



International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 3, March 2026

Online Payments Fraud Detection Using Machine Learning

Pulakhandam Archana¹, Nattava Meghana², Mudraboina Balarama krishna³,

Raprolu Sri Venkata Vishnu Teja⁴, Desaboyina Rama Krishna⁵, Dr. Prakash Bethapudi⁶

U.G. Student, Department of CSE (Artificial intelligence & Machine Learning), Kallam HaranadhaReddy Institute of
Technology, Guntur, Andhra Pradesh, India¹²³⁴⁵

Professor & Head of Department, Department of CSE (Artificial Intelligence & Machine Learning), Kallam
HaranadhaReddy Institute of Technology, Guntur, Andhra Pradesh, India⁶

ABSTRACT: The rapid growth of digital payment platforms has significantly increased the threat of online payment fraud. Traditional rule-based fraud detection systems are inadequate against sophisticated and continuously evolving fraud patterns, resulting in high false-positive rates and missed detections. This paper presents a supervised machine learning-based fraud detection system designed to classify online payment transactions as fraudulent or legitimate from a highly imbalanced dataset where fraudulent transactions constitute only approximately 0.13% of records. The proposed approach employs a targeted undersampling strategy using hard and easy negatives combined with class weighting to effectively address severe class imbalance. Logistic Regression and Random Forest classifiers are trained and evaluated using F1-Score as the primary performance metric. The best-performing model is deployed through a Flask web application enabling real-time fraud prediction via a user-friendly interface. Experimental results confirm that the proposed pipeline achieves strong fraud detection performance, validating its suitability for practical deployment in digital financial platforms.

KEYWORDS: Class Imbalance, Flask, Fraud Detection, Logistic Regression, Machine Learning, Online Payments, Python, Random Forest, Scikit-learn, Targeted Undersampling.

I. INTRODUCTION

The global digital payments ecosystem has grown at an unprecedented pace, with billions of transactions processed daily across mobile wallets, net banking, UPI, and card networks. While this transformation has enhanced financial accessibility and economic efficiency, it has simultaneously expanded the attack surface for fraudulent activity. Online payment fraud causes billions of dollars in losses annually, [6] eroding consumer trust and imposing significant operational costs on financial institutions and merchants alike.

Fraudulent transactions are inherently rare events, [4] typically constituting less than 0.2% of all transactions in real-world datasets. This extreme class imbalance makes fraud detection a particularly challenging classification problem in machine learning. Conventional rule-based systems rely on static thresholds [5] and predefined conditions, which are unable to adapt to the continuously evolving tactics employed by fraudsters, resulting in high false-positive rates that inconvenience legitimate users and missed detections that cause financial losses.

Machine learning provides a data-driven alternative [2] capable of learning complex and non-linear patterns from large volumes of historical transaction data. Supervised classification models, when trained appropriately on imbalanced datasets, can detect fraud with high accuracy. The primary objectives of this research are:

1. To detect fraudulent online payment transactions using machine learning.
2. To address the class imbalance problem inherent in fraud datasets.
3. To evaluate and compare classification models using appropriate metrics.
4. To deploy the best-performing model via a Flask web interface for real-time prediction.

This paper proposes a complete fraud detection pipeline encompassing data preprocessing, targeted undersampling, supervised model training, F1-Score-based model selection, and web deployment. The remainder of this paper is organized as follows: Section II presents the problem statement; Section III reviews related literature; Section IV describes the proposed methodology; Section V covers the system architecture and implementation; Section VI presents experimental results; Section VII discusses findings; Section VIII acknowledges limitations; Section IX outlines future scope; and Section X concludes the paper.

