*FUDMA Journal of Sciences (FJS)*
*ISSN online: 2616-1370*
*ISSN print: 2645 - 2944*
*Vol. 10 No. 12, June, 2026, pp 79 – 84*
*DOI:* https://doi.org/10.33003/fjs-2026-1012-5285

# A Systematic Ablation-Based Optimisation Protocol for Convolutional Neural Networks in Electronic Banking Fraud Detection

***[1]Karen Ochuwa Ohwomado, [1]Maureen Ifeanyi Akazue and [2]Arnold Adimabua Ojugo**

[1] Department of Computer Science, Delta State University, Abraka, Delta State, Nigeria.
[2]Department of Computer Science, College of Science, Federal University of Petroleum Resources, Effurun, Delta State, Nigeria.

*Corresponding authors' email: karenohwomado@gmail.com

**Received:** 15th June, 2026
**Accepted:** 13th July, 2026
**Published:** 28th July. 2026

**ABSTRACT**
Reliable deep learning for electronic banking fraud detection remains constrained by extreme class imbalance. Standard evaluation methods frequently struggle because convolutional network choices are often assessed alongside simultaneous methodological modifications, making it difficult to determine the independent contribution of architectural design decisions. To address this problem, this study introduces the Systematic Ablation-Based Optimisation Protocol (SAOP) as a controlled evaluation framework. The protocol examines predefined CNN variations in convolutional depth and dropout regularisation under identical preprocessing, resampling, training, and evaluation conditions. Empirical testing relied on the Credit Card Fraud Detection benchmark dataset, which contains 284,807 transactions with an explicit fraud prevalence of 0.172%. Within this heavily skewed search space, internal ablation results indicate that dropout regularisation variations exerted a more measurable influence on performance than changes in convolutional depth. The proposed CNN was benchmarked against traditional machine learning models using stratified five-fold cross-validation. This architecture achieved a mean accuracy of 0.9988 ± 0.0003, a Matthews Correlation Coefficient (MCC) of 0.7081, a Receiver Operating Characteristic–Area Under the Curve (ROC-AUC) of 0.9659, and a Log Loss of 0.0104. The CNN recorded both the highest MCC and the lowest Log Loss among all evaluated models, showing stable minority-class discrimination alongside reliable probability calibration. These results indicate that architectural design choices remain an important consideration in CNN-based fraud detection under severe class imbalance.

**Keywords:** Class imbalance, deep learning, regularisation, minority-class detection, synthetic oversampling

## INTRODUCTION

The European Banking Authority (EBA, 2023) reported losses of €4.3 billion in 2022 and €2.0 billion during the first half of 2023, while global fraud losses reached USD 485.6 billion in 2023 (Nasdaq Verafin, 2024). These figures highlight the continuing scale of electronic payment fraud. Electronic banking fraud detection continues to face several methodological challenges despite advances in automated detection systems. One challenge arises from high-dimensional transactional data, which frequently require tree-based ensembles to capture complex feature interactions (Baisholan et al., 2025). Extreme class imbalance presents another difficulty because legitimate transactions greatly outnumber fraudulent ones, and minority-class oversampling is often applied (Du et al., 2024). Real-time, high-confidence decision requirements introduce an additional constraint, as high fraud-risk scores can trigger card blocking and increase the cost of false-positive predictions (Dal **P**ozzolo et al., 2017).

Early fraud detection systems depended on rigid, set rules and criteria that were difficult to maintain (Bolton & Hand, 2004). Subsequent studies introduced machine learning–based approaches to improve fraud detection performance (Ojugo et al., 2015). As transaction volumes and complexity rose, transaction-level systems evolved; however, these systems frequently analysed transactions in isolation (Whitrow et al., 2009). Concept drift, excessive class imbalance, and delayed supervision became significant impediments to successful fraud detection (Dal Pozzolo et al., 2017).

