International Information and Engineering Technology Association
Advancing the World of Information and Engineering

International Journal of Safety and Security Engineering
Vol. 15, No. 2, February, 2025, pp. 331-337
Journal homepage: http://iieta.org/journals/ijsse

# Hybrid Machine Learning for Fraud Detection: Balancing Accuracy and Security in Digital Transactions

A. Anil Kumar, S. Hrushikesava Raju*

Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Guntur 522302, India

Corresponding Author Email: hkesavaraju@gmail.com

https://doi.org/10.18280/ijsse.150214

**Received:** 3 December 2024
**Revised:** 31 January 2025
**Accepted:** 13 February 2025
**Available online:** 28 February 2025

***Keywords:***
*challenges, transactions, hybrid method, random forests, ensemble, fraudulent activities, accuracy, performance*

## ABSTRACT

Nowadays, frauds would occur by hackers and non-legitimate users, which would create losses for specific users and damage their identity. The kinds of fraud that popularly happen are transaction fraud, card fraud (card not present), phishing, and account takeover. To prevent and minimize the losses, the hybrid model is designed and demanded. The combination of random forests, LightGBM, and Ensemble is used to improve overall performance and accuracy improvement and ensure privacy and security concerns. In this methodology, random forests reduce overfitting, support large datasets, prefer ranked features, are less sensitive to noise, and result in improvement in accuracy. The role of LightGBM is to ensure boosting in speed and memory usage, support large datasets and imbalanced datasets, and ensure reduced false positives and false negatives. The necessity of an ensemble strategy in this scenario is to combine the benefits of random forest and LightGBM, ensure overall performance, and eliminate flagging legitimate transactions as fraudulent. The performance measures are evaluated and compared against the considered models in this domain.

## 1. INTRODUCTION

There is a scenario from which, most customers would experience identity theft through specific links clicking or loss of amounts by trapping with huge discounts or by valuable gifts. In modern days, many innocent people although they are good at technology usage, are trapped with social benefit aspirations. When using social platforms for their connections with friends, third-party party advertisements and gifs shown would trap with offering huge discounts for purchasing specific items. Customers who see unintended content for the first time may experience a loss of money or loss of identity. The maintenance of the site admin would ask for feedback on the portions of the website. If the customer experiences negative behavior in the sense of loss of money, they would immediately tag that portion with a fraud tag. Future customers would benefit from clicking such advertisements. In this way, the admin of the site controls the portions that appear in the content of the social website/platform. Various machine learning approaches are suggested to classify the unverified portions as fraud or non-fraud. There is another scenario, where detecting fraud transactions in the history of transactions using machine learning techniques is challenging. From this scenario, the existing hybrid approach would be flexible to new updates as well as tune with upcoming techniques to further the level of security. Among specific machine learning approaches, the hybrid approach is designed to achieve more accuracy, and performance compared to other existing methods.

From Table 1, there is a scope for deriving the hybrid method that have multiple benefits as well as care is taken while designing the principle. From Table 2, trends were highlighted from the introduction of computers to many machine learning models, then the usage of modern technologies such as AI, and Deep learning models, and the current trend is on hybrid methodologies to favor more benefits than other individual approaches. In the evolvement of fraud detection, the assessment of techniques to be applied is demonstrated in Table 3. From Table 3, the machine learning model is considered for fraud detection, able to integrate with new approaches in a flexible manner, and involves moderate complexity.

**Table 1.** Methods to be used for classification

| Method | Advantages | Disadvantages |
|---|---|---|
| Decision Trees | Easy to interpret and visualize<br>Handles both numerical and categorical data well | Prone to overfitting<br>Sensitive to noisy data |
| Random Forest | Reduces overfitting through ensemble learning<br>Handles large datasets effectively | Less interpretable than single decision trees<br>Can be computationally intensive |
| Support Vector | Effective in high-dimensional spaces | Less effective on very large datasets |

| | | |
|---|---|---|
| Machines | Robust against overfitting in high-dimensional data | Requires careful tuning of parameters |
| Logistic Regression | Simple and efficient for binary classification<br>Provides probabilities for outcomes | Assumes linear relationship between features and outcome<br>Not suitable for complex relationships |
| Naive Bayes | Fast and efficient for large datasets<br>Works well with text classification tasks | Assumes independence between features<br>May perform poorly if this assumption is violated |
| Neural Networks | Capable of capturing complex patterns<br>Highly flexible and adaptable to various tasks | Requires large amounts of data<br>Can be a "black box", making interpretation difficult |
| Ensemble Methods | Combines strengths of multiple models<br>Generally, improves accuracy and robustness | More complex to implement and tune<br>Can be computationally expensive |
| Hybrid Machine Learning | Leverages strengths of different models for better accuracy<br>Can reduce false positives effectively | Requires careful design and validation |

