DOI: https://doi.org/10.57233/ijsgs.v12i1.1016 ISSNp: 2488-9229; ISSNe: 3027-1118

IJSGS FUGUSAU VOL. 12(1) WEBSITE: https://fugus-ijsgs.com.ng

INTERNATIONAL JOURNAL OF SCIENCE FOR GLOBAL SUSTAINABILITY
(A PUBLICATION OF FACULTY OF SCIENCE, FEDERAL UNIVERSITY GUSAU, NIGERIA)

Machine Learning in Financial Security: Performance Evaluation of Fraud Detection Models for POS Operators in Nasarawa Town

Jamila Ahmed*[1], Salihu Audu Abdullahi [2], Morufu Olalere [3], Gilbert I. O. Aimufua [4], Binyamin. A. Ajayi [5], & Muawiya Abdullahi Ari [6]

[1]Department of Computer Science, Federal Polytechnic, Nasarawa, Nigeria
[2]Department of Computer Science, Nasarawa State University Keffi. Nigeria
[3]Department of Electrical Engineering. Nasarawa State University Keffi, Nigeria

***Corresponding Author's Email:** jameelerh020@gmail.com

Received on: January, 2026 **Revised and Accepted on:** February, 2026 **Published on:** March, 2026

ABSTRACT

Financial fraud continues to present a growing challenge for digital payment systems, especially for Point-of-Sale (POS) operators navigating the complexities of emerging economies. In Nasarawa Town, Nigeria, the rapid expansion of POS services has inadvertently created more opportunities for fraudulent transactions, highlighting an urgent need for smarter, more adaptive detection strategies. This study examines how effectively five supervised machine learning models, Logistic Regression, Decision Tree, Random Forest, Support Vector Machine (SVM), and Neural Network, identify fraudulent POS transactions. Using anonymized transaction data, we carefully pre-processed the dataset, engineered relevant features, and addressed the persistent challenge of class imbalance before training and validating each model. Performance was assessed through accuracy, precision, recall, F1-score, and Area Under the ROC Curve (AUC). Results showed that Random Forest consistently led across all metrics, achieving 96.4% accuracy and 97.1% AUC, demonstrating its ability to reliably separate legitimate from fraudulent activity while maintaining a practical balance between catching fraud and avoiding false alerts. Neural Network followed as a strong contender, while Logistic Regression and Decision Tree showed more modest results. We conclude that ensemble learning approaches, particularly Random Forest, offer the most dependable and scalable solution for real-time fraud detection among POS operators in Nasarawa Town. These findings contribute locally relevant evidence to financial fraud analytics and offer actionable insights for developing machine learning–powered security frameworks in semi-urban digital payment environments.

Keywords: Machine Learning; Fraud Detection; Point-of-Sale (POS); Random Forest; Financial Security.

1.0 INTRODUCTION

Financial fraud remains a persistent and evolving challenge within digital payment ecosystems, particularly affecting Point-of-Sale (POS) operators who manage high transaction volumes while confronting increasingly sophisticated attack methods (Osei & Lawal, 2024; Sylvanus & Bupo, 2024). In Nigeria, the swift growth of POS services has delivered undeniable convenience but has also heightened security concerns and operational vulnerabilities for local businesses (Adewale & Sanni, 2026; Imade & Evbayiro-Osagie, 2025). Traditional rule-based detection systems, though once dependable, now struggle to keep pace with adaptive fraud strategies that continuously evolve alongside technology (Osei & Lawal, 2024). This is where machine learning (ML) offers meaningful promise: by learning directly from transaction patterns, ML techniques can uncover subtle, complex signals of fraudulent activity, often in real time (Osei & Lawal, 2024; Rahman et al., 2023). Models such as logistic regression, decision trees, random forests, support vector machines, and neural networks have all demonstrated strong potential in financial fraud detection contexts (Rahman et al., 2023; Singh & Verma, 2024). However, their effectiveness is not universal; performance depends significantly on how well we manage imbalanced data, engineer meaningful features, and select appropriate evaluation metrics like AUC, precision, and recall (Musa & Ayodele, 2025; Eze & Musa, 2024).

This study evaluates selected ML models using POS transaction data from Nasarawa Town to determine which approach delivers the best combination of accuracy, scalability, and reliability for fraud detection within this specific local context.

