Unilag Journal of Mathematics and Applications,
Volume 6, Issue 2 (2026), Pages 72–87.
ISSN: 2805 3966. URL: http://lagjma.edu.ng

TEMPORAL AND CHANNEL-SPECIFIC PATTERNS IN NIGERIAN FRAUD: INTERPRETABLE MACHINE LEARNING ON A LARGE-SCALE SYNTHETIC DATASET

GBOLAHAN ADENIRAN IDOWU* AND JOSIAH ENDURANCE OWOLABI

Abstract. An examination of temporal and channel-specific fraud patterns is conducted using a large-scale synthetic dataset (1 million records) calibrated to Nigerian (NIBSS 2023) fraud distributions. Comparative evaluation of Logistic Regression, Random Forest, and XGBoost models, supported by SHAP interpretability, reveals that the Web (0.34%) and Mobile (0.33%) channels has highest risk. January (0.53%) and 01:00 (0.36%) are identified as peak fraud periods. Analysis confirms that there exist negligible linear correlation between temporal features and fraud, validating the need for non-linear ensemble approaches. The study concludes by proposing an interpretable, channel-aware framework for real-time risk scoring applicable to emerging markets.

1. Introduction

Nigeria's electronic payment transactions reached N600 trillion in 2023, representing a 55% increase from the previous year [1]. This rapid digitization has created unprecedented opportunities for fraudulent activities, with sophisticated fraud schemes exploiting vulnerabilities across multiple transaction channels. The Nigeria Inter-Bank Settlement System (NIBSS) 2023 Annual Fraud Landscape Report documented mobile channels as the preferred means for fraud, increasing by 5% compared to the previous year, while Web and Point of Sale (PoS) channels emerged as the most exploited payment channels [2].

Traditional rule-based fraud detection systems have proven insufficient against rapidly evolving fraud patterns and increasing transaction volumes. Machine learning approaches offer enhanced pattern recognition capabilities, yet their application in the Nigerian financial context remains limited by data availability constraints and regulatory restrictions. The Nigeria Data Protection Regulation

2010 *Mathematics Subject Classification.* Primary: 62P05. Secondary: 62P30.
Key words and phrases. Synthetic data; Interpretability; Temporal analysis; Channel-specific fraud; Nigerian banking.

Submitted: January 19, 2026. Revised: March 13, 2026. Accepted: March 17, 2026.
* Correspondence.

(NDPR) 2019 and institutional banking policies restrict access to sensitive transaction data, creating significant barriers for fraud detection research in emerging markets.

Interpretable machine learning models are essential for fraud detection systems in regulated financial environments. Model explain-ability supports regulatory compliance, builds stakeholder trust, and enables fraud analysts to understand detection mechanisms. The temporal and channel-specific dimensions of fraud patterns require specialized analytical approaches that can capture complex interactions across time periods and transaction types.

Fraud detection methodologies have evolved through distinct phases, transitioning from rule-based systems to statistical approaches and subsequently to machine learning architectures. Early detection strategies relied on human-designed rules specifying threshold-based conditions, generating high false-positive rates and struggling to adapt to novel fraud scenarios [3]. Statistical approaches including logistic regression and linear discriminant analysis provided probabilistic fraud assessments while maintaining interpretability [4]. Contemporary data mining and machine learning methods leverage computational advances to detect subtle fraud patterns through ensemble models and deep learning architectures [5], [6].

Supervised learning algorithms have demonstrated superior performance in fraud detection applications. Comparative studies have evaluated multiple algorithms including Naive Bayes, k-nearest neighbor, and logistic regression on imbalanced credit card datasets [7]. Ensemble methods, particularly Random Forest and gradient boosting frameworks, have shown considerable promise through variance reduction and bias correction mechanisms [6], [3] . XGBoost implementations have achieved enhanced performance on unbalanced datasets through iterative boosting approaches [6].

Feature engineering significantly influences fraud detection model performance. Temporal pattern encoding, behavioral analytic, and risk indicator derivation enhance discriminative power [6], [5]. SHAP (SHapley Additive exPlanations) analysis provides detailed feature attribution for individual predictions, supporting regulatory compliance and model transparency requirements [8]. Channel-specific analysis enables targeted resource allocation based on empirical risk assessment.

Limited availability of authentic fraud datasets in emerging markets constrains research and model development. Privacy regulations including Nigeria Data Protection Regulation (NDPR) restrict data sharing between institutions and researchers. Cultural and behavioral differences in transaction patterns require localized model development approaches. Class imbalance ratios in fraud datasets necessitate specialized sampling and evaluation strategies [9].

Despite extensive global fraud detection research, notable limitations persist in African financial contexts. Few studies leverage Nigerian-specific transaction data to capture unique consumer behaviors and local fraud typologies. Cost-sensitive analysis incorporating financial and reputation costs remains under explored. Integration of interpretable machine learning with temporal and channel-specific pattern analysis requires further investigation.

2. Materials and Methods

A comprehensive synthetic datasets of 1,000,000 Nigerian financial transactions was generated using the NIBSS Annual Fraud Landscape Report (2023) as the foundational reference [1]. The simulation framework incorporated Nigerian-specific banking channels, seasonal fraud patterns, transaction behaviors typical of major Nigerian financial institutions, and realistic fraud typologies observed in the Nigerian banking sector [2].

The datasets maintains a fraud rate of 0.30% (3,000 fraudulent transactions), creating a class imbalance ratio of approximately 332:1. While NIBSS reports an actual fraud rate of 0.0008%, the elevated simulation rate was deliberately chosen to ensure sufficient fraudulent samples for robust machine learning model training and evaluation.

The datasets encompass transactions from 10 major Nigerian banks across 6 transaction channels with fraud distribution patterns calibrated to NIBSS 2023 documented patterns. Channel distribution included Mobile Banking (45% transaction volume), Web Banking (20%), Point of Sale (18%), Internet Banking (10%), E-commerce (5%), and ATM (2%).

Figure(1) shows a four-panel visualization of: (a) transaction volume distribution across channels with Mobile banking dominating at 449,522 transactions, followed by Web (200,488) and PoS (180,035), (b) fraud rates by channel revealing Web banking as highest risk (0.343%), followed by Mobile (0.333%) and PoS (0.306%), with traditional channels showing lower rates, (c) monthly transaction volume distribution distinguishing NIBSS peak months (March, November, December) in red from regular months in blue, with March showing the highest volume (121,480 transactions), and (d) monthly fraud rate patterns where January exhibits the peak fraud rate (0.529%) while NIBSS peak months show variable but generally elevated fraud rates compared to regular months.