**Table 2.** Summary of trends in detection of fraud in decades

| Decade | Trend | Description |
|---|---|---|
| 1980s | Emergence of Computerized Fraud Detection | Computerized systems were introduced for detecting fraudulent transactions, primarily in banking and finance. |
| 1990s | Data Mining Techniques | Specific data mining tools used to analyze large datasets for patterns indicative of fraud, leading to more sophisticated detection systems. |
| 2000s | Machine Learning Algorithms | Machine learning algorithms were increased, such as decision trees and neural networks, to improve accuracy in fraud detection and classification. |
| 2010s | Big Data Analytics | Bigdata tools were enabled to process vast amounts of transaction data in real time, enhancing the ability to detect fraud as it occurs. |
| 2020s | AI and Deep Learning | Specific Deep learning and AI mechanisms were used for more nuanced fraud detection, including anomaly detection and predictive analytics. |
| | Focus on Identity Theft | Growing concern over identity theft, leading to enhanced measures for protecting personal information and monitoring for fraudulent activities. |
| | Regulatory Compliance | Increased emphasis on compliance with regulations related to fraud prevention, such as GDPR and PCI DSS, impacts how organizations approach fraud detection. |
| | Hybrid Approaches | Development of hybrid models that combine multiple machine learning techniques to improve detection rates and reduce false positives. |

**Table 3.** Techniques recommended for fraud detection

| Technique | Description | Pros | Cons |
|---|---|---|---|
| Real-Time Monitoring | Systems that analyze transactions as they occur. | Immediate detection of suspicious activities. | Extensive resource consumption, and create many dales positives. |
| Machine Learning Algorithms | Models that learn from historical data to identify fraud patterns. | Can adapt to new fraud techniques; improves accuracy over time. | Takes time for training and involves complexity in tuning. |
| Custom Risk Rules | Tailored rules to flag transactions based on specific criteria. | Flexibility to adapt to business needs; can quickly address emerging threats. | May require continuous updates; risk of missing nuanced fraud patterns. |
| Address Verification Services | Verifies billing addresses against bank records. | Reduces risk of unauthorized transactions. | May inconvenience legitimate customers; not foolproof against all fraud types. |
| Behavioral Analytics | Analyzes user behavior to detect anomalies. | Identifies unusual patterns that may indicate fraud. | Requires baseline data; may struggle with legitimate changes in user behavior. |
| Chargeback Analysis | Monitoring chargebacks to identify potential fraud. | Provides insights into customer behavior and fraud trends. | Would be reactive rather than proactive, and may not for all types of fraud. |
| Integration with AML Workflows | Combines fraud detection with anti-money laundering processes. | Streamlines compliance; and enhances overall risk monitoring. | Complexity in integration; may require additional resources and training. |
| Multi-Factor Authentication | Adds extra verification steps during transactions. | Increases security; and reduces unauthorized access. | Lead to an abandonment of transactions if too cumbersome. |

## 2. LITERATURE REVIEW

There are certain studies on fraud detection in financial transactions that cause loss of money for the customer as well as bank too in some cases. To overcome these issues, the studies involved in this domain are analyzed and demonstrated here. Achary and Shelke [1], the usage of machine learning and AI would quickly detect fraud, which enables the taking of necessary steps to prevent the loss of money. The methodology used to get better accuracy than traditional methods used in this scenario. From Maskale et al. [2], the history of transactions is analyzed and cleaned using data preprocessing and applied using machine learning models. These models' accuracy is computed and compared. The objective is for the number of customers' churning rate to be detected and to provide the best practices to retain those customers. From Gandhi and Gajjar [3], the review is conducted on various domains that increase fraud detection rates and increase protection on customer interests in making secure payments over digital transactions. From Akash et al. [4], demonstrated many methodologies for financial fraud detection. Effective protection schemes as well as by combining a few methodologies for efficient financial transactions are provided to safeguard the organizational resources. According to Tatineni [5], the integration of ML approaches with blockchain technology avoids easy fraudulent activity. This integration improves traceability as well as secure financial transactions. From Ismail, M.M., Haq [6], the demonstration of various ML approaches with AI, are compared for accuracy. The random forest against other classifiers is evaluated and found random forest has having best accuracy. From Kajol et al. [7], demonstrated the motivators for the adoption of digital technology such as fast accomplishment, security, comfort, and others. The challenges also identified such as training, cost, complexity, and others that would stop from expansion of adoption. From Abad-Segura and González-Zamar [8], demonstrates the publications that have recently in the domain of banking, and financial-related transactions. In this, oxford students have done many publications in this domain. This signifies the importance of financial transactions today. From Ushadevi [9], the differences between mobile transaction banking and traditional banking are demonstrated. The revolution in usage of applications of many banks in India made paperless, and easy to do tasks in terms of depositing as well as fund transfer. From Westermeier [10], the European countries suffer from technology, political, and economic issues. When individual data is transformed into application data, where the customer can perform transactions. This became base for more insights to perform any trending analysis.