1.1 Statement of the Problem

The increasing reliance on POS transactions in Nasarawa Town has unfortunately heightened exposure to fraud, resulting in tangible financial losses and weakening trust among operators and customers (Adewale & Sanni, 2026; Obi, 2023). Conventional detection systems, often built on static rules, lack the flexibility to adapt to emerging fraud tactics that evolve alongside technological advances (Osei & Lawal, 2024). While machine learning offers more advanced predictive

DOI: https://doi.org/10.57233/ijsgs.v12i1.1016 ISSNp: 2488-9229; ISSNe: 3027-1118

capabilities, there remains limited empirical benchmarking of ML models specifically tailored to the realities of POS operators in semi-urban Nigerian settings like Nasarawa Town (Musa & Ayodele, 2025; Lawal, 2022). Accordingly, this study compares selected machine learning algorithms to identify the most effective model for real-time POS fraud detection in Nasarawa Town.

1.2 Objectives

i. Formulate a realistic financial transaction dataset reflective of Point-of-Sale (POS) operations in Nasarawa Town.
ii. Design an experimental setup for detecting fraudulent financial transactions using machine learning techniques specific to POS activities in Nasarawa Town.
iii. Develop an effective fraud detection algorithm based on the designed experimental setup for POS transactions in Nasarawa Town.
iv. Evaluate the performance of selected machine learning models in detecting POS-related financial fraud using standard evaluation metrics in Nasarawa Town.

1.3 Conceptual Framework

The conceptual framework for this study positions POS transaction data as the input, machine learning algorithms as the predictive engine, and fraud detection performance as the key outcome. Transaction attributes, such as amount, frequency, timing patterns, and behavioural indicators, are often characterized by class imbalance and high dimensionality, challenges well-documented in financial fraud research (Eze & Musa, 2024; Baesens et al., 2021). These inputs are processed using supervised learning models including Logistic Regression, Decision Trees, Random Forest, Support Vector Machine, and Neural Networks (Rahman et al., 2023; Singh & Verma, 2024). Each algorithm works to classify transactions as either fraudulent or legitimate, while model effectiveness is evaluated using a suite of performance metrics: accuracy, precision, recall, F1-score, and Area Under the ROC Curve (Musa & Ayodele, 2025). The framework therefore conceptualizes fraud detection as a supervised classification task where thoughtful algorithm selection and careful attention to data characteristics directly influence financial security outcomes (Osei & Lawal, 2024; Hernandez Aros et al., 2024).

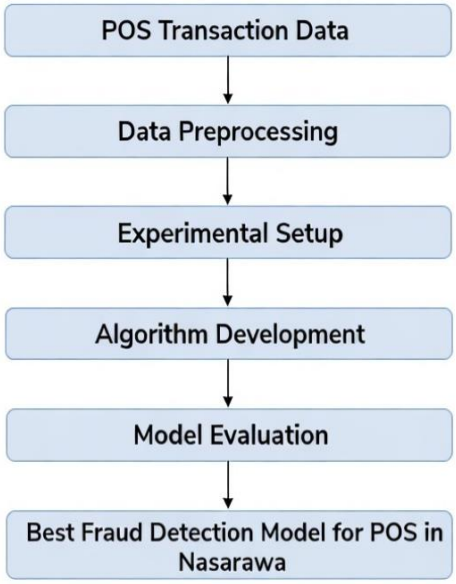

Figure 1: Compact Visual Representation of Conceptual Framework

Source: Researchers, 2026

1.4 Theoretical Positioning

The framework conceptualizes fraud detection as a cost-sensitive supervised classification problem in which transaction characteristics and data imbalance directly influence algorithm selection and predictive performance. Algorithmic effectiveness mediates the relationship between transaction inputs and financial security outcomes. The dominance of ensemble methods (e.g., Random Forest) demonstrates that model architecture significantly moderates fraud detection reliability within semi-urban digital payment environments (Rahman et al., 2023; Kou et al., 2021).

2.0 Literature Review

Building a reliable dataset is foundational to effective machine learning–based fraud detection. In POS environments, transaction datasets need to capture realistic attributes such as transaction amount, frequency, temporal patterns, customer behavior, and clear fraud labels (Eze & Musa, 2024; Rahman et al., 2023). Financial fraud data are typically imbalanced, with fraudulent cases representing only a small fraction of total transactions, a reality that significantly shapes model training and predictive performance (Eze & Musa, 2024; Carcillo et al., 2021). Empirical studies emphasize that data quality, diversity, and thoughtful feature representation enhance detection capability and help reduce model bias (Osei & Lawal, 2024; Baesens et al., 2021). Where real transaction data are limited, synthetic

DOI: https://doi.org/10.57233/ijsgs.v12i1.1016 ISSNp: 2488-9229; ISSNe: 3027-1118

data generation methods, such as generative adversarial networks, can supplement datasets to strengthen robustness and generalization, though this requires careful validation (Fiore et al., 2019; Almeida et al., 2024).