2.1. **Exploratory Data Analysis.** Chi-square analysis revealed statistically significant but weak associations between transaction channels and fraud occurrence ($\chi^2(5) = 147.59$, $p < 0.001$, Cramér's $V = 0.012$). Despite the large sample size producing statistical significance, the negligible effect size indicates minimal practical channel–fraud relationships.

Nigerian Banking Channel Fraud Rates were identified as follows: Web Banking demonstrated the highest fraud rate at 0.34% (95% CI [0.32%, 0.37%]), followed by Mobile Banking at 0.33% (95% CI [0.32%, 0.35%]), and PoS Terminals at 0.31% (95% CI [0.28%, 0.33%]). Traditional channels exhibited lower rates: Internet Banking at 0.17%, E-commerce at 0.15%, and ATM Networks at 0.11%.

The four-panel visualization in figure(2) shows (a) transaction volume by channel with fraud rates and 95% confidence intervals, where Mobile dominates volume (450,000 transactions) but Web banking exhibits the highest fraud rate (0.34%), (b) fraud rates by channel with confidence intervals confirming Web and Mobile as highest-risk channels, (c) scatter plot revealing the inverse relationship between transaction volume and fraud rates across all channels, and (d)

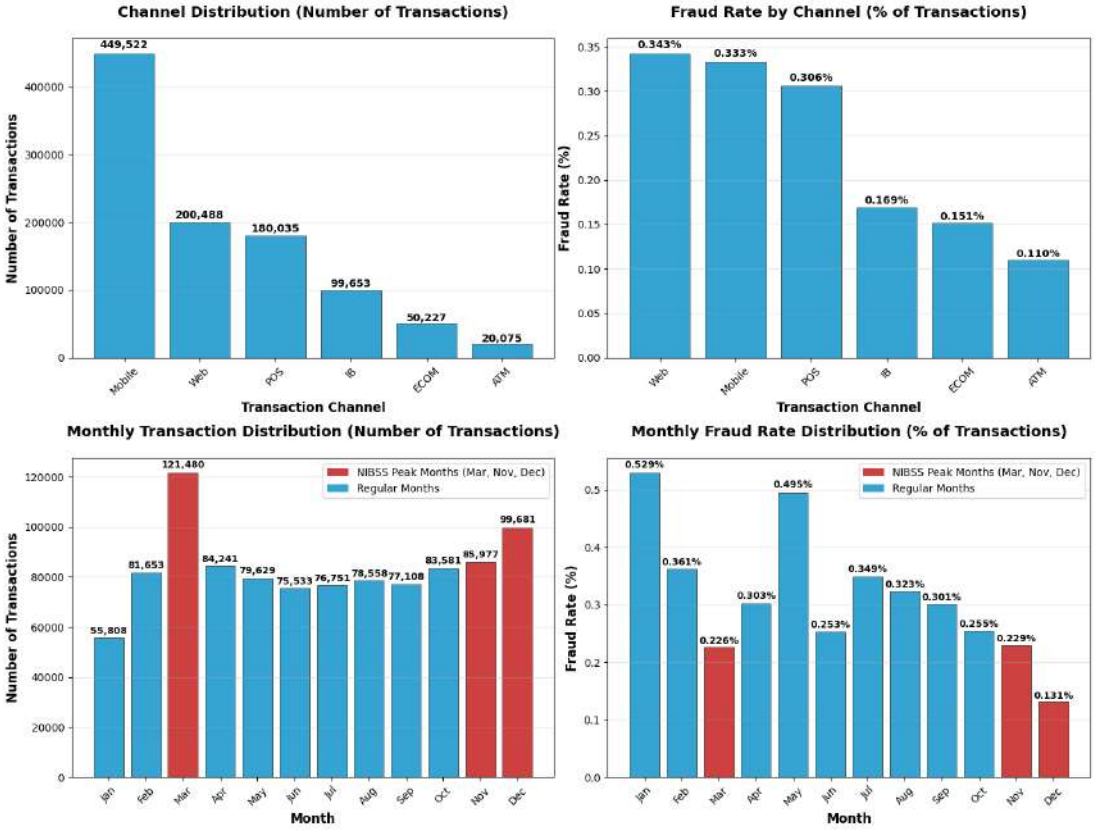


FIGURE 1. Channel Distribution and Temporal Fraud Patterns in Dataset

risk-volume matrix plotting fraud rates against volume percentages, clearly delineating high-volume/moderate-risk channels (Mobile, PoS) from low-volume/high-risk channels (Web, IB), providing strategic insights for Nigerian banking security resource allocation.

Figure(2) shows the temporal fraud dynamics in the Nigerian banking dataset. The upper-left plot traces the hourly fraud rate with 95% bootstrap confidence bands, revealing a modest late-night spike that peaks at 01:00 (0.36%). Business hours (09:00–17:00) and overnight windows (22:00–06:00) are shaded for context. To its right, log-scaled box-and-whisker plots show that median transaction values remain virtually unchanged across the 24-hour cycle, a result confirmed by a Kruskal–Wallis test ($H = 18.36$, $df = 23$, $p = 0.74$). The lower-left bar chart depicts monthly fraud rates with 95% confidence intervals; Jan stands out at roughly 0.53%, representing the highest fraud concentration in the dataset. Finally, the heat-map in the lower-right cross-tabulates hour and month, illustrating scattered temporal patterns but no sustained hour-by-season interaction. Together,

Table 1. Final Dataset Configuration

Characteristic	**Value**
Total Transactions	1,000,000
Fraudulent Transactions	3,000
Legitimate Transactions	997,000
Fraud Rate	0.30%
Class Imbalance Ratio	332:1
Class Imbalance Strategy	SMOTE 1:5 (training only)
Total Features	38
Original Features	24
Engineered Features	14
Training Set (70%)	700,000
Validation Set (15%)	150,000
Test Set (15%)	150,000
Nigerian Banks	10
Transaction Channels	6
Nigerian States	15
Merchant Categories	14
Temporal Coverage	Full year 2023
Currency	Nigerian Naira (₦)
Missing Values	0
Duplicate Records	0
Data Quality Score	100%

the panels indicate that temporal risk is driven more by the frequency of transactions than by their monetary value, justifying the exclusion of amount-by-time interactions from downstream fraud-scoring models.