From Aburbeian andFernández-Veiga [11], demonstrated two level layers which are MFA and ML techniques. There are ML models such as Random Forest, Logistic regression, and other models that were used, and their accuracies are evaluated. This system validates authentication and increases security measures. From Kajol and Singh [12], the users in India status on digital transactions is reported that male members have more ideas on digital awareness, and challenges listed in this study. This survey is done by imposing a set of questionnaires to a few samples to know the digital awareness of our Indian people. From Liu et al. [13], demonstrated the fintech research in terms of adoption, and its development. There were many articles published in this domain. Mostly. classification is one popular approach against 5 measures that showcase current status and future analysis. From Salam et al. [14], the challenges in the banking sector faced during the pandemic are highlighted and are minimized with the increase in mobile banking applications with security and user comfort. Most people's lives are safe and threats is minimized using mobile banking applications, and usage of them are increased thereafter. From Pereira et al. [15], demonstrated avoiding and minimizing cyberbullying using normalization of data preprocessing, then a decision tree algorithm with sophistication, and also used PSO for forecasting financial marketing. these models are compared and recommended network models with feature extraction for achieving more accuracy and efficiency. From Gaur and Verma [16], demonstrated advertisements, and necessary steps to promote the usage of digital and mobile financial applications in Haryana. The initiations that government agencies, NGO firms, to invest and service agencies provide effective services. From Malagatti et al. [17], demonstrated the various tools and assessments to increase digital platform usage awareness. The objective of Fintech is to assess the usage of digital platforms using techniques such as correlation, regression, and Few tests. From Kotni and Botta [18], demonstrated the people's patterns of Visakhapatnam City who perform digital transactions, and their demographics. This reports people are less usage of cash but make use of mostly digital platforms for money transactions. The union budget initiations for deep awareness on digital literacy. From Al-Hashedi and Magalingam [19], demonstrated the articles published during specific periods in which most are done on bank fraud, and insurance fraud, using popular method SVM, then followed other models such as random forest, and naive Bayesian. From Dama et al. [20], demonstrated the various models that minimize the false positives in fraudulent activities. This system focused on detecting unusual patterns as well as able to detect new types of vulnerabilities also effectively. From Al Marri and AlAli [21], the fraudulent tasks were detected using many ML techniques, and their accuracies were compared. Their challenges are addressed in this study. From West et al. [22], demonstrated various approaches that were used to detect fraud behavior. In this, traditional and automated processes are analyzed, and compared. From Ali et al. [23], demonstrated the type of fraud called credit card fraud, and its detection using famous methods such as Support vector machines and Neural network approaches. Many articles are studied and explored their gaps and restrictions for further future development. The other studies represent storage and distribution of load in which Dey and Sangaraju [24] demonstrated the issues of using local, global load balancing strategies for the distribution of workload among the available entities over the cloud and Dey and Sangaraju [25] demonstrated effective mechanisms for evaluating the performance of load balancing involved over the cloud usage. In regard to work of Talukder et al. [26], the combination of methods used and integrated are such as Decision Trees, Random Forests, Multilayer perceptron, K-nearest neighbor, and instant hardness threshold approach together. Their performances, and accuracies when compared in which proposed hybrid approach produces too far better result but complexity, and lack of appropriate links among the strategies is the drawback of this model. In the view of Btoush et al. [27], the considered models from machine learning and deep learning are used and ensemble approaches such as stacking and resampling are applied. The best method which produces better accuracy, and performance is taken and yields higher F1-score than others used in the evaluation but considering many methods results complexity of the process.

