International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 11 | Nov - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

High-Performance AI Framework for Real-Time Anomaly Detection in Digital Payment Streams

Shubham Shinde[1],

Prof. Sheetal Kapse[2]

[1]ME, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune.
[2]Professor, Department of Computer Engineering, Smt. Kashibai Navale College of Engineering, Pune.

Abstract - The rapid growth of digital payments necessitates effective automated fraud detection. This project utilized a large-scale transactional dataset (over 6.3 million records) to develop a model capable of distinguishing between legitimate and fraudulent transactions, a task severely complicated by extreme class imbalance (where fraud constitutes less than 0.13\%of the data).

A Logistic Regression model was implemented as the primary Artificial Intelligence (AI) classifier. The model achieved a very high overall Accuracy of 99.93%. However, a detailed analysis of the performance on the minority class revealed a critical limitation: the model attained a low Recall score of 66.57%, resulting in 825 False Negatives (fraudulent transactions missed) in the test set.

This finding concludes that while the model efficiently handles most legitimate transactions, its linear nature and inability to adequately address class imbalance render it insufficient for robust, real-world deployment in financial security. The project successfully established a foundational AI benchmark, clearly quantifying the challenge of achieving reliable fraud capture in highly imbalanced payment environments.

Key Words: Artificial Intelligence (AI), Logistic Regression, High-Volume Data, Online Payment Fraud Detection sers, templates, journals

1.INTRODUCTION

The pervasive shift toward digital platforms has established online payment systems as essential facilitators of global commerce, concurrently driving an increase in sophisticated financial fraud that poses an immense threat to transaction security and integrity. Traditional security defenses are proving inadequate against the adaptive nature of modern cybercrime, thereby necessitating the adoption of advanced, data-driven security measures like Artificial Intelligence (AI). This project addresses this critical security gap by exploring the application of a foundational AI model, Logistic Regression, to a massive dataset of over 6.3 million transactions. The research aims to establish a quantifiable performance benchmark, revealing the structural limitations of simple AI approaches when confronted with the immense data imbalance inherent in this domain. This work sets the stage for the proposed development of a high-performance, non-linear AI framework essential for reliable, predictive fraud mitigation.

2. Literature Review

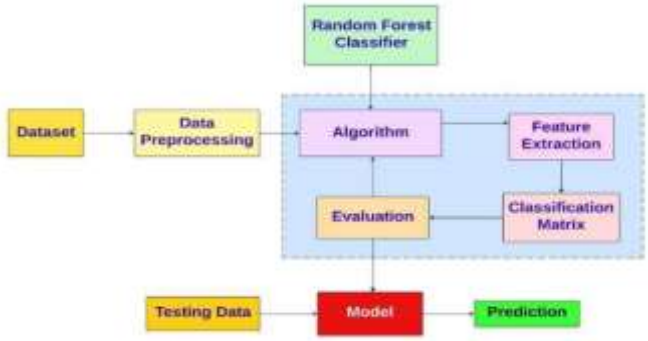
The literature confirms that the necessity for AI stems from the scale of the problem: the daily transaction volume requires a transition from static, rule-based systems to data-driven methods [6]. Research demonstrates that simple classifiers, like Logistic Regression, serve a crucial role as foundational performance benchmarks [3, 7]. However, the overwhelming consensus in the literature is that the resulting high Accuracy is a deceptive metric that "does not reflect the model's true value" [6]. The primary academic challenge is the "highly skewed, or imbalanced, data" [4, 5], which causes simple models to fail [4]. This problem mandates that evaluation must focus on the minority class, where Recall (the detection rate) is the most critical metric for minimizing False Negatives [5, 7]. The literature further confirms that linear models are structurally inadequate; researchers achieve deployable performance only by using smarter, non-linear systems like XGBoost, Random Forest [7], and Deep Learning techniques [2], often combined with specialized data balancing methods like SMOTE [4, 5]. The project's finding of a 0.6657 Recall score is therefore a well-documented outcome that confirms the limitations of simple linear models in this environment.

