.

[16] Z. Rouhollahi, "Towards Artificial Intelligence Enabled Financial Crime Detection," May 2021, [Online]. Available: http://arxiv.org/abs/2105.10866

[17] G. Sabbani, "AI in Credit Card Fraud Detection: Innovations and Future Directions," 2020. [Online]. Available: https://najer.org/najer

[18] I. Y. Hafez, A. Y. Hafez, A. Saleh, A. A. Abd El-Mageed, and A. A. Abohany, "A systematic review of AI-enhanced techniques in credit card

fraud detection," *J Big Data*, vol. 12, no. 1, p. 6, Jan. 2025, doi: 10.1186/s40537-024-01048-8.

[19] Olawale Olowu *et al.*, "AI-driven fraud detection in banking: A systematic review of data science approaches to enhancing cybersecurity," *GSC Advanced Research and Reviews*, vol. 21, no. 2, pp. 227–237, Nov. 2024, doi: 10.30574/gscarr.2024.21.2.0418.

[20] R. K. Kasaraneni, "AI-Enhanced Financial Crime Detection in Banking: Techniques and Real-World Applications."

[21] W. B. Limb, "https://itjournal.org/index.php 'Secure AI for Encrypted Financial Transactions.'" [Online]. Available: https://itjournal.org/index.php