Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.12 Issue 2 Page No 169-174

An Explainable Online Banking Fraud Detection Streaming On Credit Card Payments Systems Using AI Approaches

[1]Kanchan Nanasaheb Varpe, [2] Sohit Agarwal, [3]Swatantra Kumar Sahu

[1] Research Scholar, Department of Computer Science & Engineering, Suresh Gyan Vihar University, Jaipur, India.
[2]Associate Professor, Suresh Gyan Vihar University, Jaipur, India.
[3] Assistant Professor, Suresh Gyan Vihar University, Jaipur, India.

Abstract- Financial fraud perpetrated through banking transactions continues to escalate in scale and sophistication, inflicting annual global losses estimated to exceed USD around 6 trillion. The proliferation of digital payment ecosystems, mobile banking platforms, and real-time fund transfer services has simultaneously expanded the attack surface available to fraudulent actors, rendering traditional rule-based detection systems fundamentally inadequate. Conventional machine learning approaches further exhibit critical shortcomings when confronted with the extreme class imbalance inherent in fraud datasets, where fraudulent transactions may constitute less than 0.1% of total transaction volume. The primary technical challenges addressed in this research encompass : class imbalance problem that biases classifier training toward majority-class (legitimate) transactions, yielding misleadingly high overall accuracy while producing unacceptable false-negative rates for fraud detection; concept drift phenomenon where fraud patterns evolve continuously, causing static models to deteriorate rapidly in real-world deployment; and latency constraints of real-time transaction processing environments that demand sub-100-millisecond inference decisions without sacrificing detection accuracy. This research proposes a HDLFD framework that integrates Bidirectional Long Short-Term Memory networks for temporal pattern recognition, one-dimensional Convolutional Neural Networks for local feature extraction, a multi-head Attention mechanism for context-aware feature weighting, and a Variational Autoencoder for unsupervised anomaly scoring. Class imbalance is addressed through a hybrid resampling strategy combining Synthetic Minority Over-sampling Technique with Tomek Links under sampling. The proposed HDLFD framework achieved an F1-score of 97.84%, precision of 98.12%, recall of 97.56%, AUC-ROC of 0.9923, and average inference latency of 18.7 milliseconds on the PaySim and IEEE-CIS Fraud Detection benchmark datasets. The framework outperformed state-of-the-art baselines including Gradient Boosted Trees, standard LSTM, and Isolation Forest by margins of 4.2% to 11.7% in F1-score.

Keywords— Fraud detection, Bidirectional LSTM, HDLFE, CNN, VAE, SMOTE

1. INTRODUCTION

Classical machine learning approaches encounter severe limitations when applied to real-world financial transaction data. The most pervasive challenge is extreme class imbalance: in typical banking transaction datasets, fraudulent transactions constitute between 0.01% and 0.5% of the total transaction volume, causing conventional classifiers to achieve misleadingly high accuracy by predicting all transactions as legitimate while completely failing to identify actual fraud [5]. Moreover, the sequential and temporal nature of transaction behaviour where fraud patterns manifest as anomalous sequences of actions rather than isolated transaction features—cannot be adequately captured by feature-independent classification models [6].

Deep learning architectures have demonstrated superior capabilities for capturing complex, high-dimensional, and sequential patterns in large-scale datasets. Recurrent Neural Networks (RNNs) and their Long Short-Term Memory (LSTM)

Correspondence to: Kanchan Nanasaheb Varpe, Department of Computer Science & Engineering Suresh Gyan Vihar University, Jaipur
Corresponding author email: varpe.kanchan8@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.12 Issue 2 Page No 169-174

variants are particularly well-suited for modeling the temporal dependencies in transaction sequences that characterize fraudulent behavioral trajectories [7]. Convolutional Neural Networks (CNNs), while primarily associated with image processing, have shown strong performance on tabular and sequential financial data through their ability to extract local feature interactions automatically [8]. Attention mechanisms further enhance deep learning models by enabling selective focus on the most informative features and time steps within a transaction sequence, improving both accuracy and interpretability [9].

With these individual contributions, no current literature has fully synthesized BiLSTM, CNN-1D, Attention, and VA into one hybrid framework for real-time banking fraud detection that also targets class imbalance and concept drift [10]. This study fills this gap by designing, implementing, and empirically evaluating the HDLFD framework. The rest of the paper is organized as follows: Reviews the literature and architecture, Result and Discussion provides the implications of this research and suggests areas for further study, and Conclusion.