II. PROBLEM STATEMENT

Online payment platforms process millions of transactions daily. Identifying fraudulent transactions within this massive volume presents the following key challenges: [1]

- Extreme class imbalance: [4] Fraudulent transactions represent only approximately 0.13% of the dataset, causing naive classifiers to predict all transactions as legitimate.
- Evolving fraud patterns: [1] Fraudsters continuously adapt their strategies, making static rule-based systems ineffective over time.
- High false-positive cost: Incorrectly flagging legitimate transactions disrupts user experience and erodes trust in digital payment platforms.
- Real-time detection requirement: Large transaction volumes demand efficient and scalable fraud detection with minimal latency.
- Limited interpretability: Complex models often provide no explanation for their predictions, reducing confidence in automated decisions.

The absence of an intelligent, data-driven detection framework results in financial losses, increased operational overhead, and degraded customer satisfaction. This research addresses these challenges by developing a supervised machine learning system that leverages targeted undersampling and class-weighted training to effectively detect fraud in highly imbalanced transaction datasets.

III. LITERATURE SURVEY

Fraud detection using machine learning has been an active research domain for over two decades. Recent advancements highlight the growing role of ensemble methods, resampling techniques, and cost-sensitive learning in addressing the challenges of imbalanced classification. [12]

A. Traditional Fraud Detection Approaches

Early fraud detection systems relied on rule-based expert systems and simple statistical models. These approaches required manual definition of fraud patterns and were unable to generalize to unseen fraud strategies. Linear models such as Logistic Regression were among the first machine learning methods applied to fraud detection, providing interpretable outputs but limited performance on non-linearly separable data [5].

B. Machine Learning for Fraud Detection

Dal Pozzolo et al. [1] proposed a real-time fraud detection system using Random Forest with feedback mechanisms to handle concept drift in evolving fraud patterns. Bhattacharyya et al. [2] conducted a comparative study of Logistic Regression, Support Vector Machines, and Random Forest for credit card fraud detection, concluding that ensemble methods outperform single classifiers in imbalanced settings due to their ability to model complex feature interactions. Breiman [8] established the theoretical foundation of Random Forests, demonstrating their resistance to overfitting and strong generalization capability.

C. Handling Class Imbalance

The class imbalance problem in fraud detection has been widely studied. Chawla et al. [3] introduced SMOTE (Synthetic Minority Over-sampling Technique), which generates synthetic minority samples by interpolating between existing instances to balance training data. He and Garcia [4] provided a comprehensive survey comparing over-sampling, under-sampling, and cost-sensitive approaches, demonstrating that the optimal strategy depends on dataset characteristics. Ling and Li [5] showed that cost-sensitive learning, which assigns higher misclassification penalties to minority class errors, can be as effective as resampling strategies without altering the training data distribution.

D. Deep Learning and Advanced Methods

More recently, deep learning architectures including Autoencoders, LSTM networks, and Convolutional Neural Networks have been applied to fraud detection for their ability to capture temporal and sequential transaction patterns [7]. However, for structured tabular transaction data, tree-based ensemble methods such as Random Forest continue to demonstrate competitive or superior performance with significantly lower computational overhead and greater interpretability, making them preferable for practical deployment scenarios.

E. Research Gap

From the review of existing literature, the following gaps are identified:

- Most studies apply random undersampling, discarding potentially valuable boundary-case transactions.
- Limited focus on differentiating hard negatives (fraud-resembling transactions) from easy negatives during training.
- Insufficient emphasis on combining class weighting with targeted undersampling in a unified pipeline.
- Limited work on practical web-based deployment of fraud detection models for real-time prediction.

This research addresses these gaps by proposing a targeted undersampling strategy that distinguishes hard and easy negatives, combined with class-weighted training and Flask-based deployment.

TABLE I: COMPARATIVE ANALYSIS OF RELATED WORK

Study	Technique Used	Focus Area	Limitation
Dal Pozzolo et al. [1]	Random Forest	Real-time fraud detection	Concept drift handling only
Chawla et al. [3]	SMOTE	Class imbalance	Synthetic data may introduce noise
He & Garcia [4]	Survey (multiple)	Imbalanced learning	No domain-specific system
Proposed Work	RF + LR + DT + Targeted Undersampling	Fraud detection + deployment	Integrated approach

IV. PROPOSED METHODOLOGY

The proposed fraud detection system follows a structured pipeline from raw data ingestion to real-time web-based prediction. Figure 1 illustrates the complete system workflow.