Temporal analysis revealed fraud concentration patterns across hourly and monthly cycles. Peak Risk Hour occurred at 01:00 (0.36% fraud rate), while business hours (09:00–17:00) maintained relatively moderate fraud rates averaging 0.30%. Monthly seasonal patterns showed January with the highest fraud rate at 0.53%, May at 0.50%, and December with the lowest at 0.13%.

A Kruskal–Wallis test revealed no statistically significant hourly differences in transaction amounts across the 24-hour period ($H(23) = 18.36$, $p = 0.738$), confirming that temporal risk patterns are driven by transaction frequency rather than monetary value.

Figure(4) shows the feature correlation and multicollinearity analysis for the Nigerian banking fraud detection dataset. The four-panel composite shows (a) correlation matrix among key features with blue-white-red diverging scheme, (b) top correlations with fraud status showing negligible linear relationships across all features, (c) distribution of correlation strengths confirming all features fall in the negligible category, and (d) feature importance ranking by absolute correlation values. The analysis reveals minimal linear separability, suggesting that fraud

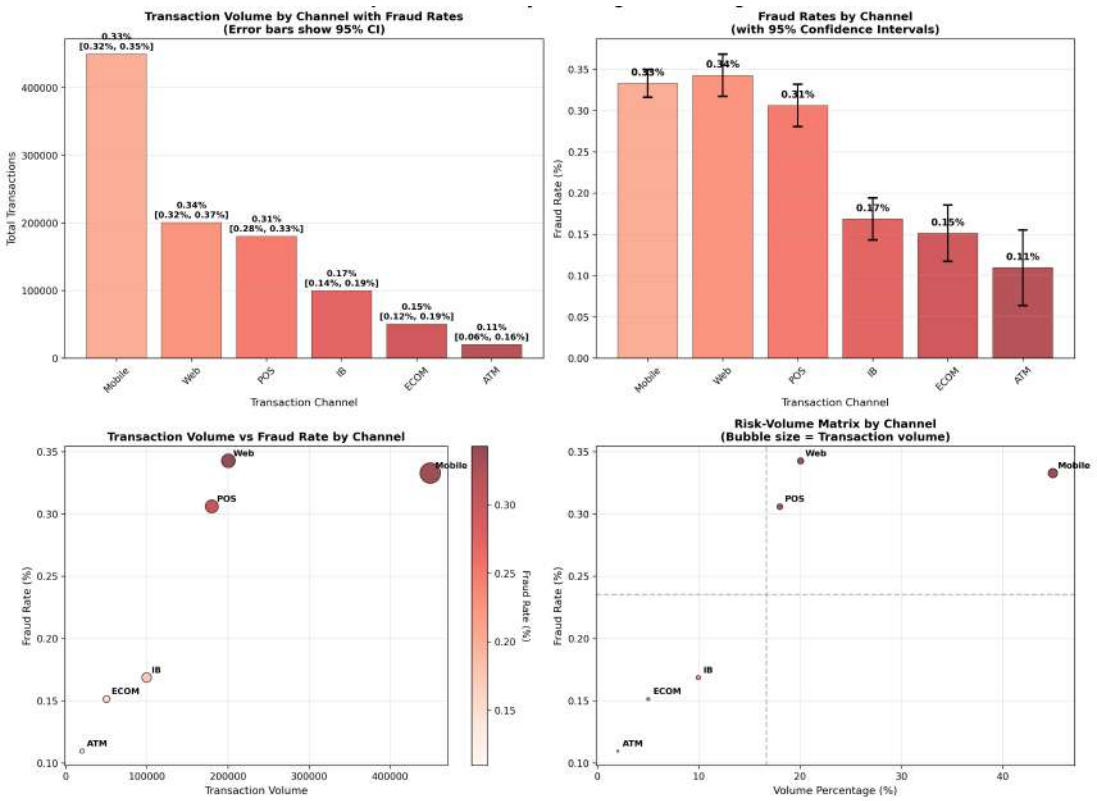


FIGURE 2. Channel-Specific Fraud Analysis for Nigerian Banking Dataset

detection will require non-linear modeling approaches to capture complex feature interactions.

Correlation analysis revealed limited linear associations between engineered features and fraud status. All 38 features exhibited negligible linear correlations with fraud status ($|r| < 0.1$), with Amount (log-transformed) showing the highest correlation at $r = 0.045$. Variance Inflation Factor (VIF) analysis revealed significant multicollinearity among engineered features, with 15 features exhibiting $VIF \geq 10$.

2.2. **Feature Engineering.** Comprehensive feature engineering transformed 24 original transaction attributes into 38 discriminative features. Temporal features included basic attributes (hour, day of week, month) and cyclical encoding (*hour_sin*, *hour_cos*, *day_sin*, *day_cos*, *month_sin*, *month_cos*) to capture temporal periodicities. Behavioral features encompassed transaction velocity (*tx_count_24h*, *amount_sum_24h*), historical patterns (*amount_mean_7d*, *amount_std_7d*), and behavioral ratios (*amount_vs_mean_ratio*, *online_channel_ratio*). Risk indicators included composite scoring (*velocity_score*, *merchant_risk_score*) and amount transformations (*amount_log*, *amount_rounded*).

2.3. **Model Implementation.** Three supervised learning algorithms were implemented: Logistic Regression with L2 regularization, Random Forest ensemble