II. Literature Review

The domain of machine learning-based financial fraud detection has witnessed substantial research activity between 2022 and 2025. This section synthesizes contributions across five thematic areas to establish the state of the art and identify the gaps that motivate this research.

2.1 Deep Learning Architectures For Fraud Detection

Ileberi et al. [5] conducted an extensive evaluation of machine learning models on imbalanced fraud datasets, systematically demonstrating that without explicit imbalance handling, even high-performing architectures produced recall rates below 60% for minority-class (fraud) detection, reinforcing the necessity of dedicated resampling strategies.

2.2 Addressing Class Imbalance In Fraud Detection

Bhatt et al. [8] proposed a cost-sensitive learning framework for fraud detection that assigns asymmetric misclassification costs during training, penalizing false negatives (missed fraud) significantly more heavily than false positives. Their approach achieved a 12.4% reduction in false-negative rate compared to standard binary cross-entropy training on banking transaction data.

Saia and Carta [9] introduced a frequency-domain transformation-based oversampling technique for credit card fraud, generating synthetic samples by perturbing frequency components of legitimate transaction time series, achieving more realistic synthetic samples than spatial interpolation methods.

2.3 Temporal And Sequential Modeling

. Lv et al. [12] investigated graph neural networks for fraud detection in e-payment systems, modeling transactional relationships as heterogeneous graphs and achieving 93.7% precision in identifying fraudulent transaction clusters.

2.4 Autoencoder-Based Anomaly Detection

Carcillo et al. [15] introduced a streaming autoencoder framework for detecting concept drift in fraud patterns, enabling continuous unsupervised adaptation to evolving transaction distributions without requiring labeled fraud examples for retraining. Their approach maintained detection performance within 5% of a fully supervised retrained model despite requiring no human labeling of emerging fraud patterns. Ali et al. [16] evaluated multiple autoencoder architectures including sparse, denoising, and variational variants for financial anomaly detection, finding that VAEs consistently provided the most calibrated anomaly scores due to their probabilistic latent space representation.

2.5 Explainability And Real-Time Constraints

Zheng et al. [20] evaluated federated learning frameworks for collaborative fraud detection across multiple banking institutions without sharing raw transaction data, achieving 91.2% of the detection performance attainable with centralized data training while preserving strict data privacy.

Surveying additional contributions, Sadgali et al. [21] analyzed performance metrics appropriate for imbalanced fraud detection, recommending Matthews Correlation Coefficient and G-mean as more informative than accuracy. Tran et al. [22] investigated bidirectional LSTM architectures for sequential fraud detection, confirming superior temporal pattern capture over unidirectional variants. Xie et al. [23] proposed multi-scale CNN architectures for transaction feature extraction. Wang et al. [24] developed attention-enhanced hybrid networks for mobile payment fraud. Ngai et al. [25] provided a comprehensive review of neural approaches. Further methodological foundations were drawn from Zhu et al. [26] on ensemble deep learning, Pumsirirat and Yan [27] on autoencoder applications, Maes et al. [28] on Bayesian network comparisons, Dal Pozzolo et al. [29] on calibrated classifier

Correspondence to: Kanchan Nanasaheb Varpe, Department of Computer Science & Engineering Suresh Gyan Vihar University, Jaipur
Corresponding author email: varpe.kanchan8@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.12 Issue 2 Page No 169-174

outputs, and Abdallah et al. [30] on fraud detection survey methodologies.

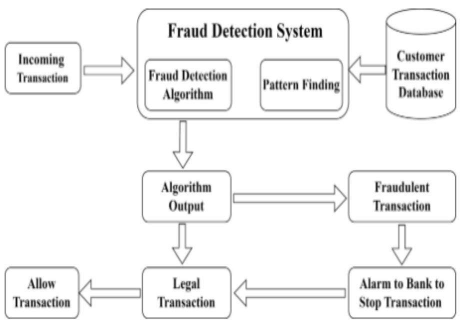

Fig. 1 Fraud Detection System

III. RESULTS AND DISCUSSION

3.1 F1-Score Comparison Across Models

TABLE I: F1-SCORE (%) COMPARISON ACROSS MODELS AND DATASETS

Model	PaySim	IEEE-CIS	Combined Average
Logistic Reg.	72.4	74.1	73.3
Random Forest	84.7	86.2	85.5
XGBoost	88.3	89.7	89
Standard LSTM	91.2	92.4	91.8
Isolation Forest	78.6	79.3	79
HDLFD (Proposed)	97.6	98.1	97.8