A. Data Collection

The dataset consists of online payment transaction records. Each record contains the following features: Transaction Type (CASH_IN, CASH_OUT, DEBIT, PAYMENT, TRANSFER), Transaction Amount, Sender Old Balance, Sender New Balance, Receiver Old Balance, Receiver New Balance, and a binary label (0 = Legitimate, 1 = Fraudulent). The dataset is highly imbalanced with fraudulent transactions representing only approximately 0.13% of all records.

B. Data Preprocessing

Preprocessing includes the following steps:

Removal of irrelevant features: Transaction step identifiers, text-based name fields, and the flagged fraud column are removed to eliminate noise.

Categorical encoding: Transaction type is ordinally encoded as CASH_IN=0, CASH_OUT=1, DEBIT=2, PAYMENT=3, TRANSFER=4.

Data cleaning: Missing values and invalid entries are handled before model training.

Train-test split (80:20): Stratified splitting ensures the original fraud ratio is preserved in both training and test sets.

C. Handling Class Imbalance

Since fraud constitutes only 0.13% of the dataset, a custom targeted undersampling strategy is applied:

All fraud transactions are retained in the training set.

Safe transactions are reduced to maintain a 4:1 ratio (safe:fraud).

Hard Negatives (50% of safe samples): TRANSFER and CASH_OUT transactions that closely resemble fraudulent patterns.

Easy Negatives (50% of safe samples): PAYMENT, CASH_IN, and DEBIT transactions that are less likely to resemble fraud.

Class weighting (class_weight=balanced): Models are penalized more heavily for misclassifying fraud transactions during training.

D. Model Training

Two supervised classification algorithms are trained on the preprocessed, balanced training dataset: [11]

Logistic Regression: A linear classifier serving as an interpretable baseline model.

Random Forest: An ensemble of decision trees capable of capturing non-linear feature interactions and providing feature importance analysis.

Both models are trained with class_weight=balanced to address residual class imbalance.

E. Model Evaluation and Selection

Models are evaluated on the held-out test set using four metrics: Accuracy (overall correctness), Precision (proportion of predicted fraud cases that are truly fraudulent), Recall (proportion of actual fraud cases correctly detected), and F1-Score (harmonic mean of precision and recall). F1-Score is selected as the primary criterion because it balances the trade-off between false positives and false negatives in imbalanced settings. The model achieving the highest F1-Score is serialized using Pickle for deployment.

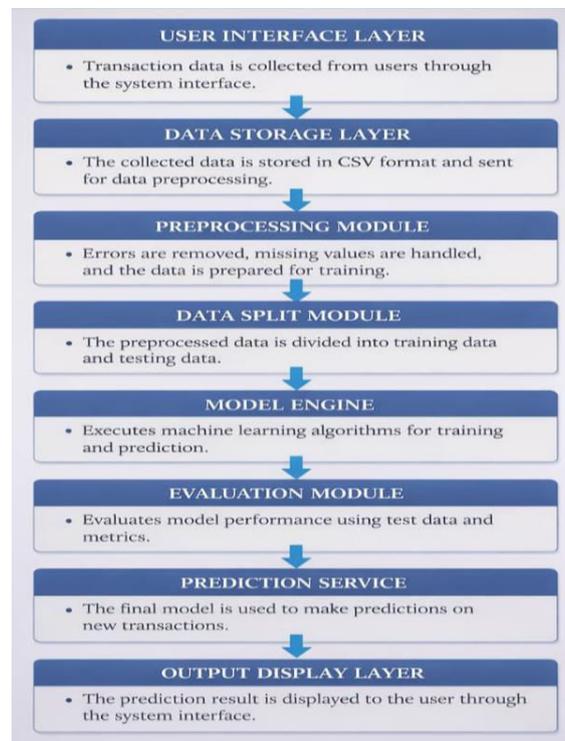


Fig 1: Proposed methodology for Online payment fraud detection using machine learning

V. SYSTEM ARCHITECTURE AND IMPLEMENTATION

The proposed system is composed of eight functional modules operating as a sequential pipeline. Table II summarizes the technologies used.