## 3. PROPOSED METHODOLOGY

In this, the proposed system consists of Random Forest, Light GBM, and Ensemble approaches for securing expected performance and better accuracy. In this, Figure 1 demonstrates the module's interaction that involves the History of transactions as a dataset, validation that the customer is the right real entity, data preprocessing on the unstructured transactions, applying a hybrid model for training to produce output is fraud or non-fraud, and evaluation of metrics for assessing the effectiveness of the model, Figure 2 depicts the ER Model that consists of significant entities and their activities to be used, and Figure 3 represents the flow of activities for efficient fraud detection that involve functionalities such as validation, flagging the fraud transaction, scrutinizing using rules and scoring system, usage of MFA for further level of increasing security, and applying of compliance, and auditing. The PS1 and PS2 represent Hybrid approach logic and ensemble approach definitions.

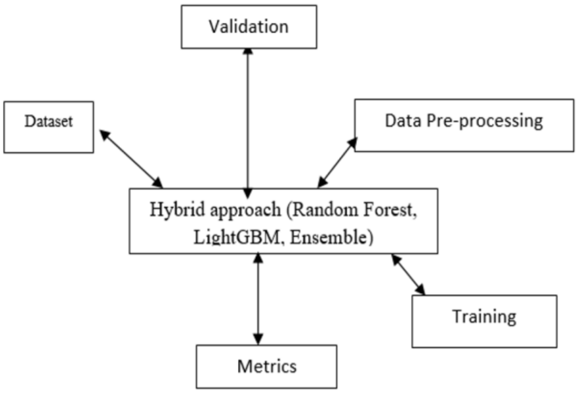

**Figure 1.** Modules of hybrid approach for fraud detection

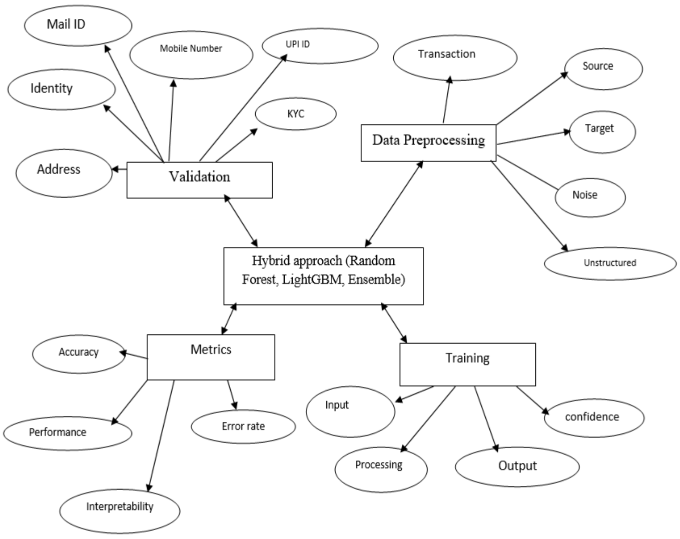

**Figure 2.** ER model of hybrid approach for fraud detection

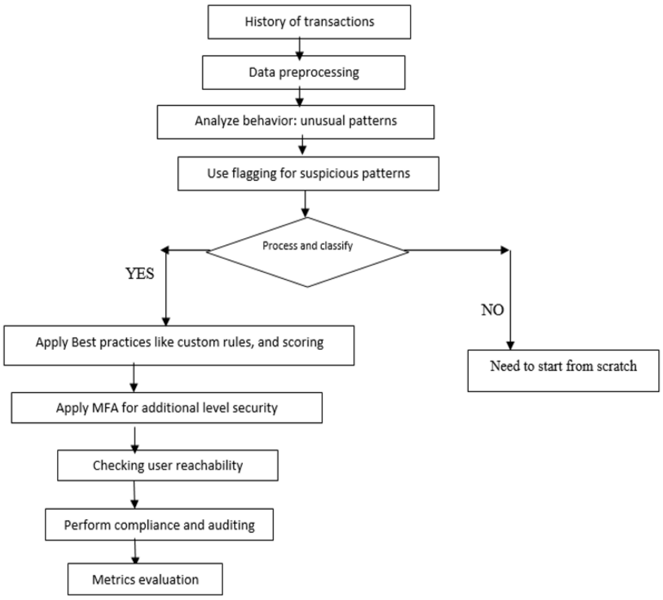
History of transactions
Data preprocessing
Analyze behavior: unusual patterns
Use flagging for suspicious patterns
Process and classify
YES
NO
Apply Best practices like custom rules, and scoring
Need to start from scratch
Apply MFA for additional level security
Checking user reachability
Perform compliance and auditing
Metrics evaluation

**Figure 3.** Flow of activities in the hybrid model for fraud detection

The PS1 demonstrates on hybrid model that involves both the machine learning methods such as random forest and LightGBM. The data preprocessing is applied before the model is applied. The significant parameters are applied to determine the fraud intensity. The output of these models would be given to the ensemble approach stacking for refined and better measures.