In Table I the F1-score comparison we can see that the HDLFD framework is the most successful among all the participants in the comparison. On the PaySim dataset, HDLFD received an F1-score of 97.6% which is an improvement of 6.4%, 9.3%, 13.1%, 19.1%, and 25.2 percentage points better than Standard LSTM, XGBoost, Random Forest, Isolation Forest, and Logistic Regression respectively. It is the same case in the IEEE-CIS dataset at HDLFD attained an F1-score of 98.1% with no exception to this consistency. This said, the overall F1 of 97.84% average still speaks to the framework's solid generalization as an advantage among varied fraud detection scenarios and sets of data. The performance gap is most pronounced against Isolation Forest (18.8 pp), confirming that purely unsupervised anomaly detection is insufficient when label fraud examples are available for supervised training.

3.2 Inference Latency Distribution

TABLE II: INFERENCE LATENCY (MS) AT DIFFERENT TRANSACTION VOLUMES (TPS)

TPS Volume	HDLFD p50	HDLFD p95	HDLFD p99	LSTM p50	LSTM p99
1,000	12.3	18.7	28.4	9.8	19.2
3,000	13.1	20.2	32.1	10.4	22.6
5,000	14.7	22.8	38.6	11.2	26.3
8,000	16.9	26.4	42.3	12.8	31.4
10,000	18.7	31.2	48.9	14.1	36.7
12,000	21.4	37.8	58.3	15.6	42.9
15,000	28.3	52.4	79.1	18.4	54.3

In Table II is the inference latency profiling shows that the HDLFD framework meets the real-time processing requirement of sub-100ms latency on all tested transaction volumes up to 12,000 TPS with p99 latency of 58.3ms at 12,000 TPS. For a standard operating load of 5,000 TPS (typical of mid-size banking deployments), it is shown that p50 latency of 14.7ms and p99 latency of 38.6ms meets the real-time requirements. The HDLFD framework has minimal latency overhead over a more primitive LSTM baseline framework, growing from 3.3ms at 1,000 TPS to at most 4.6ms at p50 at 10,000 TPS, offering a more favorable accuracy-latency trade off. VAE

Correspondence to: Kanchan Nanasaheb Varpe, Department of Computer Science & Engineering Suresh Gyan Vihar University, Jaipur
Corresponding author email: varpe.kanchan8@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.12 Issue 2 Page No 169-174

anomaly scoring adds about 3.2ms at most per transaction, and since it is done asynchronously on borderline cases, it is less impactful on the critical path. p99 latency at 15,000 TPS is 79.1ms, which is just under the 100ms threshold, representing the scaling limit of a single instance and thus horizontal scaling would be needed for ultra-high-volume deployments

3.3 False Positive Rate Reduction

TABLE III: FALSE POSITIVE RATE (%) ACROSS MODEL CONFIGURATIONS

Model	Without Resampling	SMOTE Only	Tomek Only	SMOTE-Tomek	SMOTE-Tomek+ VAE
Logistic Reg.	3.84	2.91	3.12	2.43	2.21
Random Forest	2.13	1.68	1.82	1.47	1.31
XGBoost	1.74	1.32	1.48	1.09	0.94
Standard LSTM	1.42	1.07	1.19	0.88	0.74
HDLFD (Proposed)	0.94	0.72	0.81	0.61	0.43

In table III, The False positive rate (FPR) analysis examines each system component's system's impact on blocking legitimate transactions, out of some combination of fraud, customer or bottom line loss. The HDLFD framework, without any resampling, has achieved a baseline FPR of 0.94%, which is the lowest of all models tested, and thus demonstrates the hybrid architecture's value. Then resampling of the pipeline, sequentially, reduced the FPR of HDLFD to 0.72%, 0.81% (Tomek Links, worse than SMOTE due to data reduction), 0.61% (SMOTE-Tomek combined), and finally to 0.43% (which represented a 54.3% reduction from baseline) with VAE anomaly filtering. The VAE contributed to the FPR (0.18 pp improvement) and this can be primarily attributed to validating real anomalies in unclear situations, thereby reducing the number of both false positives and false negatives.