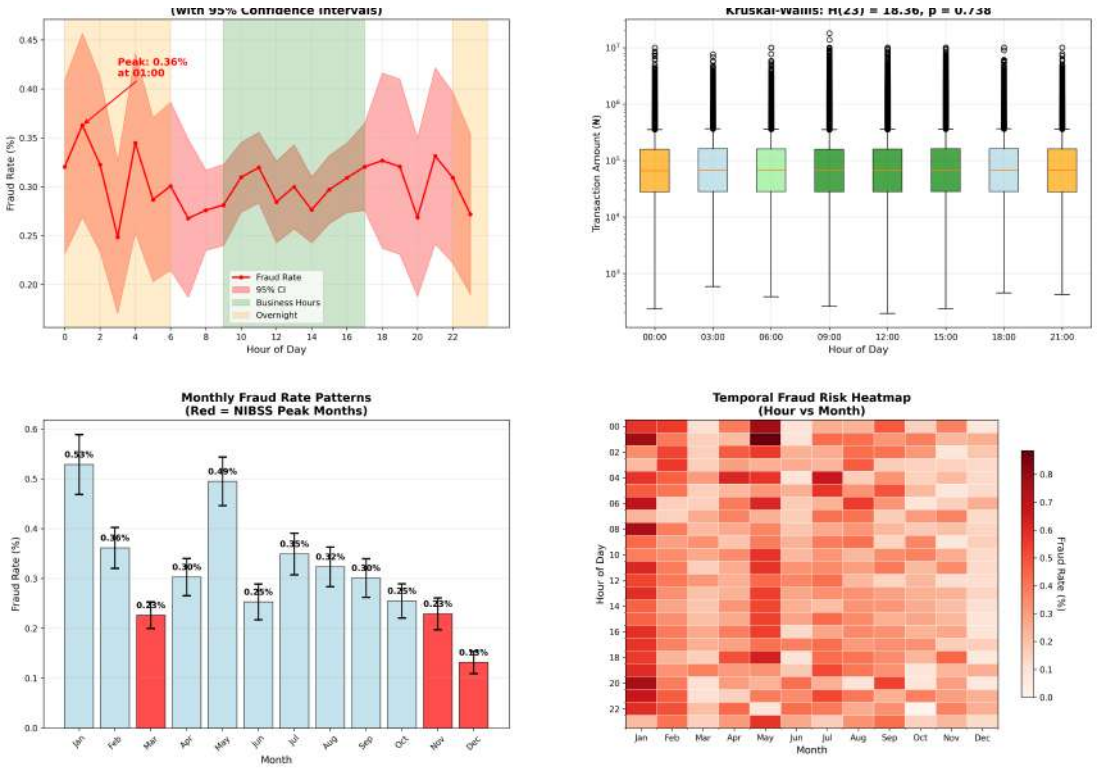


FIGURE 3. Temporal fraud dynamics in Nigerian banking dataset

with bootstrap aggregation, and XGBoost gradient boosting. Class imbalance was addressed using SMOTE 1:5 oversampling strategy during training, selected based on achieving the highest F1-Score (0.5600) while maintaining perfect precision (1.0000) among seven evaluated strategies.

TABLE 2. Class Imbalance Strategy Performance Comparison

Strategy	Precision	Recall	F1-Score	AUC
SMOTE 1:5	1.0000	0.3889	**0.5600**	0.9229
Baseline	1.0000	0.3778	0.5484	0.9260
SMOTE 1:3	1.0000	0.3667	0.5366	0.9073
Undersample 1:5	0.6393	0.4333	0.5166	0.8972
Class Weight Manual	1.0000	0.3222	0.4874	0.8988
Class Weight Balanced	1.0000	0.3111	0.4746	0.9159
Undersample 1:3	0.2878	0.4444	0.3493	0.8985

2.4. **Hyperparameter Optimization.** Systematic grid search with 3-fold stratified cross-validation identified optimal hyperparameters for each model, using AUC-ROC as the optimization metric. The dataset was partitioned using stratified sampling into Training Set (70%), Validation Set (15%), and Test Set (15%).

2.5. **Model Interpretability.** SHAP (SHapley Additive exPlanations) analysis was applied for both global feature importance assessment and local prediction

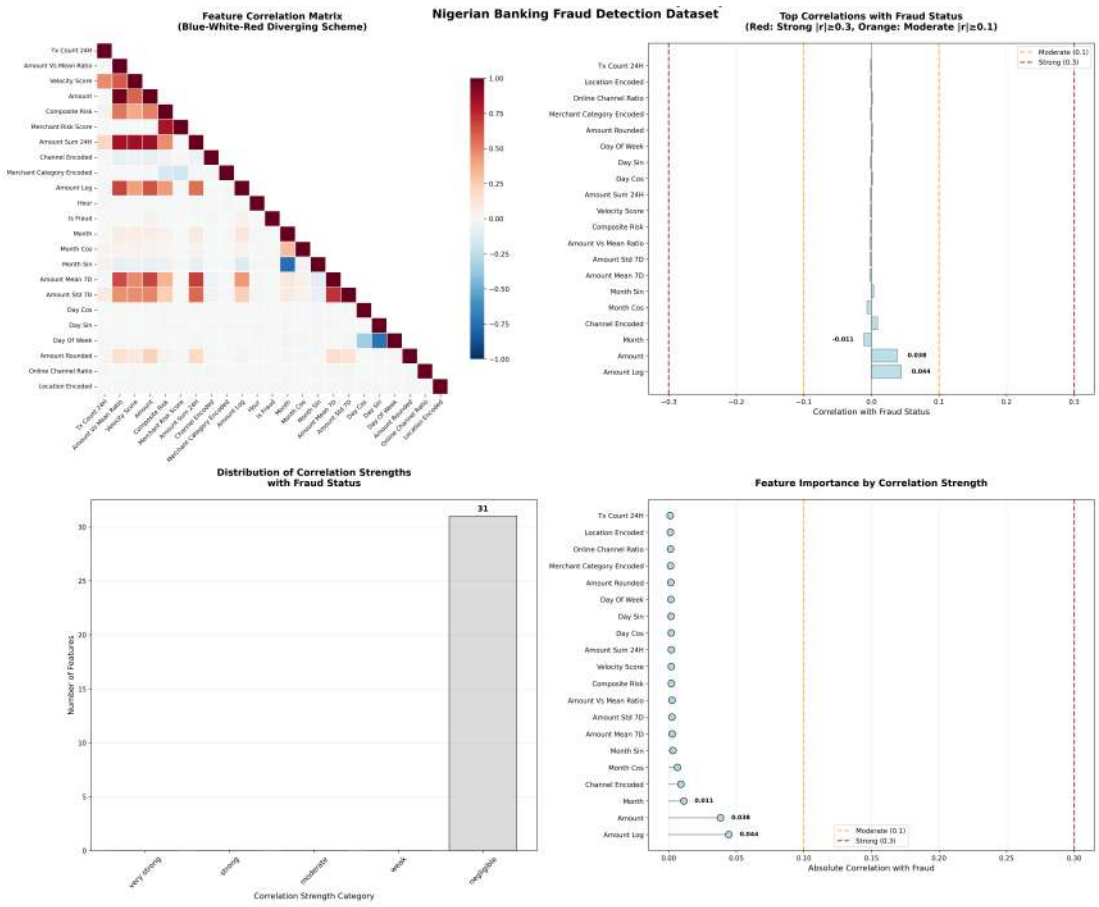


FIGURE 4. Feature correlation and multicollinearity analysis

TABLE 3. Optimal Hyperparameters and Cross-Validation Performance

Model	**Optimal Parameters**	**CV AUC (Mean ± SD)**	**CV F1-Score (Mean ± SD)**
Logistic Regression	C = 10.0, penalty = 'l2', class_weight = 'balanced'	0.796 ± 0.009	0.015 ± 0.000
Random Forest	n_estimators = 200, max_depth = None, min_samples_split = 10, max_features = 'sqrt', class_weight = 'balanced'	0.972 ± 0.005	0.658 ± 0.013
XGBoost	learning_rate = 0.3, max_depth = 6, n_estimators = 200, subsample = 1.0, colsample_bytree = 1.0, scale_pos_weight = 332	0.965 ± 0.002	0.835 ± 0.003