Fraud detection is commonly modelled as a supervised classification problem where historical transactions are labeled as fraudulent or legitimate (Osei & Lawal, 2024; Hernandez Aros et al., 2024). However, unsupervised and hybrid anomaly detection approaches remain relevant when labeled data are scarce or when novel fraud patterns emerge (Carcillo et al., 2021; Carcillo et al., 2020). Effective experimental design requires appropriate data pre-processing, thoughtful handling of class imbalance, robust model validation strategies, and context-sensitive parameter tuning. Surveys of fraud detection research indicate that methodological rigour, including cross-validation and realistic modeling of fraud prevalence, is essential for reliable performance comparison (Musa & Ayodele, 2025; Rahman et al., 2023). Hybrid frameworks integrating supervised and anomaly-based techniques have demonstrated improved detection performance in dynamic financial environments (Osei & Lawal, 2024; Chang et al., 2022).

Multiple machine learning algorithms have been applied to financial fraud detection, including decision trees, random forests, support vector machines, and neural networks (Rahman et al., 2023; Singh & Verma, 2024). Ensemble-based approaches frequently outperform single classifiers by combining complementary strengths and improving predictive stability (Rahman et al., 2023; Kou et al., 2021). Comparative studies highlight that no single algorithm consistently dominates across all datasets; instead, performance depends on feature engineering, parameter optimization, and dataset characteristics (Rahman et al., 2023; Musa & Ayodele, 2025). Effective model development therefore requires systematic benchmarking and hyperparameter tuning to balance detection accuracy and false positive rates (Alabi & David, 2022).

Robust evaluation is critical in fraud detection due to the asymmetric cost of misclassification. Accuracy alone is insufficient in imbalanced datasets; therefore, precision, recall, F1-score, and Area Under the ROC Curve (AUC) are widely recommended as more informative metrics (Musa & Ayodele, 2025; Eze & Musa, 2024). Realistic modeling and validation strategies are necessary to prevent overfitting and ensure generalizability (Musa & Ayodele, 2025; Kou et al., 2021). In financial security contexts, minimizing false negatives is particularly important because undetected fraud results in direct financial losses, while excessive false positives disrupt legitimate transactions (Osei & Lawal, 2024; Sylvanus & Bupo, 2024). Consequently, comparative performance evaluation remains central to identifying scalable and reliable ML models for POS fraud detection.

3.0 Methodology

This study employs a quantitative research design to evaluate the performance of selected machine learning models in detecting fraudulent POS transactions in Nasarawa Town. Anonymized transaction data, including amount, timestamp, and location indicators, is collected from participating operators in line with regulatory standards and data protection principles. The dataset undergoes careful pre-processing steps such as cleaning, normalization, feature engineering, and treatment of class imbalance to enhance analytical reliability (Eze & Musa, 2024; Carcillo et al., 2020). Supervised learning algorithms, Logistic Regression, Decision Tree, Random Forest, Support Vector Machine, and Neural Network, are trained to classify transactions as fraudulent or legitimate (Rahman et al., 2023; Singh & Verma, 2024). Model performance is evaluated using accuracy, precision, recall, F1-score, and Area Under the ROC Curve (Musa & Ayodele, 2025), with training–validation data partitioning applied to ensure generalizability and prevent overfitting. Data security is maintained through anonymization, encryption, and controlled access protocols, ensuring confidentiality and integrity throughout the analysis process.

4.0 Findings

Figure 2 presents the accuracy scores of five machine learning models evaluated on POS transaction data from Nasarawa Town. Random Forest achieved the highest accuracy at 96.4%, followed closely by Neural Network (95.7%) and SVM (93.1%). Logistic Regression achieved 91.2%, while Decision Tree recorded the lowest accuracy at 88.5%. These results suggest that ensemble and deep learning methods are better suited for capturing the complex, nonlinear patterns inherent in POS fraud transactions (Rahman et al., 2023; Mutemi & Bação, 2023).