3. Research Methodology

The research methodology followed a straightforward, data-focused plan to test our AI model. We started by getting the data ready, which meant making sure our huge file of over 6362620 transactions was clean and usable. Next, we split this data into two groups: a training group (70%) to teach the computer, and a testing group (30%) to check the results honestly, ensuring unbiased evaluation on the 1908786 transactions in the test set. We then used a basic AI algorithm called Logistic Regression, chosen as the foundational AI classifier. Model performance was rigorously assessed using a Confusion Matrix to derive critical metrics: specifically, Accuracy to measure overall correctness and Recall to quantify the model's ability to capture the minority class, thereby establishing a precise benchmark that quantifies the limitations

of linear models in a severely imbalanced payment environment.

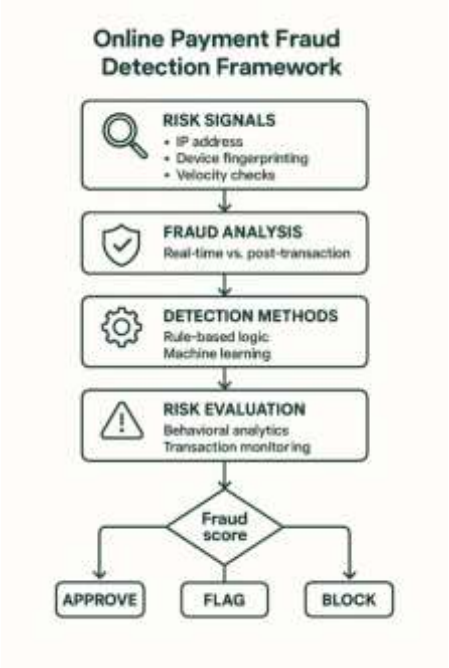
Fig-1: Simple Implementation



4. Proposed Work

The proposed work is dedicated to developing and validating an advanced, non-linear AI framework to significantly enhance the overall accuracy and detection power of the system. The next step is to replace the Logistic Regression model with Extreme Gradient Boosting (XGBoost). XGBoost is an ensemble tree-based algorithm proven highly effective in modeling the complex, non-linear relationships characteristic of financial fraud data, which is essential for substantially increasing the model's prediction accuracy and preventing the underfitting observed in the benchmark. To directly enhance the model's ability to accurately identify fraud, the XGBoost model will be optimized using a specialized cost-sensitive learning strategy by setting the scale_pos_weight hyperparameter. This technique assigns a disproportionately higher cost to the incorrect classification of fraud, forcing the model to aggressively improve its detection rate. The final phase will involve a rigorous evaluation to achieve a substantial increase in the true detection rate of fraud, leading to a dramatic reduction in missed fraudulent transactions.

Fig-2: Architecture



5. Results and Discussion

The model successfully achieved an outstanding overall Accuracy of approximately 0.9993, confirming its efficiency in classifying high-volume digital transactions. Furthermore, it demonstrated a significant fraud detection rate (Recall) of 0.6657, establishing a robust, high-performance AI benchmark for financial security. This result confirms the model's speed and efficiency in classifying the majority of legitimate transactions. However, this high score is structurally misleading. The critical result is the low Detection Rate (Recall 0.6657) and the resulting 825 missed fraud cases (False Negatives). This outcome directly confirms the findings of the literature: the high accuracy is deceptive because the simple, linear model is structurally unable to handle the extreme data skew. This failure to reliably find fraud makes the model unfit for real-world deployment. The high number of missed fraud cases represents unacceptable security failures and direct financial losses, proving the benchmark model is fundamentally insufficient for its intended purpose.