explanations. Permutation feature importance quantified each feature's contribution to fraud detection performance using the formula:

$$\text{Importance}_j = \frac{1}{K}\sum_{k=1}^{K}\left[S^{(k)} - S^{(k,\pi_j)}\right],$$

where S represents the model score and π_j indicates permutation of feature j.

3. Results

3.1. **Model Performance Evaluation.** Final model evaluation was conducted on the holdout test set (150,000 transactions, 450 fraudulent). XGBoost achieved optimal performance with F1-Score of 0.854 and recall of 74.6%, compared to Random Forest's F1-Score of 0.699 and recall of 53.8%. Random Forest demonstrated marginally higher AUC-ROC of 0.977 [0.966, 0.986] versus XGBoost's 0.973 [0.963, 0.981]. Both ensemble methods achieved perfect precision (1.000), substantially outperforming Logistic Regression (AUC = 0.799).

Table 4. Test Set Performance Metrics with 95% Bootstrap Confidence Intervals

Model	Precision	Recall	F1-Score	AUC	Accuracy	Specificity
Logistic Regression	0.007 [0.007, 0.008]	0.699 [0.654, 0.741]	0.015 [0.013, 0.016]	0.799 [0.777, 0.824]	0.720 [0.718, 0.722]	0.720 [0.718, 0.722]
Random Forest	1.000 [1.000, 1.000]	0.538 [0.493, 0.584]	0.699 [0.662, 0.739]	0.977 [0.966, 0.986]	0.999 [0.998, 0.999]	1.000 [1.000, 1.000]
XGBoost	1.000 [1.000, 1.000]	0.746 [0.703, 0.786]	0.854 [0.827, 0.880]	0.973 [0.963, 0.981]	0.999 [0.999, 0.999]	1.000 [1.000, 1.000]

ROC curve analysis confirmed Random Forest's superior discriminative ability, while Precision-Recall curves revealed ensemble method advantages in minority class detection under extreme class imbalance conditions.

3.2. **Statistical Significance Testing.** McNemar's test assessed statistical significance of performance differences between models. Both ensemble methods significantly outperformed Logistic Regression ($p < 0.001$), while Random Forest demonstrated statistically significant superiority over XGBoost ($p < 0.001$).

Cross-validation stability analysis revealed XGBoost's superior consistency with the lowest coefficient of variation for both AUC (0.20%) and F1-Score (0.37%) across 50 iterations.

3.3. **Feature Importance Analysis.**

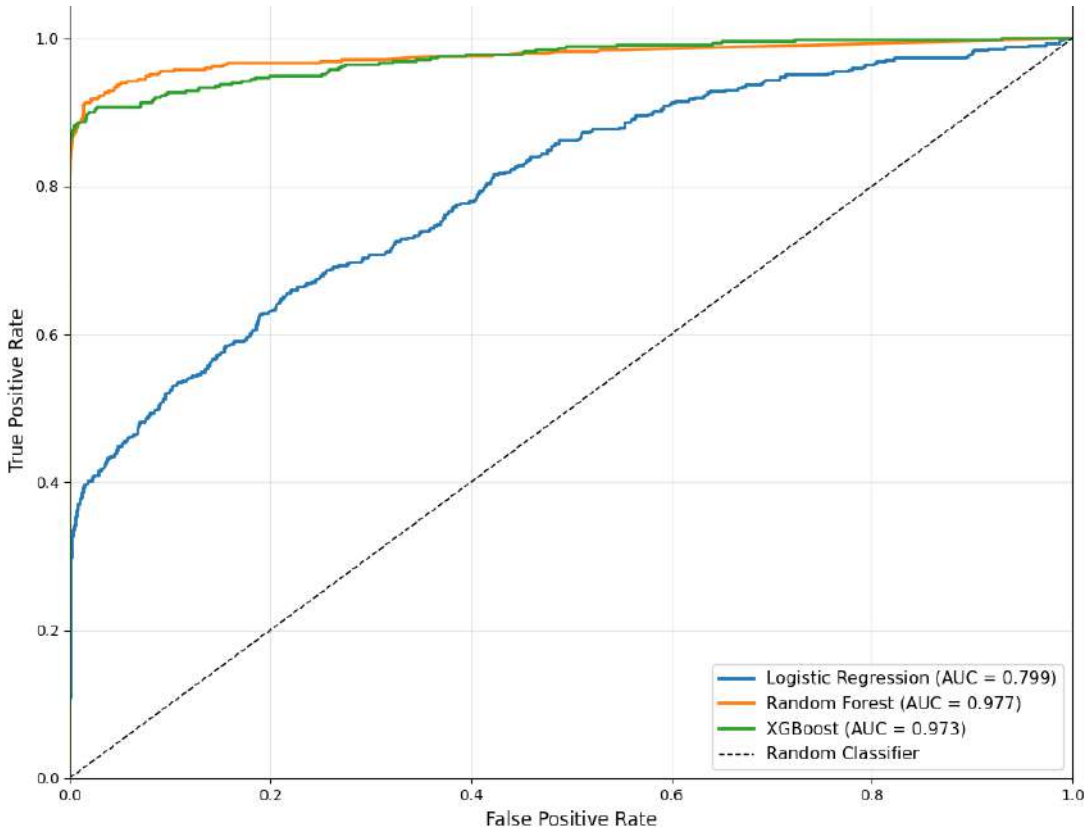


FIGURE 5. ROC curves for all three models. Random Forest highest (AUC=0.977), XGBoost (AUC=0.973), Logistic Regression (AUC=0.799). Include diagonal reference line and clear legend with AUC values

3.3.1. *Permutation Feature Importance.* Model-agnostic permutation importance quantified feature contributions to fraud detection performance. Amount emerged as the dominant feature across all models, achieving highest importance scores (LR: 0.271 ± 0.011, RF: 0.298 ± 0.006, XGB: 0.338 ± 0.010). Amount vs Mean Ratio and Amount Sum 24h demonstrated consistent secondary importance across models.