Severe class imbalance significantly complicates model evaluation. Conventional metrics such as accuracy and F1-score may appear high while providing little insight into minority-class (fraud) detection performance, particularly when fraud incidence is extremely low (Sun et al., 2025). This limitation motivates the use of recall-oriented and precision–recall-based measures (Baisholan et al., 2025), as accuracy-driven learning inherently favors the majority class and exacerbates issues such as class overlap, minor disjuncts, and noise (Carvalho et al., 2025). The Matthews Correlation Coefficient (MCC) provides a balanced evaluation by incorporating all elements of the confusion matrix (Chicco & Jurman**,** 2020).

Class imbalance may be addressed by modifying the training data using sampling procedures, such as upsizing the minority class or reducing the majority class (He & Garcia, 2009), and various strategies have been proposed, including data-level, algorithm-level, and hybrid approaches (Krawczyk, 2016). Among oversampling techniques, SMOTE produces synthetic minority-class examples rather than repeating existing instances (Chawla et al., 2002). Recent studies have demonstrated that data resampling techniques can improve detection performance when integrated with ensemble learning models (Okpor et al., 2024).

Borderline-SMOTE focuses on minority-class cases along the class decision boundary (Han et al., 2005). Adaptive Synthetic Sampling (ADASYN) further changes the number of generated minority samples according to the learning difficulty of individual minority occurrences (He et al., 2008). While SMOTE may be effective in low-dimensional settings, prior studies indicate that it may be less effective or introduce misleading correlations in high-dimensional datasets (Blagus & Lusa, 2013). Similarly, cost-sensitive learning overcomes class imbalance by optimising predictions to lower anticipated misclassification costs and may be performed by converting traditional classifiers using cost-proportionate weighting (Elkan, 2001; Zadrozny et al., 2003). ROC curves may be misleading under severely skewed class distributions, as they may hide poor minority-class performance despite high overall scores (Davis & Goadrich, 2006; Saito & Rehmsmeier, 2015). Consequently, different evaluation measures, such as precision–recall curves and the MCC, allow a more realistic assessment of classifier performance under large class imbalance (Chicco & Jurman, 2020).

Hybrid deep-learning frameworks have been adopted to improve credit card fraud detection by combining complementary architectures and imbalance-handling strategies (Aghware et al., 2023; Umaru et al., 2025). Hybrid CNN-based models utilize attention mechanisms with SMOTE oversampling (Akour et al., 2025), convolutional feature processing (Fu et al., 2016), and weighted loss functions combined with undersampling and SMOTE (Ndama et al., 2024). However, despite these advances, such approaches often intertwine architectural design with preprocessing and imbalance-handling techniques, making it difficult to isolate the independent contribution of CNN architecture.

Recent studies have explored fraud detection using machine learning and deep learning techniques, including ensemble-based and hybrid models (Ojugo et al., 2023; Aghware et al., 2023). Related approaches have also been applied in broader cybersecurity domains such as phishing detection, intrusion detection, and anomaly detection (Akazue et al., 2022; Akazue et al., 2024; Ojugo et al., 2012; Ojugo & Ekurume, 2021; Ojugo et al., 2023; Yoro et al., 2025). This methodological coupling highlights a critical limitation in the current literature. Architectural depth, regularisation, and imbalance-handling strategies are frequently modified simultaneously, obscuring causal relationships and limiting reproducibility. Consequently, controlled architecture-focused evaluation frameworks capable of disentangling architectural effects from preprocessing and training variability under realistic fraud detection constraints remain limited.

CNN architectures are routinely inherited or selected heuristically, while oversampling approaches such as SMOTE or GAN-based augmentation are widely utilised despite acknowledged drawbacks relating to noise, unrealistic sample generation, and overfitting risk (Du et al., 2024). Furthermore, improper application of oversampling prior to data partitioning can introduce information leakage and inflate performance estimates. These methodological limitations highlight the absence of a principled, reproducible framework for analysing CNN architectures under extreme class imbalance. To address this limitation, the proposed Systematic Ablation-Based Optimisation Protocol (SAOP) formalises architecture evaluation through the controlled examination of architectural variables while maintaining consistent preprocessing, resampling, optimisation, and evaluation procedures, thereby isolating the effects of architectural design choices. The study focuses on the effects of convolutional depth and dropout regularisation within a controlled experimental setting. The results indicate that dropout regularisation exerts a greater influence on performance than increased convolutional depth within the evaluated search space. In addition, the study evaluates both classification performance and probability calibration using Matthews Correlation Coefficient (MCC) and Log Loss. Overall, the findings demonstrate that a one-dimensional CNN can achieve competitive fraud detection performance under severe class imbalance while maintaining reliable probabilistic predictions.