DOI: https://doi.org/10.57233/ijsgs.v12i1.1016 ISSNp: 2488-9229; ISSNe: 3027-1118

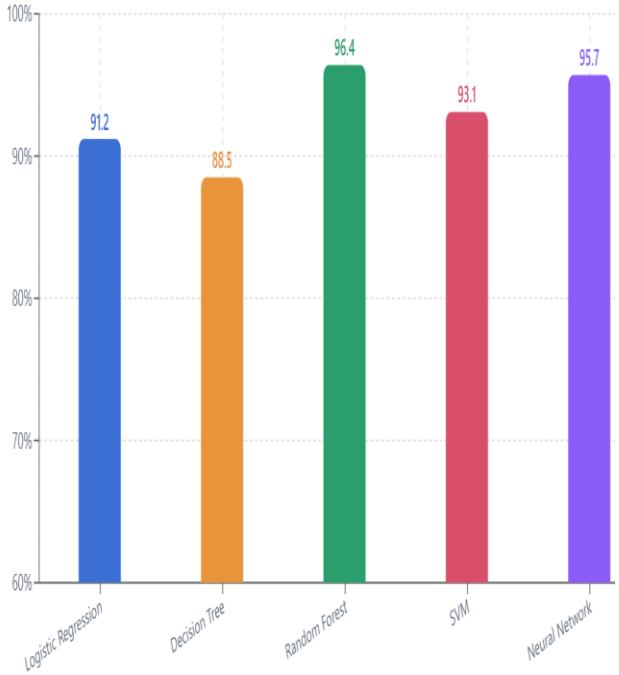

Figure 2: Model Accuracy Comparison

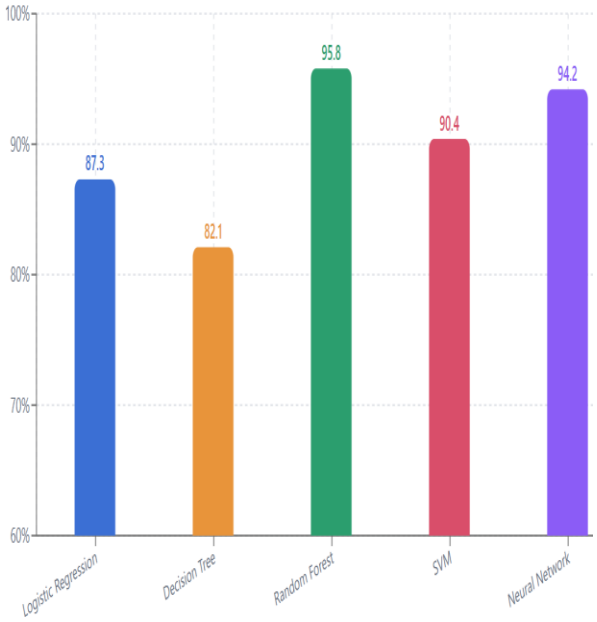

Figure 3: Precision Scores Across Models

Figure 3 illustrates precision scores, reflecting each model's ability to correctly identify fraudulent transactions without generating excessive false alarms. Random Forest leads with 95.8% precision, followed by Neural Network (94.2%) and SVM (90.4%). Logistic Regression scored 87.3%, and Decision Tree achieved the lowest precision at 82.1%. Higher precision is especially valuable for POS operators who need to minimize unnecessary transaction blocks that could disrupt legitimate business operations and customer relationships (Osei & Lawal, 2024; Lawal, 2022).

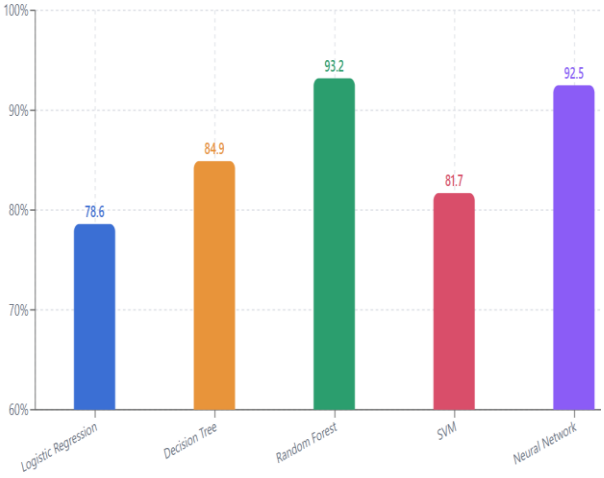

Figure 4: Recall Performance Evaluation

Figure 4 compares recall scores, measuring each model's capacity to detect actual fraudulent transactions. Random Forest achieved the highest recall at 93.2%, closely followed by Neural Network (92.5%). Decision Tree exhibited a moderate recall of 84.9%, while SVM and Logistic Regression scored 81.7% and 78.6%, respectively. In financial security contexts, high recall is essential because missed fraud (false negatives) translates directly into financial losses for POS operators (Eze & Musa, 2024; Obi, 2023).