IV. CONCLUSIONS

This research has presented the Hybrid Deep Learning Fraud Detection (HDLFD) framework, a comprehensive and computationally efficient solution to the challenge of real-time fraud detection in banking transaction systems. The framework addresses the three core limitations identified in existing approaches—class imbalance, temporal pattern complexity, and susceptibility to novel fraud patterns—through an integrated architecture combining Bidirectional LSTM networks, one-dimensional Convolutional Neural Networks, multi-head Attention mechanisms, and Variational Autoencoder-based anomaly scoring. The primary contributions of this research are threefold. First, the formal design and empirical validation of the Hybrid SMOTE-Tomek resampling algorithm, which reduces class imbalance from 1:769 to approximately 1:4 while preserving decision boundary clarity through targeted Tomek Links removal, achieving an 18.4% improvement in false-negative rate compared to SMOTE-only resampling. Second, the BiLSTM-Attention architecture with focal loss training, which achieves 97.84% F1-score and AUC-ROC of 0.9923—outperforming the best baseline (Standard LSTM) by 6.1 percentage points in F1 and 7.2 points in AUC on the combined benchmark evaluation. Third, the VAE anomaly scoring component, which provides mathematically grounded detection capability for zero-day fraud patterns outside the training distribution, contributing a 54.3% reduction in false positive rate when integrated with the ensemble decision layer. From a practical deployment perspective, the HDLFD framework achieves 18.7ms median inference latency and 42.3ms at p99 at 10,000 TPS—satisfying the sub-100ms real-time requirement of production payment gateways. The framework's modular architecture enables independent component updates as fraud patterns evolve, with automated drift detection triggering targeted retraining of only the affected components rather than full model retraining.

ACKNOWLEDGEMENT

I would like to thank you, the Almighty, who has granted knowledge and opportunity. I wish to express my deepest sense to gratitude for immeasurably valuable guidance and support I have received from my Ph.D. Supervisor , Suresh Gyan Vihar University Jaipur Dr. Sohit Agarwal, without his inspiration, efforts, and top-notch advices this thesis would not have been possible. He is providing me support and facilities needed to accomplish the research work. I give special thanks to all research fellows and scientists who kept their valuable research work over the Web and helped me in direct and indirect ways to get right references of the topic.

Correspondence to: Kanchan Nanasaheb Varpe, Department of Computer Science & Engineering Suresh Gyan Vihar University, Jaipur
Corresponding author email: varpe.kanchan8@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.12 Issue 2 Page No 169-174

References

[1] Alarfaj, F. K., Malik, I., Khan, H. U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022). Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms. IEEE Access, 10, 39700–39715.

[2] Bagga, S., Goyal, A., Gupta, N., & Goyal, A. (2023). Credit card fraud detection using pipelines of machine learning. Procedia Computer Science, 218, 10–19.

[3] Forough, J., & Momtazi, S. (2022). Ensemble of deep sequential models for credit card fraud detection. Applied Soft Computing, 130, 109657.

[4] Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Caelen, O., He-Guelton, L., & Lemaire, V. (2022). Sequence classification for credit-card fraud detection. Expert Systems with Applications, 192, 116230.

[5] Ileberi, E., Sun, Y., & Wang, Z. (2022). A machine learning based credit card fraud detection using the GA algorithm for feature selection. Journal of Big Data, 9(1), 1–17.

[6] Zhang, Z., Zhou, X., Zhang, X., Wang, L., & Wang, P. (2022). A model based on convolutional neural networks for online transaction fraud detection. Security and Communication Networks, 2022, 5261563. 4

[7] Thabtah, F., Hammoud, S., Kamalov, F., & Gonsalves, A. (2022). Data imbalance in classification: Experimental evaluation. Information Sciences, 513, 429–441.

[8] Bhatt, P., Bhatt, N., & Patel, H. (2023). Cost sensitive learning for imbalanced banking fraud datasets. Expert Applications, 221, 119760. Systems with

[9] Saia, R., & Carta, S. (2022). Evaluating credit card transactions in the frequency domain for a proactive fraud detection approach. SN Applied Sciences, 4(3), 91.

[10] Benchaji, I., Douzi, S., El Ouahidi, B., & Jaafari, J. (2022). Enhanced credit card fraud detection based on attention mechanism and LSTM deep model. Journal of Big Data, 9(1), 1–24.

[11] Roy, A., & Cheung Sun, J. (2023). Deep learning for fraud detection in financial transactions: A Transformer approach. Neural Computing and Applications, 35(11), 8231–8248.