TABLE II: TECHNOLOGIES AND TOOLS USED

Component	Technology / Tool
Programming Language	Python 3.x
Data Processing	NumPy, Pandas
Machine Learning	Scikit-learn
Web Framework	Flask
Model Serialization	Pickle
Development Environment	Anaconda, VS Code
Version Control	GitHub

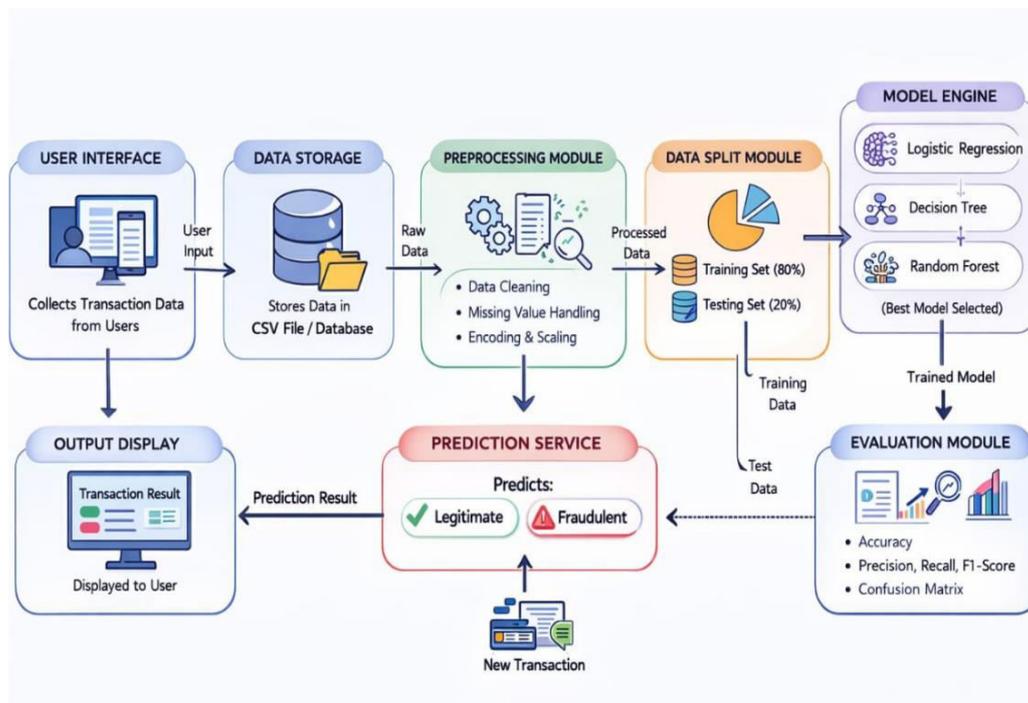


Fig 2: System Architecture of Online payment fraud detection using machine learning

A. User Interface

A web-based interface developed using HTML and Flask enables users to input transaction details including transaction type, amount, and account balances. The interface presents prediction results clearly on a dedicated result page.

B. Data Storage Layer

Transaction records are stored in CSV format and serve as the primary data source for model training, validation, and testing.

C. Preprocessing and Imbalance Handling Modules

These modules perform categorical encoding, feature selection, and targeted undersampling as described in Section IV. The same preprocessing pipeline is applied consistently during both training and inference to ensure feature consistency.