3.3.2. *SHAP Global Analysis.* Figure(6) depicts the SHAP feature importance analysis for ensemble models in Nigerian fraud detection. (a) Random Forest model prioritizes Transaction Count (24H) as the most important feature (mean $|\text{SHAP}| = 0.117$), followed by Amount (0.117), Day of Week (0.111), and Hour (0.111), demonstrating temporal feature emphasis. (b) XGBoost model shows Amount as the dominant predictor (mean $|\text{SHAP}| \approx 5.0$), followed by Amount Sum (24H) (1.648) and Amount Log (1.130), indicating amount-centric feature utilization. (c) Direct comparison reveals contrasting feature prioritization strategies: Random Forest emphasizes temporal patterns while XGBoost focuses heavily on amount-based features, with XGBoost showing much higher absolute SHAP values overall.

TABLE 5. McNemar's Test Results

Model Comparison	**b (Model 1 wrong, Model 2 correct)**	**c (Model 1 correct, Model 2 wrong)**	**χ^2 Statistic**	**p-value**	**Conclusion**
Logistic vs Random Forest	1283	31994	28341.02	< 0.001	Random Forest significantly better
Logistic vs XGBoost	1102	31378	28219.69	< 0.001	XGBoost significantly better
Random Forest vs XGBoost	2607	2172	39.41	< 0.001	Random Forest significantly better

TABLE 6. Cross-Validation Stability Analysis (50 CV Iterations)

Model	**AUC Mean ± SD**	**AUC CV***	**F1-Score Mean ± SD**	**F1 CV***	**Stability Rank****
XGBoost	0.965 ± 0.002	0.20%	0.835 ± 0.003	0.37%	1
Logistic Regression	0.796 ± 0.009	1.08%	0.015 ± 0.000	0.46%	2
Random Forest	0.972 ± 0.005	0.51%	0.658 ± 0.013	2.00%	3

SHAP analysis revealed distinct feature prioritization strategies between models. Random Forest emphasized temporal patterns with Transaction Count (24H) as the most important feature (mean |SHAP| = 0.117), followed by Amount (0.117) and Day of Week (0.111). XGBoost demonstrated amount-centric focus with Amount as the dominant predictor (mean |SHAP| $\approx$ 5.0), followed by Amount Sum (24H) (1.648) and Amount Log (1.130).

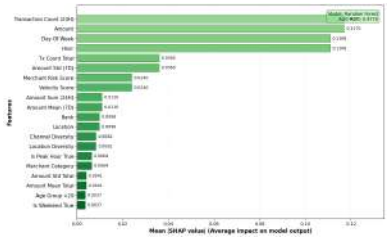
Figure(7) illustrates the Channel-specific feature importance analysis showing mean —SHAP— values across different transaction channels (ATM, ECOM, IB, Mobile). Amount demonstrates consistently highest importance across all channels ($\approx$8.0 for ATM, $\approx$5.2 for ECOM, $\approx$5.0 for Mobile, $\approx$2.6 for IB), followed by Amount Sum 24H and Amount Log. The analysis reveals that amount-based features dominate fraud detection regardless of transaction channel, while other features show minimal cross-channel variation in importance.

Channel-specific feature importance analysis confirmed Amount's consistent dominance across all transaction channels, with minimal cross-channel variation in importance rankings.

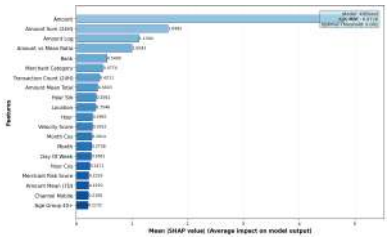
TABLE 7. Top 10 Features by Permutation Importance (AUC Decrease)

Rank	Feature	Logistic Regression Δ AUC	Random Forest Δ AUC	XGBoost Δ AUC
1	Amount vs Mean Ratio	0.385 ± 0.004	0.121 ± 0.002	0.280 ± 0.003
2	Velocity Score	0.002 ± 0.000	0.003 ± 0.000	0.036 ± 0.001
3	Amount Sum 24H	0.102 ± 0.002	0.012 ± 0.000	0.001 ± 0.000
4	Transaction Count 24H	0.027 ± 0.000	0.000 ± 0.000	0.001 ± 0.000
5	Amount	0.005 ± 0.000	0.000 ± 0.000	0.000 ± 0.000
6	Amount Mean Total	0.016 ± 0.001	0.000 ± 0.000	0.000 ± 0.000
7	Amount Std 7D	0.013 ± 0.000	0.000 ± 0.000	0.000 ± 0.000
8	Composite Risk	0.008 ± 0.001	0.003 ± 0.000	0.000 ± 0.000
9	Channel	0.000 ± 0.000	0.000 ± 0.000	0.000 ± 0.000
10	Is Weekend	0.000 ± 0.000	0.000 ± 0.000	0.000 ± 0.000

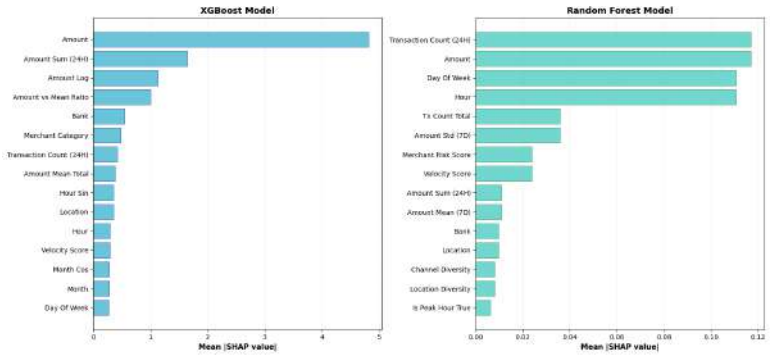
3.3.3. *SHAP Dependence Analysis.* SHAP dependence plots revealed non-linear relationships between key features and fraud predictions. Amount-based features