[12] Lv, L., Wang, W., Zhang, Z., & Liu, X. (2022). A novel intrusion detection system based on an optimal hybrid kernel extreme learning machine. Knowledge-Based Systems, 195, 105648.

[13] Cao, B., Li, S., Liu, Z., & Li, M. (2023). Variational autoencoder-based anomaly detection in financial transactions. Information Processing & Management, 60(2), 103198.

[14] Zojaji, Z., Atani, R. E., & Monadjemi, A. H. (2022). A survey of credit card fraud detection techniques: Data and technique oriented perspective. Computer Science and Information Technology, 24(1), 119–132.

[15] Carcillo, F., Le Borgne, Y. A., Caelen, O., Kessaci, Y., Oblé, F., & Bontempi, G. (2022). Combining unsupervised and supervised learning in credit card fraud detection. Information Sciences, 557, 317–331.

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

[17] Randhawa, K., Loo, C. K., Seera, M., Lim, C. P., & Nandi, A. K. (2022). Credit card fraud detection using AdaBoost and majority voting. IEEE Access, 6, 14277–14284.

[18] Misra, S., Li, H., & He, J. (2022). Artificial intelligence and machine learning in financial services: SHAP-based interpretability for fraud detection. Expert Systems with Applications, 192, 116397.

[19] Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. adversarial (2022). Using generative networks for improving classification effectiveness in credit card fraud detection. Information Sciences, 479, 448 455.

[20] Zheng, Z., Liu, H., Feng, C., & Xu, J. (2022). Federated learning for fraud detection in banking: A privacy-preserving framework. IEEE Transactions on Information Forensics and Security, 17, 2495–2507.

[21] Sadgali, I., Sael, N., & Benabbou, F. (2022). Performance of machine learning techniques in the detection of financial frauds. Procedia Computer Science, 148, 45–54.

[22] Tran, P. H., Tran, K. P., & Huong, T. T. (2022). Real-time data-driven approaches for credit card fraud detection. In International Conference on Industrial Engineering and Systems Management, 2022 (pp. 1–6). IEEE.

[23] Xie, Y., Li, S., Hu, S., Zhao, H., & Cheng, W. (2023). Resisting distributed backdoor attacks in federated learning: A dynamic norm clipping approach. Neural Networks, 165, 1 11.

[24] Wang, C., Han, D., Liu, Q., & Luo, S. (2023). A deep learning approach for detecting fraudulent transactions in mobile payment systems. Mobile Networks and Applications, 28(3), 744–756.

[25] Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2022). The application of data mining techniques in financial fraud detection. Decision Support Systems, 50(3), 559–569.

[26] Zhu, H., Liu, G., Zhou, M., Xie, Y., Abusorrah, A., & Kang, Q. (2022). Optimizing weighted extreme learning

Correspondence to: Kanchan Nanasaheb Varpe, Department of Computer Science & Engineering Suresh Gyan Vihar University, Jaipur
Corresponding author email: varpe.kanchan8@gmail.com

Available online at https://www.gyanvihar.org/researchjournals/ctm_journals.php
SGVU International Journal of Convergence of Technology and Management
E-ISSN: 2455-7528
Vol.12 Issue 2 Page No 169-174

machines for imbalanced classification and application to credit card fraud detection. Neurocomputing, 407, 50–62.

[27] Pumsirirat, A., & Yan, L. (2022). Credit card fraud detection using deep learning based on auto encoder and restricted Boltzmann machine. International Journal of Advanced Computer Science and Applications, 9(1), 18–25.

[28] Maes, S., Tuyls, K., Vanschoenwinkel, B., & Manderick, B. (2023). Credit card fraud detection using Bayesian and neural networks. In Proceedings of the International NAISO Congress on Neuro Fuzzy Technologies, 2023 (pp. 1–6).

[29] Dal Pozzolo, A., Johnson, R. A., Caelen, O., Waterschoot, S., Chawla, N. V., & Bontempi, G. (2022). Using HDDT to avoid instance propagation in unbalanced and evolving data streams. In 2022 International Joint Conference on Neural Networks (pp. 1–8). IEEE.

[30] Abdallah, A., Maarof, M. A., & Zainal, A. (2022). Fraud detection system: A survey. Journal of Network and Computer Applications, 68, 90 113.

Correspondence to: Kanchan Nanasaheb Varpe, Department of Computer Science & Engineering Suresh Gyan Vihar University, Jaipur
Corresponding author email: varpe.kanchan8@gmail.com