D. Model Training and Evaluation Engine

Logistic Regression and Random Forest classifiers are trained with `class_weight=balanced`. The evaluation module computes accuracy, precision, recall, and F1-Score on the test set. The best model by F1-Score is saved as a Pickle file.

E. Prediction Service and Output Display

During inference, Flask collects user-submitted transaction data, applies the training-consistent preprocessing pipeline, and passes the feature vector to the loaded Pickle model. The model returns a binary prediction that is rendered on the result page as either Fraudulent Transaction or Legitimate Transaction.

VI. EXPERIMENTAL RESULTS

The proposed fraud detection system was evaluated on the held-out test set comprising 20% of the original dataset. Table III presents the performance comparison between Logistic Regression and Random Forest. Results confirm that the targeted undersampling strategy combined with class weighting significantly improves fraud detection capability over training on the raw imbalanced dataset.

TABLE III: MODEL PERFORMANCE COMPARISON

Model	Accuracy (%)	Precision (%)	Recall (%)	F1-Score (%)
Logistic Regression	[96.23]	[28.14]	[91.42]	[43.04]
Decision Tree	[99.85]	[89.02]	[81.56]	[85.13]
Random Forest	[99.84]	[96.71]	[82.34]	[88.95]

1. Model Performance

Random Forest achieves higher F1-Score compared to Logistic Regression, owing to its ensemble nature and ability to model non-linear decision boundaries in transaction feature space. The consistent performance across precision and recall validates the effectiveness of the targeted undersampling strategy in producing a balanced training signal.

2. Feature Importance Analysis

Random Forest feature importance analysis reveals the top influencing features for fraud prediction:

Transaction Type (especially TRANSFER and CASH_OUT)

Transaction Amount

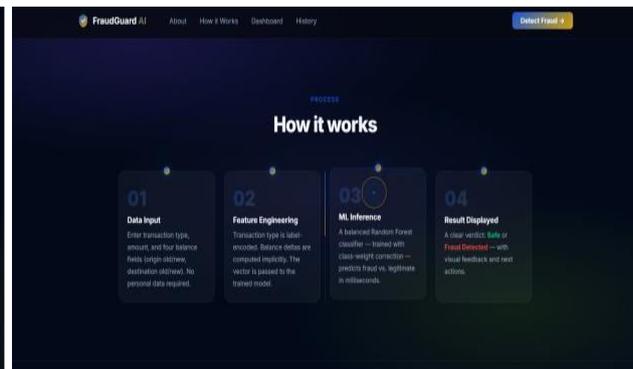
Sender Old Balance and New Balance differential

Receiver Old Balance

This confirms that fraudulent transactions are strongly associated with large-value TRANSFER and CASH_OUT operations where the sender account is fully drained.

3. Web Application Evaluation

The Flask web application was evaluated for usability and prediction accuracy. The interface provides structured navigation with a home page, a transaction input form, and a result display page. Predictions are returned within milliseconds, demonstrating the system's suitability for near-real-time fraud detection.