The PS2 demonstrates on meta-model approach, and uses hyper parameters for training and testing. The prediction would result in better accuracy and expected performance.

```
PS1: Pseudo_Procedure Hybrid_Approach_fruad_detection(Transactions):
Input:Transactions
Output: Classification as Fraud or Non-Fraud
Step1: History of transactions
Step2: Data preprocessing for cleaning and forming them in structured content
Step3: Checking validation level, highest level includes MFA for increased security
Step4: Analyze the hyperparameters such as speed of performing transactions, device change, number of logins failed attempts, multiple payment types, previous fraudulent behavior history, etc.
Step5: For the random forest method, set up the number of trees, and maximum depth level
Step6: Divide the dataset into training and testing
Step7: Train the random forest methodology over the training set
Step8: Apply prediction on the testing set
Step9: Evaluate the measures such as accuracy, precision, recall, and F-Score
Step10: Apply the refined dataset over LightGBM method
Step11: Apply preprocessing as before random forest
Step12: Define hyperparameters, and define new features if required from existing features
Step13: Divide the refined set into training, and testing
Step14: Define the learning rate, and number of leaves in the training
Step15: Apply prediction on testing set
Step16: Evaluate the measures such as accuracy, precision, recall, and F-Score
```

Accuracy=True Positives+True Negatives/ Total Number of Cases Where True Positives (TP): The number of correctly identified relevant data points, True Negatives (TN): The number of correctly identified irrelevant data points, Total Number of Cases: The sum of true positives, true negatives, false positives, and false negatives.

In PS1, there are modules such as data preprocessing to eliminate the inconsistencies, Random Forests to achieve performance, and reduce overfitting, LightGBM in which speed and memory usage optimal are applied for identifying fraud behavior such as involved Fraud or non-Fraud. In this, evaluated the False Positives, and False Negatives.

```
PS2: Pseudo_Procedure Ensemble_fruad_detection(Models):
Input: Models
Output: Performance
Step1: Load the refined dataset after random forest, and LightGBM
Step2: Apply data preprocessing
Step3: Apply stacking for meta-model use, and predictions
Step4: Divide the refined dataset into training and Testing
Step5: Train using Stacking
Step6: Do a prediction on using testing
```

Step7: Evaluate the measures such as accuracy, precision, recall, and F1-Score

Accuracy=True Positives+True Negatives/ Total Number of Cases

Precision = TP / (TP + FP)

Recall = TP / (TP + FN)

F1-Score = 2 * (Precision * Recall) / (Precision + Recall)

Error rate= Number of either (False Positives, False Negatives) predictions

From PS2, Ensemble strategy stacking is considered. In this, Combined methodology is applied, and produces measures such as F1-score, Recall, and Precision.

## 4. RESULTS

Table 4 demonstrates on expected measure intensity, Table 5 represents measure values, Table 6 denotes measures of performance evaluation, and Table 7 involves error rates of considered methods. Figure 4 denotes the effectiveness of the models from which hybrid model has more satisfying measures, Figure 5 denotes measures involved in performance evaluation, and Figure 6 depicts on which model has minimum error rates, that decides to choose best model.

The implication of Table 4 is that a hybrid model defined and derived would experience extraordinary results compared to other considered individual models.

**Table 4.** Metrics intensity against specific metrics

| Technique | Accuracy | Performance | Interpretability | Error Rate | Cost |
|---|---|---|---|---|---|
| Random Forest | High | Good for large datasets | Moderate | Moderate | Moderate |
| Support Vector Machine (SVM) | High | Good, but slower with large datasets | Low | Low | High |
| Logistic Regression | Moderate to High | Fast | High | Moderate | Low |
| Neural Networks | Very High | High, but resource-intensive | Low | Low | High |
| XGBoost | Very High | Fast and efficient | Moderate | Low | Moderate to High |
| Hybrid Approach (RF, LightGBM, Ensemble) | Very High | Very efficient | Moderate | Very Low | Moderate |