## MATERIALS AND METHODS

### Data Collection and Description

This study uses the Credit Card Fraud Detection dataset, comprising 284,807 transactions with a fraud prevalence of 0.172%. Each transaction contains 30 numerical features (V1–V28, Time, and Amount) and a binary class label (0: legitimate; 1: fraudulent). The V1–V28 variables are anonymised Principal Component Analysis (PCA) features, while the original Time and Amount attributes are retained as CNN inputs.

### Data Preprocessing

Data preprocessing included integrity checks, feature scaling, and class imbalance handling. All numerical features (Time, Amount, and V1–V28) were standardised using StandardScaler and reshaped to (samples, 30, 1) for one-dimensional convolutional processing. Because fraudulent transactions accounted for only 0.172% of the dataset, SMOTE was applied exclusively to the training data within each cross-validation fold, while the validation data retained its original class distribution. This approach prevented information leakage and enabled evaluation under realistic class imbalance conditions, consistent with recommendations that SMOTE should be applied after data partitioning to avoid artificial correlations and optimistic performance estimates in high-dimensional datasets (Blagus & Lusa, 2013). No additional feature selection was performed, preserving the original feature representation throughout the analysis despite the recognised importance of feature selection and data handling in transactional fraud detection (Akazue et al., 2024; Deborah et al., 2023; Akazue et al., 2023).

### Systematic Ablation-Based Optimisation Protocol (SAOP)

Figure 1 presents the experimental workflow, including data preprocessing, training-only SMOTE application, architectural analysis, benchmark model evaluation, and performance assessment. The proposed Systematic Ablation-Based Optimisation Protocol (SAOP) evaluates predefined CNN architectural configurations using stratified five-fold cross-validation while maintaining consistent preprocessing, resampling, optimisation, and evaluation procedures. By varying only architectural factors while keeping non-architectural variables constant, the protocol reduces potential confounding effects and provides a structured, reproducible framework for evaluating CNN architectural design choices under controlled conditions.

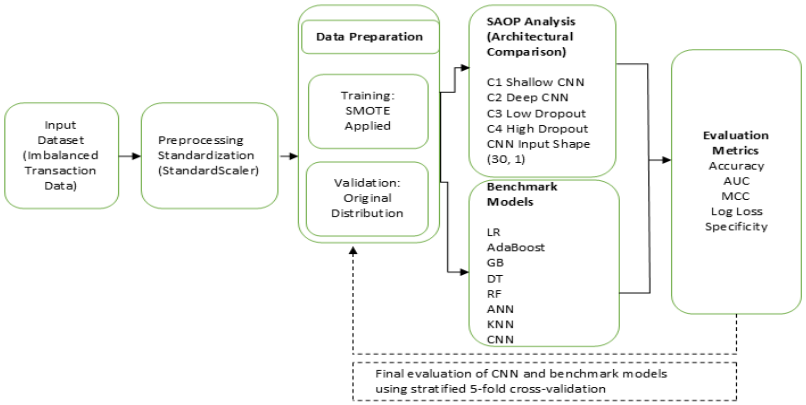


Figure 1: Proposed System Architecture of the SAOP-Based Fraud Detection Framework

**Systematic Ablation-Based Optimisation Protocol (SAOP)**

(Architectural analysis framework)

Input: Imbalanced transaction dataset; fixed preprocessing pipeline; fixed hyperparameters.

Output: Performance comparison of predefined CNN architectural configurations.