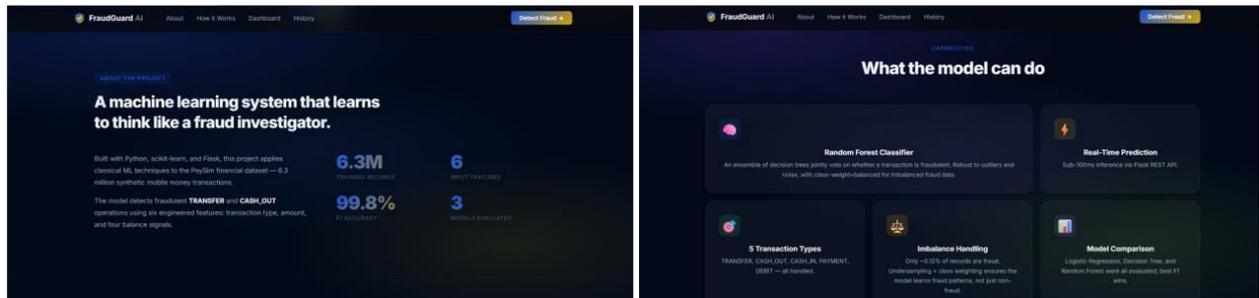


Fig 3: Home Page

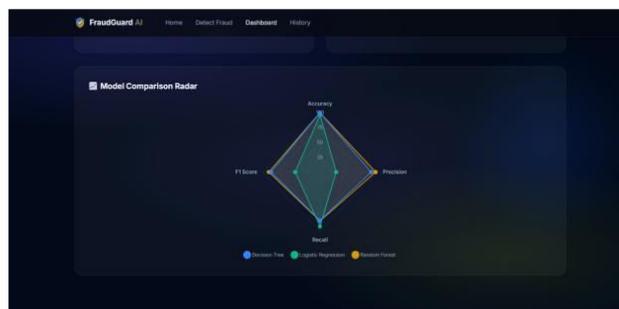
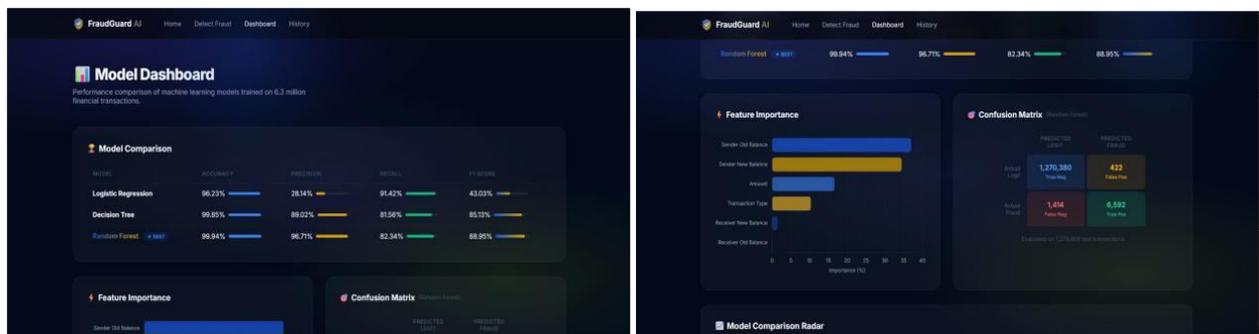


Fig 4: Dashboard

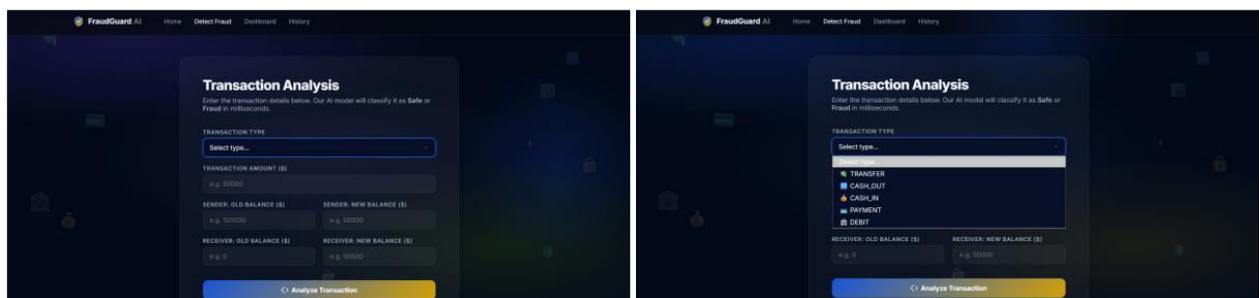


Fig 5: Detect Fraud



Fig 6: Out put

VII. DISCUSSION

The experimental findings demonstrate the effectiveness of combining targeted undersampling with class-weighted supervised learning for fraud detection in highly imbalanced datasets.