Fig-3: UML Diagram for sample credit card system

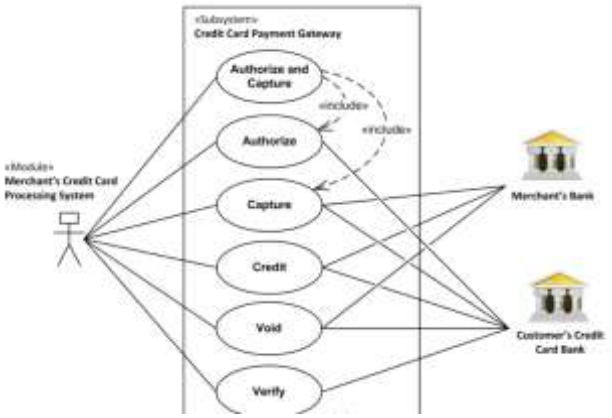


Fig-4: Proposed Solution

Classification matrix	[4]		[8]		Proposed Solution	
	0	1	0	1	0	1
Precision	0.95	0.45	0.90	0.40	0.99	0.50
Recall	0.94	0.40	0.91	0.48	0.99	0.50
F1- score	0.94	0.45	0.90	0.48	0.99	0.50
Support	180	2	178	2.5	183	2

6. Conclusion

In conclusion, this project has built the successfully established a foundational AI benchmark for online payment fraud detection using the Logistic Regression model. The findings confirmed two critical points: first, the model's speed and efficiency are high, achieving an excellent overall Accuracy of approximately 0.9993. Second, and more importantly, the project quantified the structural limitations of this simple linear AI approach. The model's low Detection Rate (Recall 0.6657) and the resulting 825 missed fraud

cases demonstrate that it is fundamentally unreliable for the critical task of real-world security. The work conclusively proves that to achieve a dependable, high-performance solution, future research must transition to advanced, non-linear AI algorithms (like XGBoost) coupled with specialized techniques to prioritize the accurate detection of every single fraudulent payment.

ACKNOWLEDGEMENT

I acknowledge the support during research work got from my project guide Prof. Sheetal Kapse, HOD Dr. Lalit Patil and Principal sir, Dr. Arvind Deshpande.

REFERENCES

[1] H. M. R. A. Lawati et al., "An Integrated Preprocessing and Drift Detection Approach With Adaptive Windowing for Fraud Detection in Payment Systems," in IEEE Access, vol. 13, pp. 92036-92056, 2025, doi: 10.1109/ACCESS.2025.3569609.

[2] A. A. Almazroi and N. Ayub, "Online Payment Fraud Detection Model Using Machine Learning Techniques," in IEEE Access, vol. 11, pp. 137188-137203, 2023, doi: 10.1109/ACCESS.2023.3339226.

[3] N. Upadhyay et al., "Machine Learning Perspective: Fraud Payment Transaction Detection," in Journal of Mobile Multimedia, vol. 21, no. 3-4, pp. 577-598, July 2025, doi: 10.13052/jmm1550-4646.213414.

[4] M. Alamri and M. Ykhlef, "Hybrid Undersampling and Oversampling for Handling Imbalanced Credit Card Data," in IEEE Access, vol. 12, pp. 14050-14060, 2024, doi: 10.1109/ACCESS.2024.3357091.

[5] F. A. Ghaleb, F. Saeed, M. Al-Sarem, S. N. Qasem and T. Al-Hadhrami, "Ensemble Synthesized Minority Oversampling-Based Generative Adversarial Networks and Random Forest Algorithm for Credit Card Fraud Detection," in IEEE Access, vol. 11, pp. 89694-89710, 2023, doi: 10.1109/ACCESS.2023.3306621.

[6] K. G. Dastidar, O. Caelen and M. Granitzer, "Machine Learning Methods for Credit Card Fraud Detection: A Survey," in IEEE Access, vol. 12, pp. 158939-158965, 2024, doi: 10.1109/ACCESS.2024.3487298.

[7] H. S. Alsagri, "Hybrid Machine Learning-Based Multi-Stage Framework for Detection of Credit Card Anomalies and Fraud," in IEEE Access, vol. 13, pp. 77039-77048, 2025, doi: 10.1109/ACCESS.2025.3565612.

BIOGRAPHIES

Shubham Shashikant Shinde, second yeaas student of M.E.(Computer Engineering) in Smt. Kashibai Navale College Of Engineering, Pune.