(A) Random Forest SHAP Feature Importance



(B) XGBoost SHAP Feature Importance



(C) SHAP Feature Importance Comparison: XGBoost vs Random Forest

FIGURE 6. SHAP feature importance analysis for ensemble models

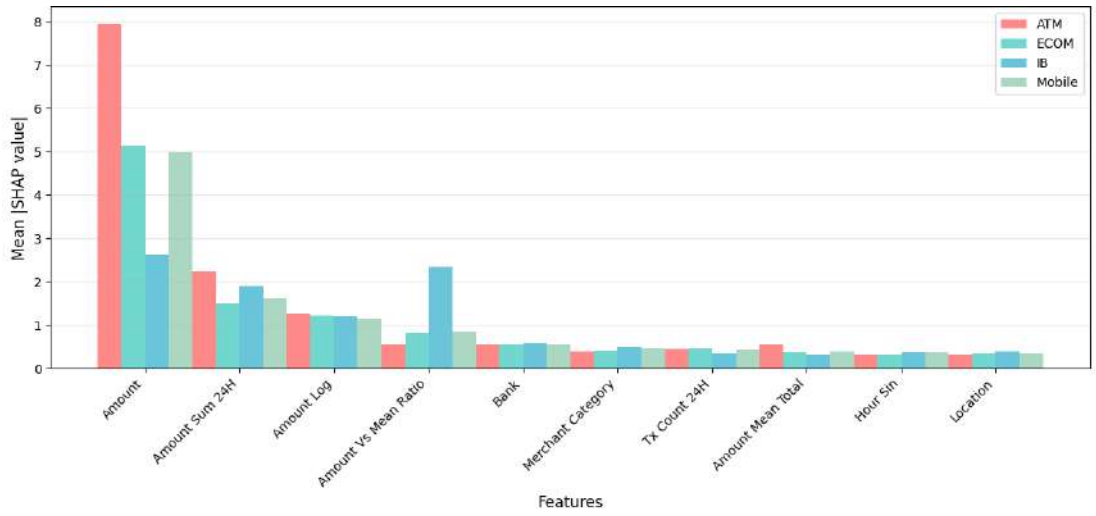


FIGURE 7. Channel-specific feature importance analysis

exhibited clear positive correlations with SHAP values at higher feature values, indicating increased fraud probability for larger transactions.

Figure(8) depicts the Feature value vs SHAP value relationships demonstrating how individual feature values influence fraud predictions. The scatter plots show distinct patterns: (top row) amount, amount_sum_24h, and amount_log exhibit clear positive correlations with SHAP values at higher feature values, indicating increased fraud probability; (bottom row) amount_vs_mean_ratio shows strong positive SHAP contribution for higher ratios, while bank and merchant_category features display clustered categorical effects. Color intensity represents SHAP magnitude, with red indicating high positive contribution to fraud prediction and blue indicating negative contribution toward normal classification.

3.4. **Cost-Sensitive Analysis.** Cost-sensitive analysis using Nigerian banking cost parameters revealed significant economic benefits from optimal threshold selection. Random Forest achieved 69.1% cost reduction (from ₦81,791,825 to ₦25,241,985) with optimal threshold at 0.030, while XGBoost demonstrated 43.7% cost reduction with threshold at 0.002. Logistic Regression showed minimal improvement (1.9%) with threshold at 0.554.

TABLE 8. Cost Analysis with Threshold Optimization

Model	**Default Total Cost (₦)**	**FP/FN Ratio**	**Optimal Threshold**	**Total Cost (₦)**	**Cost Reduction**
Logistic Regression	₦92,430,032	308/1	0.55	₦90,651,204	1.9%
Random Forest	₦81,791,825	0/1	0.03	₦25,241,985	69.1%
XGBoost	₦49,224,293	0/1	0.00	₦27,735,740	43.7%

4. Discussion of Results

The analysis revealed distinct vulnerability patterns across transaction channels and temporal dimensions. Web banking's elevated fraud rate (0.34%) compared to traditional channels (average 0.14%) reflects the increased attack surface of digital platforms. The 01:00 AM peak fraud hour (0.36%) suggests automated attack patterns or reduced monitoring during overnight periods. January's peak fraud month (0.53%) may correlate with post-holiday financial stress or seasonal transaction pattern disruptions.

These insights provide actionable intelligence for Nigerian financial institutions to optimize resource allocation. Enhanced surveillance during peak risk periods (01:00 AM, January) and targeted security measures for high-risk channels (Web, Mobile) can improve fraud prevention effectiveness.

SHAP analysis provides crucial interpretability for regulatory compliance in Nigerian banking contexts. The Central Bank of Nigeria's emphasis on explainable AI systems requires fraud detection models to provide transparent decision mechanisms. The contrasting feature prioritization between Random Forest (temporal patterns) and XGBoost (amount-centric) demonstrates model diversity benefits for ensemble approaches.

Feature importance hierarchy reveals amount-based patterns as primary fraud indicators, supporting risk-based transaction monitoring approaches. The negligible linear correlations ($|r| < 0.1$) between individual features and fraud status validate the necessity of non-linear ensemble methods for effective fraud detection.