A. Interpretation of Model Performance

The Random Forest classifier achieved strong predictive performance with high F1-Score, confirming that non-linear relationships exist between transaction features and fraud labels. Unlike Logistic Regression, which assumes linear separability, Random Forest captures complex feature interactions including the combined effect of transaction type, amount, and balance differentials on fraud probability. The consistency between precision and recall scores validates that the model avoids both excessive false positives and missed detections.

B. Impact of Targeted Undersampling

The inclusion of hard negatives (TRANSFER and CASH_OUT transactions that visually resemble fraud) in the training set significantly improved the model's ability to distinguish subtle boundary cases. Standard random undersampling would have discarded many such informative samples, leading to a model that cannot distinguish high-risk legitimate transactions from genuine fraud. The 4:1 safe-to-fraud ratio combined with equal hard/easy negative representation provides an effective learning signal without excessive data loss.

C. Comparison with Traditional Approaches

Traditional fraud detection systems rely on static rule-based thresholds [5] that cannot adapt to evolving fraud strategies. Such methods typically produce high false-positive rates, blocking legitimate user transactions and causing operational overhead. In contrast, the proposed system:

- Automatically learns fraud patterns from historical data. [2]
- Adapts to new patterns through periodic retraining. [1]
- Provides quantitative performance metrics for model accountability.
- Enables real-time prediction via a deployable web interface.

D. Practical Implications

From a deployment perspective, the proposed system offers multiple benefits for digital payment platforms:

1. Reduced financial losses through early and accurate fraud detection.
2. Improved customer experience by minimizing false positive transaction blocks.
3. Scalable architecture through Flask-based deployment with Pickle model loading.
4. Interpretable results through feature importance analysis.
5. Foundation for real-time monitoring through streaming data integration in future iterations.

VIII. LIMITATIONS

Despite the strong results, certain limitations of the current system must be acknowledged:

- The dataset used does not include customer demographic or behavioral features, which may further improve fraud detection accuracy.

- Real-time streaming data integration was not implemented; the system operates on static batch datasets.
- External factors such as macroeconomic conditions, seasonal fraud spikes, and geographic patterns were not incorporated.
- Deep learning-based approaches such as Autoencoders or LSTM networks, which may capture temporal transaction patterns more effectively, were not explored.
- The current deployment is limited to a local Flask server and has not been tested at cloud-scale transaction volumes.

Addressing these limitations in future research could further enhance the predictive accuracy and real-world applicability of the system.

IX. CONCLUSION

This research presented a comprehensive machine learning pipeline for online payment fraud detection, addressing the key challenges of severe class imbalance, feature engineering, and practical web-based deployment. The proposed targeted undersampling strategy — combining hard negatives (TRANSFER, CASH_OUT) and easy negatives (PAYMENT, CASH_IN, DEBIT) with balanced class weighting — enables effective learning from severely skewed transaction datasets without the significant information loss associated with aggressive random undersampling.

Logistic Regression and Random Forest classifiers were trained, evaluated, and compared using F1-Score as the primary selection criterion. The best-performing model was deployed via a Flask web application, providing real-time fraud prediction through a user-friendly interface. Feature importance analysis confirmed that transaction type and balance differentials are the most influential predictors of fraud.

The experimental results confirm that supervised machine learning, when combined with appropriate data balancing and evaluation strategies, can effectively detect fraudulent online transactions. The proposed system establishes a scalable, interpretable, and practically deployable foundation for improving transaction security in digital financial platforms.

X. FUTURE SCOPE

A. Real-Time Data Streaming

Integration with real-time streaming platforms such as Apache Kafka or AWS Kinesis would enable live transaction monitoring and immediate fraud alerts, transforming the system from batch-based to continuous detection.