Steps:

i. Preprocess the dataset and apply SMOTE exclusively to the training data within each stratified five-fold cross-validation fold.
ii. Define CNN architectural configurations (C1–C4) by varying only convolutional depth or dropout regularisation.
iii. Evaluate each configuration under identical preprocessing, resampling, optimisation, and evaluation settings, recording MCC and other performance metrics.
iv. Compare the configurations to assess the influence of convolutional depth and dropout regularisation.
v. Benchmark the implemented CNN architecture against traditional machine learning models using stratified five-fold cross-validation.

**Training Procedure**

All SAOP configurations were evaluated under identical training conditions using the Adam optimiser (learning rate = 0.001), binary cross-entropy loss, a batch size of 128, and a maximum of 50 epochs. Early stopping monitored validation loss with a patience of five epochs and restored the best model weights. Convolutional depth and dropout regularisation were the only architectural factors varied across the SAOP configurations. Performance was assessed using Accuracy, ROC-AUC, MCC, Log Loss, and Specificity. The experiments were implemented in Python 3.x using TensorFlow 2.x and Keras, with a fixed random seed of 42 for reproducibility.

**Evaluation Framework**

Model performance was evaluated using Accuracy, Precision, Recall, F1-Score, ROC-AUC, Matthews Correlation Coefficient (MCC), and Log Loss, with particular emphasis on MCC and Log Loss because they provide complementary assessments of classification performance and probability estimation under severe class imbalance.

MCC was computed as:

$$MCC = \frac{(TP \times TN) - (FP \times FN)}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}} \quad (1)$$

Where TP, TN, FP, and FN denote true positives, true negatives, false positives, and false negatives, respectively. For benchmarking, the implemented CNN architecture was benchmarked against Logistic Regression (LR), Decision Tree (DT), Random Forest (RF), k-Nearest Neighbors (KNN), AdaBoost, Gradient Boosting (GB), and an Artificial Neural Network (ANN).

**Implemented CNN Architecture**

The CNN implemented in this study used a one-dimensional input shape of (30, 1), followed by a Conv1D layer with 32 filters and a kernel size of 3, and a MaxPooling1D layer with a pool size of 2. The extracted feature maps were flattened and passed to a 64-neuron dense layer with ReLU activation, followed by a single sigmoid output unit for fraud probability estimation.

## RESULTS AND DISCUSSION

**Results of the Systematic Ablation-Based Optimisation Protocol (SAOP)**

Configuration C4 (High Dropout) achieved the highest MCC of 0.7602, compared with 0.6983 for C3 (Low Dropout), indicating better classification balance with increased dropout regularisation. In contrast, increasing convolutional depth did not improve performance, as C1 (Shallow CNN) achieved an MCC of 0.7294 compared with 0.6961 for C2 (Deep CNN). Overall, dropout regularisation produced a greater performance variation than convolutional depth within the evaluated configurations, with C4 emerging as the best-performing configuration.

**Table 1: SAOP Ablation Configurations Evaluated Using Stratified Five-Fold Cross-Validation for Architectural Analysis**

| Configuration | Variant description | No. of conv. layers | SMOTE | Dropout | MCC |
|---|---|---|---|---|---|
| C1 | Shallow CNN | 1 | Yes | 0.2 | 0.7294 |
| C2 | Deep CNN | 2 | Yes | 0.2 | 0.6961 |
| C3 | Low Dropout | 2 | Yes | 0.1 | 0.6983 |
| C4 | High Dropout | 2 | Yes | 0.3 | 0.7602 |

**Model Selection and Final Evaluation**

Among the evaluated architectural variants, C4 (High Dropout) recorded the highest MCC (0.7602), as shown in Table 1. The best-performing configuration was subsequently benchmarked against established machine learning models under the same evaluation framework, with the comparative results presented in Table 2.