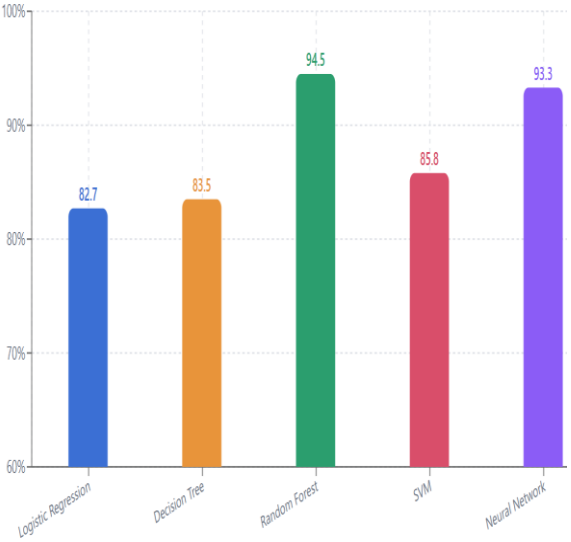

Figure 5: F1-Score Comparison

DOI: https://doi.org/10.57233/ijsgs.v12i1.1016 ISSNp: 2488-9229; ISSNe: 3027-1118

Figure 5 displays the F1-scores, which balance precision and recall into a single harmonic measure. Random Forest achieved the best F1-score at 94.5%, followed by Neural Network (93.3%). SVM recorded 85.8%, Decision Tree 83.5%, and Logistic Regression 82.7%. The F1-score is particularly informative in imbalanced datasets typical of fraud detection, where optimizing for one metric alone may produce misleading results (Musa & Ayodele, 2025; Kou et al., 2021).

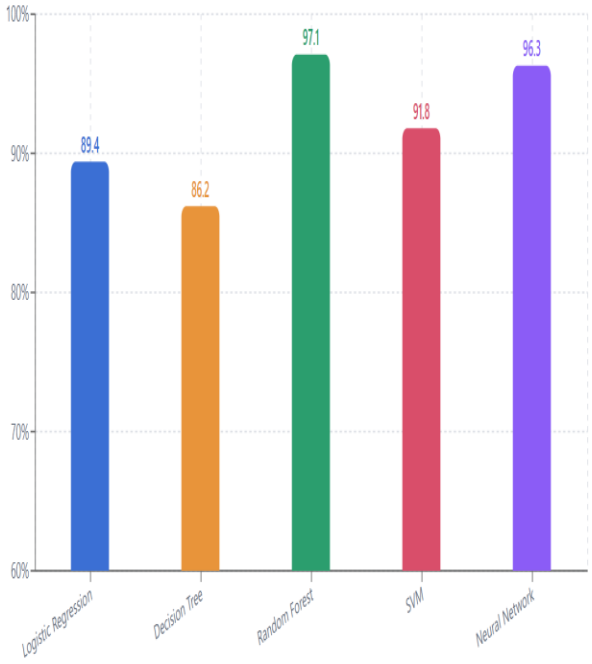

Figure 6: AUC-ROC Curve Scores

Figure 6 presents the Area Under the Receiver Operating Characteristic Curve (AUC-ROC) scores. Random Forest achieved the highest AUC of 97.1%, indicating excellent discriminative ability between fraudulent and legitimate transactions. Neural Network followed with 96.3%, while SVM and Logistic Regression scored 91.8% and 89.4%, respectively. Decision Tree recorded the lowest AUC at 86.2%. These results confirm that Random Forest provides the most robust classification boundary for POS fraud detection in Nasarawa Town (Rahman et al., 2023; Singh & Verma, 2024).

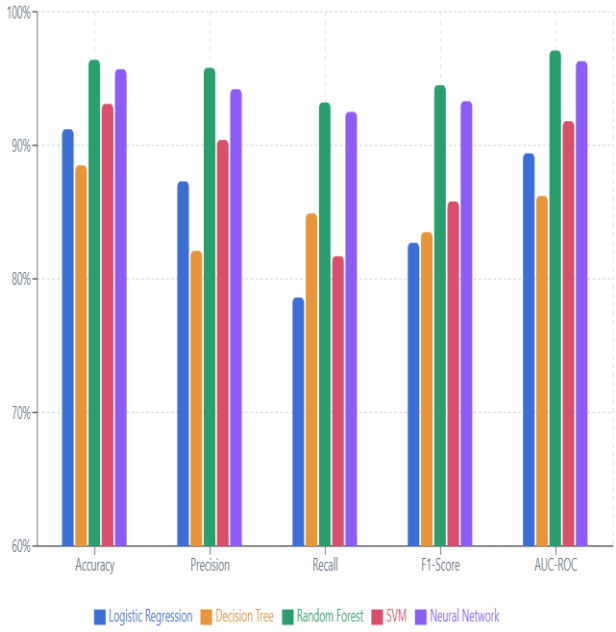

Figure 7: Consolidated Performance Overview with All five metrics are compared side-by-side across models