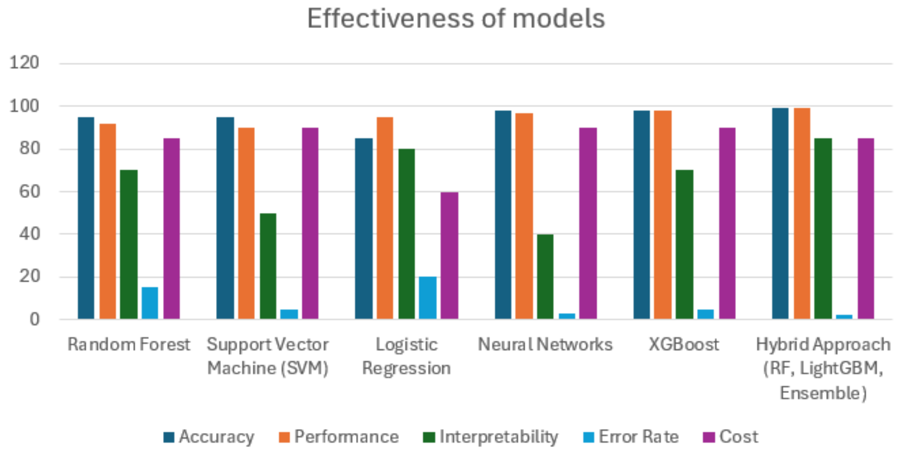

**Figure 4.** Effectiveness of models against the hybrid method for fraud detection

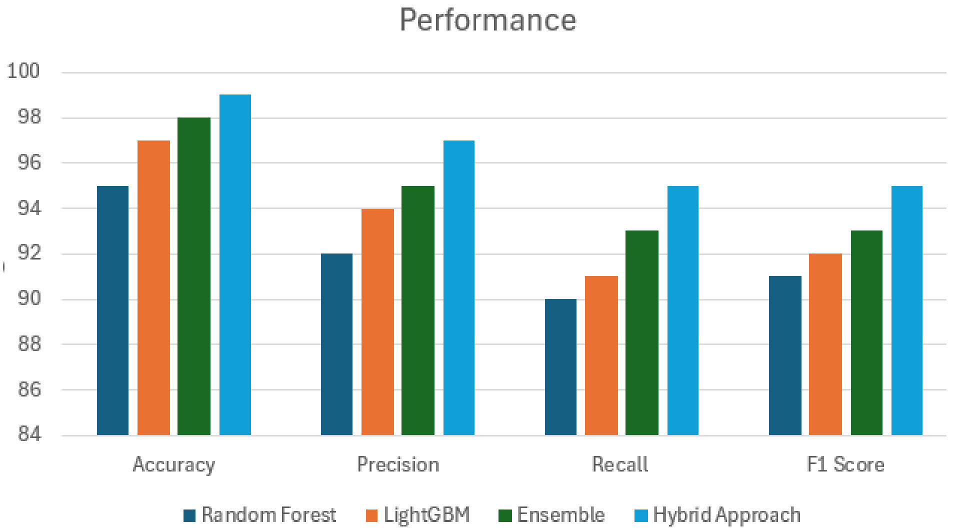

**Figure 5.** Performance of considered models separately against combined

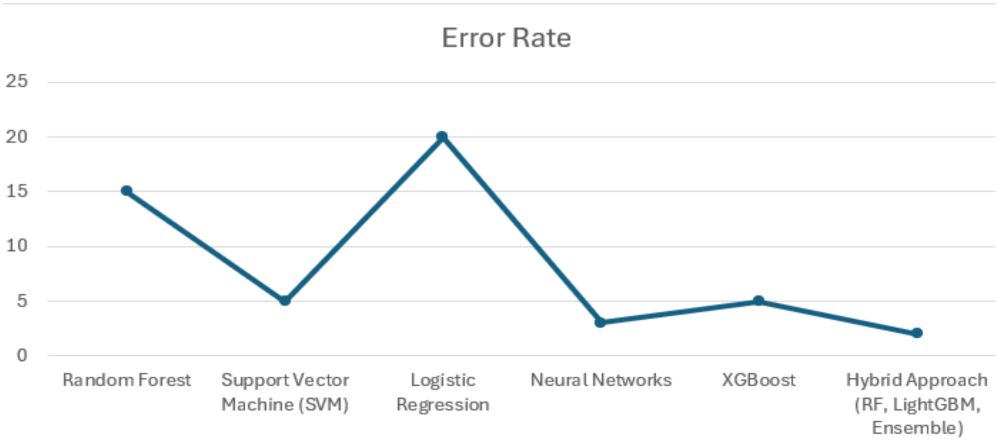

**Figure 6.** Error rate of considered models

**Table 5.** Comparison of metrics against the considered models

| Technique | Accuracy | Performance | Interpretability | Error Rate | Cost |
|---|---|---|---|---|---|
| Random Forest | 95 | 92 | 70 | 15 | 85 |
| Support Vector Machine (SVM) | 95 | 90 | 50 | 5 | 90 |
| Logistic Regression | 85 | 95 | 80 | 20 | 60 |
| Neural Networks | 98 | 97 | 40 | 3 | 90 |
| XGBoost | 98 | 98 | 70 | 5 | 90 |
| Hybrid Approach (RF, LightGBM, Ensemble) | 99 | 99 | 85 | 2 | 85 |