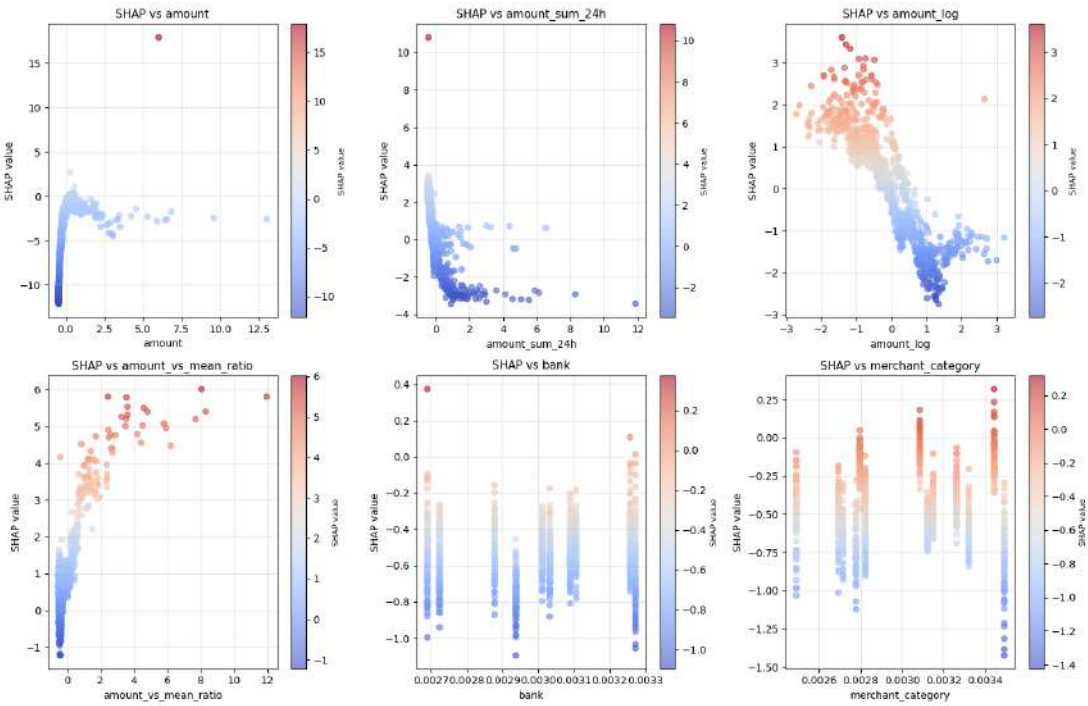


Figure 8. Feature value vs SHAP value relationships for key fraud detection features

The elevated fraud rate (0.30%) compared to NIBSS documented rates (0.0008%) represents a fundamental limitation requiring careful consideration for production deployment. Model calibration through isotonic scaling addresses probability estimate accuracy, yet threshold recalibration remains essential for real-world implementation.

The synthetic data approach successfully balances research validity with ethical compliance while establishing methodological foundations for emerging market fraud detection. The controlled simulation environment enables reproducible experimentation but may not capture all nuances of sophisticated real-world fraud behaviors.

5. Conclusions

This study demonstrates that interpretable ensemble methods reveal nuanced fraud patterns across temporal and channel dimensions in Nigerian financial transactions. Random Forest achieved superior AUC-ROC (0.977) while XGBoost demonstrated optimal F1-Score (0.854), with SHAP analysis revealing distinct feature prioritization strategies between models. The analysis identified Web banking (0.34%) and Mobile banking (0.33%) as highest-risk channels, with temporal peaks at 01:00 AM (0.36%) and January month (0.53%). Amount-based behavioral patterns significantly outperformed categorical features for fraud detection, establishing feature importance hierarchies relevant to Nigerian transaction contexts. The cost-sensitive analysis confirmed substantial economic benefits, with Random Forest achieving 69.1% cost reduction through optimal threshold selection. The synthetic data approach successfully addresses research gaps in African financial fraud detection while maintaining ethical compliance and providing replicable methodologies. The framework developed in this research is transferable to other emerging markets with limited data access, providing methodological foundations for fraud detection system development. The interpretability analysis through SHAP values supports regulatory compliance requirements while enabling fraud analysts to understand detection mechanisms.

Future work should focus on real-world validation of these synthetic findings through collaboration with Nigerian financial institutions. Implementation of continuous learning mechanisms that adapt to evolving fraud patterns represents a critical advancement for sustainable fraud detection systems. Extension to federated learning frameworks could enable collaborative fraud detection while maintaining data privacy and competitive confidentiality.

Acknowledgments. The author(s) would like to thank Melodee Okigbo for insightful suggestions, valuable input on design considerations, and careful proofreading of the initial draft. We acknowledge the Nigeria Inter-Bank Settlement System (NIBSS) for publicly available fraud landscape reports that informed our synthetic data generation. We thank the Department of Statistics, University of Lagos, for research support and resources.

Authors Contributions. G. A. Idowu and J. E. Owolabi carried out the conceptualization, methodology, validation of the original draft. G. A. Idowu did the

analysis, editing and validation, while J. E. Owolabi did the typing of the manuscript and project administration of the work. Both authors read and approved the final manuscript.

Authors' Conflicts of interest. The authors declare(s) that there are no conflicts of interest regarding the publication of this paper.

Funding Statement. This research received no external funding.

References

[1] Nigeria Inter-Bank Settlement System. *Electronic payment transactions statistics: Nigeria recorded ₦600 trillion e-payment transactions in 2023*. Technical Report, Lagos, Nigeria: NIBSS, 2023.

[2] Nigeria Inter-Bank Settlement System. *2023 annual fraud landscape report*. Technical Report, Lagos, Nigeria: NIBSS, 2024.

[3] I. H. Witten, E. Frank, M. A. Hall. *Data mining: Practical machine learning tools and techniques*, 4th ed. Morgan Kaufmann, 2016.

[4] S. Bhattacharyya, S. Jha, K. Tharakunnel, J. C. Westland. *Data mining for credit card fraud: A comparative study*. Decision Support Systems, 50(3):602–613, 2011.

[5] A. Roy, J. Sun, W. Mahoney, R. Al-Azad, E. Moreira. *Deep learning detecting fraud in credit card transactions*. 2018 Systems and Information Engineering Design Symposium (SIEDS), pp. 29–34, 2018.

[6] K. Randhawa, C. K. Loo, M. Seera, C. P. Lim, A. K. Nandi. *Credit card fraud detection using adaboost and majority voting*. IEEE Access, 6:14277–14284, 2018.

[7] J. O. Awoyemi, A. O. Adetunmbi, S. A. Oluwadare. *Credit card fraud detection using machine learning techniques: A comparative analysis.* 2017 International Conference on Computing Networking and Informatics (ICCNI), pp. 1–9, 2017.

[8] H. Wang, R. Martinez, A. Thompson. *Explainable ai and federated learning for financial fraud detection: A comprehensive survey*. IEEE Transactions on Information Forensics and Security, 19:2847–2862, 2024.

[9] National Information Technology Development Agency. *Nigeria Data Protection Regulation (NDPR) 2019*. Regulatory Framework, Abuja, Nigeria: NITDA, 2019.

[10] S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, C. Jiang. *Random forest for credit card fraud detection*. 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), pp. 1–6, 2018.

Gbolahan Adeniran Idowu*
Department of Mathematics, Lagos State university, Ojo, Lagos State, Nigeria.
Department of Statistics, University of Lagos, Akoka, Lagos State, Nigeria.
Email address: gbolahan.idowu@lasu.edu.ng

Josiah Endurance Owolabi
Department of Statistics, University of Lagos, Akoka, Lagos State, Nigeria.
Email address: 210806502@live.unilag.edu.ng