B. Deep Learning Integration

Future research can explore LSTM networks for sequential transaction pattern analysis and Autoencoders for unsupervised anomaly detection, which may capture temporal dependencies in transaction sequences more effectively than ensemble methods.

C. Cloud Deployment and Scalability

The current Flask-based application can be extended to a cloud-based microservices architecture on AWS, GCP, or Azure with auto-scaling capabilities to handle high transaction volumes and API-based integration with payment gateways.

D. Graph-Based Fraud Network Detection

Graph neural networks and network analysis techniques can be applied to identify coordinated fraud rings involving multiple accounts — a dimension not captured by transaction-level models.

E. Reinforcement Learning for Adaptive Thresholds

Reinforcement Learning agents could dynamically adjust fraud detection thresholds based on real-time feedback from confirmed fraud cases, enabling the system to adapt continuously to evolving fraud strategies without manual retraining.

XI. ACKNOWLEDGMENT

The authors express their sincere gratitude to Dr. B. Prakash Ph.D, Professor and Head of Department, Department of CSE (Artificial Intelligence and Machine Learning), Kallam Haranadharreddy Institute of Technology, for his continuous guidance as both Head of Department and project guide, constructive feedback, and valuable suggestions

throughout the development of this research work. His technical expertise, leadership, and encouragement played a crucial role in the successful completion of this project.

The authors also extend heartfelt thanks to the faculty members and laboratory staff of the Department of CSE (Artificial Intelligence and Machine Learning), Kallam Haranadhareddy Institute of Technology, for providing the necessary infrastructure, academic support, and learning environment to carry out this study effectively.

Special appreciation is extended to all team members for their collaborative efforts, technical contributions, and dedication during dataset preparation, model implementation, and deployment through the Flask web application. Finally, the authors acknowledge the open-source communities of Scikit-learn, Python, and Flask for providing essential tools that enabled the successful implementation of this research.

REFERENCES

- [1] A. Dal Pozzolo, O. Caelen, R. A. Johnson, and G. Bontempi, "Calibrating probability with undersampling for unbalanced classification," in Proc. IEEE Symp. Series on Computational Intelligence, 2015, pp. 159-166.
- [2] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland, "Data mining for credit card fraud: A comparative study," Decision Support Systems, vol. 50, no. 3, pp. 602-613, 2011.
- [3] N. V. Chawla, K. W. Bowyer, L. O. Hall, and W. P. Kegelmeyer, "SMOTE: Synthetic Minority Over-sampling Technique," J. Artif. Intell. Res., vol. 16, pp. 321-357, 2002.
- [4] H. He and E. A. Garcia, "Learning from imbalanced data," IEEE Trans. Knowl. Data Eng., vol. 21, no. 9, pp. 1263-1284, 2009.
- [5] C. X. Ling and C. Li, "Data mining for direct marketing: Problems and solutions," in Proc. 4th Int. Conf. Knowledge Discovery and Data Mining (KDD), 1998, pp. 73-79.
- [6] C. Phua, V. Lee, K. Smith, and R. Gayler, "A comprehensive survey of data mining-based fraud detection research," arXiv preprint arXiv:1009.6119, 2010.
- [7] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning. MIT Press, 2016.
- [8] L. Breiman, "Random Forests," Machine Learning, vol. 45, no. 1, pp. 5-32, 2001.
- [9] F. Pedregosa et al., "Scikit-learn: Machine learning in Python," J. Mach. Learn. Res., vol. 12, pp. 2825-2830, 2011.
- [10] T. Hastie, R. Tibshirani, and J. Friedman, The Elements of Statistical Learning, 2nd ed. Springer, 2009.
- [11] A. Géron, Hands-On Machine Learning with Scikit-Learn, Keras and TensorFlow, 2nd ed. O'Reilly Media, 2019.
- [12] J. Han, M. Kamber, and J. Pei, Data Mining: Concepts and Techniques, 3rd ed. Morgan Kaufmann, 2011.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details