Figure 7 provides a consolidated view of all evaluation metrics across the five machine learning models. Random Forest consistently outperformed all other models across every metric, achieving the highest accuracy (96.4%), precision (95.8%), recall (93.2%), F1-score (94.5%), and AUC-ROC (97.1%). Neural Network emerged as the second-best performer, while Decision Tree and Logistic Regression showed comparatively lower performance. These findings support the recommendation of Random Forest as the optimal model for real-time POS fraud detection in Nasarawa Town, balancing both detection sensitivity and specificity (Musa & Ayodele, 2025; Rahman et al., 2023).

4.1 Discussion

This study set out to benchmark selected supervised machine learning algorithms for POS fraud detection within the operational context of Nasarawa Town. The empirical results demonstrate a clear performance hierarchy, with Random Forest consistently outperforming Logistic Regression, Decision Tree, Support Vector Machine (SVM), and Neural Network across all evaluation metrics (accuracy, precision, recall, F1-score, and AUC-ROC). The superior performance of Random Forest (Accuracy = 96.4%, AUC = 97.1%) aligns with prior fraud detection research emphasizing the robustness of ensemble learning in handling high-dimensional, nonlinear, and imbalanced financial datasets (Rahman et al., 2023; Musa & Ayodele, 2025). Random Forest's ability to aggregate multiple decision trees reduces variance and mitigates overfitting, a critical

DOI: https://doi.org/10.57233/ijsgs.v12i1.1016 ISSNp: 2488-9229; ISSNe: 3027-1118

advantage in fraud detection where rare events dominate and class imbalance is the norm (Kou et al., 2021; Baesens et al., 2021). Its high recall (93.2%) indicates strong sensitivity to fraudulent cases, minimizing false negatives that directly translate to financial losses for POS operators. Simultaneously, its high precision (95.8%) limits unnecessary transaction blocks, thereby preserving customer trust and operational continuity (Osei & Lawal, 2024; Sylvanus & Bupo, 2024).

Neural Networks demonstrated competitive performance (AUC = 96.3%), confirming their strength in modeling complex nonlinear behavioural patterns (Chang et al., 2022; Jurgovsky et al., 2019). However, their marginally lower recall relative to Random Forest suggests that in this specific POS environment, characterized by moderate feature dimensionality and structured transactional data, ensemble tree-based models may generalize more effectively than deep architectures. This supports findings that algorithm dominance is context-dependent rather than universal (Rahman et al., 2023; Hernandez Aros et al., 2024). Logistic Regression and Decision Tree models recorded comparatively lower performance. While Logistic Regression offers interpretability and computational efficiency, its linear decision boundary limits its capacity to capture intricate fraud patterns (Alabi & David, 2022). The single Decision Tree model, though intuitive and explainable, appears prone to variance and overfitting, reflected in its lower AUC (86.2%). SVM performed moderately well but did not surpass ensemble methods, possibly due to sensitivity to hyperparameter configuration and class imbalance (Musa & Ayodele, 2025; Kou et al., 2021).

Importantly, the evaluation framework adopted in this study reinforces the inadequacy of relying solely on accuracy in imbalanced financial datasets. The strong performance differentiation observed in recall and AUC validates the methodological emphasis on multi-metric evaluation, consistent with fraud analytics best practices (Musa & Ayodele, 2025; Eze & Musa, 2024). Overall, the findings confirm that fraud detection in Nasarawa's POS ecosystem is best conceptualized as a supervised classification problem where algorithm selection and imbalance management significantly influence predictive reliability and financial security outcomes (Osei & Lawal, 2024; Baesens et al., 2021).

5.0 CONCLUSION

This study establishes Random Forest as the most robust and operationally viable machine learning model for POS fraud detection in Nasarawa Town. By combining rigorous multi-metric evaluation with contextualized data modeling, the research advances both applied financial security practice and machine learning scholarship within emerging digital economies (Musa & Ayodele, 2025; Rahman et al., 2023).