**Table 2. Independent Five-Fold Cross-Validation Results of the Proposed CNN and Benchmark Models**

| z | Mean Accuracy (CV) | AUC | MCC | Log Loss | Specificity |
|---|---|---|---|---|---|
| LR | 0.9748 ± 0.0014 | 0.9774 | 0.2288 | 0.1125 | 0.9749 |
| AdaBoost | 0.9660 ± 0.0030 | 0.9726 | 0.1957 | 0.5375 | 0.9661 |
| GB | 0.9871 ± 0.0015 | 0.9772 | 0.3100 | 0.0592 | 0.9873 |
| DT | 0.9880 ± 0.0009 | 0.9037 | 0.3082 | 0.0570 | 0.9882 |
| RF | 0.9983 ± 0.0002 | 0.9825 | 0.6534 | 0.0445 | 0.9985 |
| ANN | 0.9973 ± 0.0003 | 0.9665 | 0.5958 | 0.0151 | 0.9980 |
| KNN | 0.9980 ± 0.0002 | 0.9294 | 0.6290 | 0.0294 | 0.9983 |
| Proposed CNN | 0.9988 ± 0.0003 | 0.9659 | 0.7081 | 0.0104 | 0.9991 |

As shown in Table 2, the proposed CNN achieved a mean cross-validation accuracy of 0.9988 ± 0.0003, an MCC of 0.7081, an AUC of 0.9659, and a Log Loss of 0.0104, indicating strong performance under severe class imbalance and reliable probability estimation. Among the benchmark models (Table 2), the proposed CNN achieved the highest MCC (0.7081), followed by Random Forest (0.6534) and KNN (0.6290). It also recorded the lowest Log Loss (0.0104), demonstrating the strongest overall balance between classification performance and reliable probability estimation under severe class imbalance.

The confusion matrix in Figure 2 shows that the proposed CNN correctly identified 421 fraudulent transactions while failing to detect 71. Among legitimate transactions, 283,791 were correctly classified and 524 were incorrectly flagged as fraudulent, indicating strong minority-class detection with a low false-positive rate.

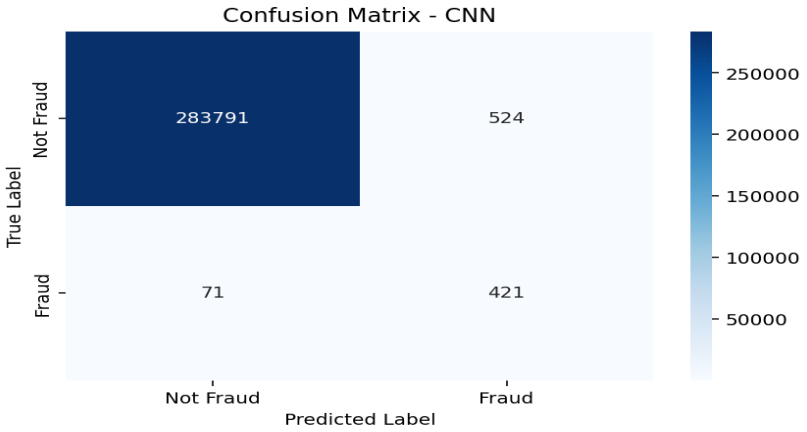


Figure 2: Confusion Matrix of the Proposed CNN Model, Illustrating Classification Performance across Fraudulent and Legitimate Transaction Classes under Extreme Class Imbalance

**Discussion**

A persistent challenge in electronic banking fraud detection research is the difficulty of isolating the contribution of CNN architecture from preprocessing and resampling strategies. The proposed Systematic Ablation-Based Optimisation Protocol (SAOP) provides a structured framework for addressing this challenge by enabling observed performance differences to be interpreted primarily as architectural effects rather than methodological variations. The use of a benchmark dataset further supports reproducibility and comparison with previous studies, while future work may evaluate the framework using evolving or streaming financial datasets.

Variations in dropout regularisation produced larger differences in MCC than changes in convolutional depth, indicating that regularisation exerted a stronger influence on minority-class discrimination within the evaluated configurations. These findings highlight the importance of appropriate regularisation when designing CNN models for severely imbalanced fraud detection tasks. The proposed CNN achieved the highest MCC (0.7081) among the evaluated models, outperforming Random Forest (0.6534) and KNN (0.6290). Although Random Forest achieved the highest ROC-AUC (0.9825), the proposed CNN produced the lowest Log Loss (0.0104), indicating stronger minority-class discrimination and more reliable probability estimation under severe class imbalance.