**Table 6.** Specific performance metrics against individual methods of hybrid model

| Model | Accuracy | Precision | Recall | F1 Score |
|---|---|---|---|---|
| Random Forest | 95 | 92 | 90 | 91 |
| LightGBM | 97 | 94 | 91 | 92 |
| Ensemble | 98 | 95 | 93 | 93 |
| Hybrid Approach | 99 | 97 | 95 | 95 |

**Table 7.** Error rate against the considered models

| Technique | Error Rate |
|---|---|
| Random Forest | 15 |
| Support Vector Machine (SVM) | 5 |
| Logistic Regression | 20 |
| Neural Networks | 3 |
| XGBoost | 5 |
| Hybrid Approach (RF, LightGBM, Ensemble) | 2 |

The implication of Table 5 analyzes the measures such as interpretability in terms of understanding and tuning, Error rate in terms of wrong predictions, time taken to complete the process is denoted by performance, and cost to implement, perfectness of the mechanism is described with evaluated values. From Table 6, the specific measures are described such as precision, recall, and F1-score, and are found good compared against individual models. From Table 7, the method that has a minimum error rate would be the best approach, and ensure reduced false positives, and effective detection rate.

## 5. CONCLUSION

The intensity of fraudulent behavior and patterns is identified with utmost accuracy, and overall performance is ensured using a hybrid approach. Although there are some fraud types that frequently occur, prevention is possible to the maximum extent when that is detected using a sophisticated approach. Hence, the combination of Random Forest, in which better accuracy is ensured and overfitting is avoided, then uses LightGBM in which optimal performance is ensured. The good choice is picked using an ensemble strategy called stacking. In this, the approaches considered are Random Forest, Support Vector Machines, Logistic Regression, Neural Networks, and XGBoost. Their effectiveness is described in terms of interpretability, cost-effectiveness, fault tolerance in terms of error rate, and optimality. In the future, the evaluation may be sustainable, and the mechanism may transform into a readymade or built-in tool for assessing whether the transaction is fraudulent or not.

## REFERENCES

[1] Achary, R., Shelke, C.J. (2023). Fraud detection in banking transactions using machine learning. In 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India, pp. 221-226. https://doi.org/10.1109/IITCEE57236.2023.10091067

[2] Maskale, V., Vaidya, V., Patil, Y., Bagal, Y., Dhamdhre, V. (2024). To design and implement application for bank customer churning rate prediction and analysis using machine learning algorithm. In 2024 MIT Art, Design and Technology School of Computing International Conference (MITADTSoCiCon), Pune, India, pp. 1-4. https://doi.org/10.1109/MITADTSoCiCon60330.2024.10575438

[3] Gandhi, V., Gajjar, T. (2024). Enhancing fraud detection

in financial transactions through cyber security measures. International Journal of Scientific Research in Computer Science Engineering and Information Technology, 10(2): 364-371. http://doi.org/10.32628/CSEIT2410281

[4] Akash, T.R., Islam, M.S., Sourav, M.S.A. (2024). Enhancing business security through fraud detection in financial transactions. Global Journal of Engineering and Technology Advances, 21(2): 79-87. https://doi.org/10.30574/gjeta.2024.21.2.0205

[5] Tatineni, S. (2020). Enhancing fraud detection in financial transactions using machine learning and blockchain. International Journal of Information Technology and Management Information Systems, 11(1): 8-15.

[6] Ismail, M.M., Haq, M.A. (2024). Enhancing enterprise financial fraud detection using machine learning. Engineering, Technology & Applied Science Research, 14(4): 14854-14861. https://doi.org/10.48084/etasr.7437

[7] Kajol, K., Singh, R., Paul, J. (2022). Adoption of digital financial transactions: A review of literature and future research agenda. Technological Forecasting and Social Change, 184: 121991. https://doi.org/10.1016/j.techfore.2022.121991

[8] Abad-Segura, E., González-Zamar, M.D. (2020). Global research trends in financial transactions. Mathematics, 8(4): 614. https://doi.org/10.3390/math8040614

[9] Ushadevi, P. (2018). A study on mobile banking financial transaction of major nationalized banks in India. International Journal of Management, Technology and Social Sciences, 3(2): 100-119.