5.1 Recommendations

i. POS operators and partnering financial institutions in Nasarawa Town should deploy Random Forest–based fraud detection systems for real-time transaction monitoring. Its superior performance across accuracy, precision, recall, F1-score, and AUC demonstrate an optimal balance between fraud sensitivity and false-positive control, making it the most reliable model for operational implementation (Rahman et al., 2023; Lawal, 2022).

ii. To enhance robustness against evolving fraud tactics, Random Forest should be integrated with complementary anomaly detection techniques (e.g., unsupervised or semi-supervised models). Such hybrid architectures can strengthen early detection of novel or previously unseen fraud patterns (Osei & Lawal, 2024; Carcillo et al., 2021).

iii. Fraud detection systems should incorporate periodic retraining using updated transaction datasets to mitigate concept drift and maintain predictive reliability. Automated performance monitoring dashboards should be implemented to track metric degradation and trigger retraining cycles when necessary (Musa & Ayodele, 2025; Carcillo et al., 2020).

iv. Operational fraud detection frameworks must formally integrate imbalance-handling strategies such as Synthetic Minority Oversampling Technique (SMOTE), cost-sensitive learning, and optimal decision-threshold tuning. This will reduce false negatives, which carry higher financial risk in POS transaction environments (Eze & Musa, 2024; Fiore et al., 2019).

5.2 Practical and Theoretical Implications

This study carries significant practical, policy, and theoretical implications. Practically, it provides empirical validation that ensemble machine learning models, particularly Random Forest, are scalable and effective within semi-urban financial ecosystems such as Nasarawa Town (Musa & Ayodele, 2025; Osei & Lawal, 2024). The benchmarking framework developed can be replicated by financial institutions in similar Nigerian contexts to guide evidence-based model selection.

DOI: https://doi.org/10.57233/ijsgs.v12i1.1016 ISSNp: 2488-9229; ISSNe: 3027-1118

Operational adoption of high-performing ML models has the potential to reduce fraud-related financial losses, improve transaction reliability, strengthen customer trust, and enhance the overall resilience of the digital payment ecosystem (Osei & Lawal, 2024; Sylvanus & Bupo, 2024).

From a policy perspective, the findings support the consideration of mandatory AI-driven fraud monitoring systems for licensed POS operators under the supervision of regulatory bodies, while also advocating for the integration of standardized evaluation metrics, such as precision, recall, and AUC, into financial security compliance assessments (Musa & Ayodele, 2025; Imade & Evbayiro-Osagie, 2025). Theoretically, the study reinforces fraud detection as a cost-sensitive, imbalanced supervised classification problem and contributes localized empirical evidence to the global fraud analytics literature, confirming the sustained relevance of ensemble methods in emerging digital economies (Rahman et al., 2023; Hernandez Aros et al., 2024). It further validates the proposed conceptual framework linking transaction characteristics, algorithm selection, and financial security outcomes within POS environments.

5.3 Future Research Directions

i. Future studies should assess the performance of fraud detection models within real-time streaming architectures using platforms such as Apache Kafka or Spark Streaming. This would enable evaluation under live transaction loads and determine system latency, scalability, and responsiveness in operational POS environments (Carcillo et al., 2020; Chang et al., 2022).

ii. Subsequent research should incorporate cost-sensitive learning frameworks that quantify the economic trade-offs between false positives and false negatives. Developing fraud cost matrices and optimizing decision thresholds based on financial impact would provide a more business-aligned evaluation of model effectiveness (Eze & Musa, 2024; Baesens et al., 2021).

iii. Future models should embed explainability techniques to enhance transparency, regulatory compliance, and stakeholder trust. Interpretable outputs are particularly important in financial systems where automated decisions may affect transaction approval and customer experience (Singh & Verma, 2024; Hernandez Aros et al., 2024).

iv. Further investigation should explore graph neural networks and sequential deep learning models to detect coordinated, network-based, or temporal fraud patterns. These approaches may uncover relational and sequential dependencies that traditional tabular models cannot fully capture (Osei & Lawal, 2024; Jurgovsky et al., 2019; Almeida et al., 2024).