These findings are consistent with previous studies reporting strong deep learning performance for fraud detection (Ojugo et al., 2023; Aghware et al., 2023**).** However, the present study demonstrates that a one-dimensional CNN can achieve competitive performance without relying on hybrid architectures or extensive feature engineering.

Overall, the findings demonstrate that careful CNN architectural design, combined with a controlled evaluation framework, can improve fraud detection performance under severe class imbalance while providing a fair and reproducible basis for comparison with established machine learning models.

## CONCLUSION

This study evaluated a one-dimensional Convolutional Neural Network (CNN) for electronic banking fraud detection under extreme class imbalance using the proposed Systematic Ablation-Based Optimisation Protocol (SAOP). The proposed CNN achieved the highest Matthews Correlation Coefficient (0.7081) and the lowest Log Loss (0.0104) among the evaluated models, demonstrating that competitive fraud detection performance can be achieved without hybrid architectures or extensive feature engineering. The proposed SAOP further provides a structured, fair, and reproducible framework for evaluating CNN-based fraud detection models under severe class imbalance.

## REFERENCES

European Banking Authority. (2023). *EBA report on payment fraud data under the PSD2 framework*. https://www.eba.europa.eu

Nasdaq Verafin. (2024). *2024 global financial crime report*. https://www.nasdaq.com/global-financial-crime-report

Baisholan, N., Dietz, J. E., Gnatyuk, S., Turdalyuly, M., Matson, E. T., & Baisholanova, K. (2025). A systematic review of machine learning in credit card fraud detection under original class imbalance. *Computers*, *14*(10), 437. https://doi.org/10.3390/computers14100437

Du, H., Lv, L., Wang, H., & Guo, A. (2024). A novel method for detecting credit card fraud problems. *PLOS ONE*, *19*(3), e0294537. https://doi.org/10.1371/journal.pone.0294537

Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2017). Credit card fraud detection: A realistic modeling and a novel learning strategy. *IEEE Transactions on Neural Networks and Learning Systems*, *29*(8), 3784–3797. https://doi.org/10.1109/TNNLS.2017.2736643

Bolton, R. J., & Hand, D. J. (2002). Statistical fraud detection: A review. *Statistical Science*, *17*(3), 235–249. https://doi.org/10.1214/ss/1042727940

Ojugo, A. A., Oyemade, D. A., Allenotor, D., Longe, O. B., & Anujeonye, C. N. (2015). Comparative stochastic study for credit-card fraud detection models. *African Journal of Computing & ICT*, *8*(1), 15–24.

Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. M. (2009). Transaction aggregation as a strategy for credit card fraud detection. *Data Mining and Knowledge Discovery*, *18*(1), 30–55. https://doi.org/10.1007/s10618-008-0116-z

Sun, W., Shen, Q., Gao, Y., Mao, Q., Qi, T., & Xu, S. (2025). Objective over architecture: Fraud detection under extreme imbalance in bank account opening. *Computation*, *13*(12), 290. https://doi.org/10.3390/computation13120290

Carvalho, M., Pinho, A. J., & Brás, S. (2025). Resampling approaches to handle class imbalance: A review from a data perspective. *Journal of Big Data*, *12*(1), 71. https://doi.org/10.1186/s40537-025-01119-4

Chicco, D., & Jurman, G. (2020). The advantages of the Matthews correlation coefficient (MCC) over F1 score and accuracy in binary classification evaluation. *BMC Genomics*, *21*(1), 6. https://doi.org/10.1186/s12864-019-6413-7

He, H., & Garcia, E. A. (2009). *Learning from imbalanced data*. *IEEE Transactions on Knowledge and Data Engineering*, *21*(9), 1263–1284. https://doi.org/10.1109/TKDE.2008.239

Krawczyk, B. (2016). Learning from imbalanced data: Open challenges and future directions. *Progress in Artificial Intelligence*, *5*(4), 221–232. https://doi.org/10.1007/s13748-016-0094-0

Chawla, N. V., Bowyer, K. W., Hall, L. O., & Kegelmeyer, W. P. (2002). SMOTE: Synthetic minority over-sampling technique. *Journal of Artificial Intelligence Research*, *16*, 321–357. https://doi.org/10.1613/jair.953