[10] Westermeier, C. (2020). Money is data–the platformization of financial transactions. Information, Communication & Society, 23(14): 2047-2063. https://doi.org/10.1080/1369118X.2020.1770833

[11] Aburbeian, A.M., Fernández-Veiga, M. (2024). Secure internet financial transactions: A framework integrating multi-factor authentication and machine learning. AI, 5(1): 177-194. https://doi.org/10.3390/ai5010010

[12] Kajol, K., Singh, R. (2022). Users' awareness towards digital financial transactions: A study conducted in India. In International Working Conference on Transfer and Diffusion of IT, Maynooth, Ireland, pp. 331-345. https://doi.org/10.1007/978-3-031-17968-6_27

[13] Liu, Q., Chan, K.C., Chimhundu, R. (2024). Fintech research: Systematic mapping, classification, and future directions. Financial Innovation, 10(1): 24. https://doi.org/10.1186/s40854-023-00524-z

[14] Salam, M.A., Saha, T., Rahman, M.H., Mutsuddi, P. (2021). Challenges to mobile banking adaptation in COVID-19 pandemic. Journal of Business and Management Sciences, 9(3): 101-113. https://doi.org/10.12691/jbms-9-3-2

[15] Pereira, S.L., Abbas, J.G., Mahalakshmi, V. (2025). Artificial intelligence in behavioural finance using a sophisticated decision-tree algorithm. International Journal of Electronic Finance. https://doi.org/10.1504/IJEF.2025.10057976

[16] Gaur, A., Verma, S. (2025). Factors affecting the adoption of e-payment system in Haryana. International Journal of Electronic Finance. https://doi.org/10.1504/IJEF.2025.10058388

[17] Malagatti, V.D., Gudagi, A., Singh, K. (2024). A study on impact of fintech in financial services of banking sector. International Journal of Management, 15(4): 177-199. https://doi.org/10.5281/zenodo.13380000

[18] Kotni, V.V., Botta, A. (2020). A study on digital financial transactions performed by citizens of Visakhapatnam city. Our Heritage, 68(1): 6365-6375.

[19] Al-Hashedi, K.G., Magalingam, P. (2021). Financial fraud detection applying data mining techniques: A comprehensive review from 2009 to 2019. Computer Science Review, 40: 100402. https://doi.org/10.1016/j.cosrev.2021.100402

[20] Dama, K., Reddy, K.P.K., Hrithik, K., Raheem, D. (2024). Fraud detection in financial transactions. Kalasalingam Academy of Research and Education. https://doi.org/10.13140/RG.2.2.33977.99685

[21] Al Marri, M., AlAli, A. (2020). Financial fraud detection using machine learning techniques. Master's project, Rochester Institute of Technology.

[22] West, J., Bhattacharya, M., Islam, R. (2015). Intelligent financial fraud detection practices: An investigation. In International Conference on Security and Privacy in Communication Networks: 10th International ICST Conference, SecureComm 2014, Beijing, China, pp. 186-203. https://doi.org/10.1007/978-3-319-23802-9_16

[23] Ali, A., Abd Razak, S., Othman, S.H., Eisa, T.A.E., et al. (2022). Financial fraud detection based on machine learning: A systematic literature review. Applied Sciences, 12(19): 9637. https://doi.org/10.3390/app12199637

[24] Dey, N.S., Sangaraju, H.K.R. (2024). A particle swarm optimization inspired global and local stability driven predictive load balancing strategy. Indonesian Journal of Electrical Engineering and Computer Science, 35(3): 1688-1701. https://doi.org/10.11591/ijeecs.v35.i3.pp1688-1701

[25] Dey, N.S., Sangaraju, H.K.R. (2023). Hybrid load balancing strategy for cloud data centers with novel performance evaluation strategy. International Journal of Intelligent Systems and Applications in Engineering, 11(3): 883-908.

[26] Talukder, M.A., Hossen, R., Uddin, M.A., Uddin, M.N., Acharjee, U.K. (2024). Securing transactions: A hybrid dependable ensemble machine learning model using IHT-LR and grid search. Cybersecurity, 7(1): 32. https://doi.org/10.1186/s42400-024-00221-z

[27] Btoush, E., Zhou, X., Gururajan, R., Chan, K.C., Alsodi, O. (2025). Achieving Excellence in cyber fraud detection: A hybrid ML+DL ensemble approach for credit cards. Applied Sciences, 15(3): 1081. https://doi.org/10.3390/app15031081