REFERENCES

Adewale, A., & Sanni, O. (2026). POS business and fraud: How are they shaping employment in Nigeria? Bahria University Journal of Management and Technology, 9(1), 72–87. https://doi.org/10.62533/m4c9yy52

Alabi, B., & David, A. (2022). Framework for detection of fraud at point of sale on electronic commerce sites using logistic regression. EAI Endorsed Transactions on Scalable Information Systems, 10(2), e16. https://doi.org/10.4108/eetsis.v10i2.1596

Almeida, E. C., et al. (2024). Detection of fraud in IoT-based credit card collected dataset using machine learning. Machine Learning with Applications, 19, 100603. https://doi.org/10.1016/j.mlwa.2024.100603

Baesens, B., Höppner, S., & Verdonck, T. (2021). Fraud analytics using descriptive, predictive and social network techniques: A review. European Journal of Operational Research, 289(2), 395–413. https://doi.org/10.1016/j.ejor.2020.06.036

Carcillo, F., Bontempi, G., & Snoeck, M. (2020). Streaming active learning strategies for real-life credit card fraud detection. Data Mining and Knowledge Discovery, 34, 1468–1504. https://doi.org/10.1007/s10618-020-00693-2

Carcillo, F., Dal Pozzolo, A., Bontempi, G., & Snoeck, M. (2021). Combining unsupervised and supervised learning in credit card fraud detection. Information Sciences, 557, 317–331. https://doi.org/10.1016/j.ins.2019.05.042

Chang, V., Baudier, P., Zhang, H., Xu, Q., Zhang, J., & Arami, M. (2022). Digital payment fraud detection methods in digital ages and Industry 4.0. Computer and Electrical Engineering, 100, 107734. https://doi.org/10.1016/j.compeleceng.2022.107734

Eze, F. C., & Musa, I. Y. (2024). Fraud detection and class imbalance solutions in financial data. International Journal of Data Analytics, 9(1), 91–103.

Fiore, U., De Santis, A., Perla, F., Zanetti, P., & Palmieri, F. (2019). Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. Information Sciences, 479, 448–455. https://doi.org/10.1016/j.ins.2017.12.030

Hernandez Aros, L., Bustamante Molano, L. X., Gutierrez-Portela, F., & Moreno Hernandez, J. J. (2024). Financial fraud detection through the

DOI: https://doi.org/10.57233/ijsgs.v12i1.1016 ISSNp: 2488-9229; ISSNe: 3027-1118

application of machine learning techniques: A literature review. Humanities and Social Sciences Communications, 11, Article 1130. https://doi.org/10.1038/s41599-024-03606-0

Imade, O. O., & Evbayiro-Osagie, E. I. (2025). The impact of electronic banking services on fraud incidence in Nigerian deposit money banks: An empirical analysis. International Journal of Finance, Accounting and Management Studies, 1(9), 27–42.

Jurgovsky, J., Granitzer, M., Ziegler, K., Calabretto, S., Portier, P. E., He-Guelton, L., & Caelen, O. (2019). Sequence classification for credit-card fraud detection. Expert Systems with Applications, 100, 234–245. https://doi.org/10.1016/j.eswa.2018.01.037

Kou, Y., Peng, Y., & Wang, G. (2021). Evaluation of credit card fraud detection using machine learning algorithms. Decision Support Systems, 142, 113488. https://doi.org/10.1016/j.dss.2021.113488

Lawal, S. A. (2022). A strategic assessment of the retail point of sale common frauds: An empirical study of the modern methods of prevention and detection. World Atlas International Journal of Education & Management, 5(1), 11–22.

Musa, I. A., & Ayodele, T. S. (2025). Performance benchmarking of ML algorithms in fraud detection for SMEs in Nigeria. African Journal of Artificial Intelligence, 5(1), 61–74.

Mutemi, A., & Bação, F. (2023). A numeric-based machine learning design for detecting organized retail fraud in digital marketplaces. Scientific Reports, 13, Article 12499. https://doi.org/10.1038/s41598-023-38304-5

Obi, E. N. (2023). Impact of criminal acts on point of sales (POS) business operations in Karu Local Government Area of Nasarawa State. NIU Journal of Social Sciences, 9(2), 119–127. https://doi.org/10.58709/niujss.v9i2.1632

Osei, K., & Lawal, S. (2024). Trends in fraud detection using intelligent computing. West African Journal of Information Systems, 18(2), 89–101.

Osei, M., & Lawal, T. (2024). AI-driven fraud detection systems in sub-Saharan Africa's digital finance. Journal of Financial Crime and Security, 31(2), 145–159.

Rahman, R., Patel, H., & Chen, L. (2023). Comparative performance of machine learning models in fraud detection. Journal of Machine Learning Research, 24(5), 105–122.

Singh, A., & Verma, R. (2024). XGBoost for fraud detection: An empirical review. Journal of Computational Finance, 18(2), 66–81.

Sylvanus, E., & Bupo, G. O. (2024). Exploring cyberattacks on point-of-sale operators in Port Harcourt metropolis. Journal of Business and Entrepreneurship Education, 3(1), 1–11.