Okpor, M. D., Aghware, F. O., Akazue, M. I., Eboka, A. O., Ako, R. E., Ojugo, A. A., Odiakaose, C. C., Binitie, A. P., Geteloma, V. O., & Ejeh, P. O. (2024). Pilot study on enhanced detection of cues over malicious sites using data balancing on the Random Forest ensemble. *Journal of Future Artificial Intelligence and Technologies*, *1*(2), 109–123. https://doi.org/10.62411/faith.2024-14

Han, H., Wang, W.-Y., & Mao, B.-H. (2005). Borderline-SMOTE: A new over-sampling method in imbalanced data sets learning. In *Proceedings of the International Conference on Intelligent Computing* (pp. 878–887). Springer. https://doi.org/10.1007/11538059_91

He, H., Bai, Y., Garcia, E. A., & Li, S. (2008). ADASYN: Adaptive synthetic sampling approach for imbalanced learning. In *Proceedings of the 2008 IEEE International Joint Conference on Neural Networks* (pp. 1322–1328). IEEE. https://doi.org/10.1109/IJCNN.2008.4633969

Blagus, R., & Lusa, L. (2013). SMOTE for high-dimensional class-imbalanced data. *BMC Bioinformatics*, *14*(1), 106. https://doi.org/10.1186/1471-2105-14-106

Elkan, C. (2001). The foundations of cost-sensitive learning. In *Proceedings of the 17th International Joint Conference on Artificial Intelligence (IJCAI-01)* (Vol. 1, pp. 973–978). Morgan Kaufmann Publishers.

Zadrozny, B., Langford, J., & Abe, N. (2003). Cost-sensitive learning by cost-proportionate example weighting. In *Proceedings of the Third IEEE International Conference on Data Mining (ICDM 2003)* (pp. 435–442). IEEE. https://doi.org/10.1109/ICDM.2003.1250950

Davis, J., & Goadrich, M. (2006). The relationship between precision-recall and ROC curves. In *Proceedings of the 23rd International Conference on Machine Learning (ICML '06)* (pp. 233–240). Association for Computing Machinery. https://doi.org/10.1145/1143844.1143874

Saito, T., & Rehmsmeier, M. (2015). The precision-recall plot is more informative than the ROC plot when evaluating binary classifiers on imbalanced datasets. *PLOS ONE*, *10*(3), e0118432. https://doi.org/10.1371/journal.pone.0118432

Aghware, F. O., Yoro, R. E., Ejeh, P. O., Odiakaose, C. C., Emordi, F. U., & Ojugo, A. A. (2023). DeLClustE: Protecting users from credit-card fraud transaction via the deep-learning cluster ensemble. *International Journal of Advanced Computer Science and Applications*, *14*(6). https://doi.org/10.14569/IJACSA.2023.0140610

Umaru, I. A., Aliyu, A. A., Ibrahim, M., Abdulkadir, S., Ahmed, M. A., Abubakar, M. A., Ahmed, A. A., & Tanko, S. A. (2025). An enhanced hybrid model combining LSTM, ResNet, and an attention mechanism for credit card fraud detection. *FUDMA Journal of Sciences*, *9*(2), 42–48. https://doi.org/10.33003/fjs-2025-0902-3072

Akour, I., Mohamed, N., & Salloum, S. (2025). Hybrid CNN-LSTM with attention mechanism for robust credit card fraud detection. *IEEE Access*, *13*, 114056–114068. https://doi.org/10.1109/ACCESS.2025.3583253

Fu, K., Cheng, D., Tu, Y., & Zhang, L. (2016). Credit card fraud detection using convolutional neural networks. In *Neural Information Processing: Proceedings of the 23rd International Conference on Neural Information Processing (ICONIP 2016)* (pp. 483–490). Springer International Publishing. https://doi.org/10.1007/978-3-319-46675-0_53

Ndama, O., Bensassi, I., & En-Naimi, E. M. (2024). Optimizing credit card fraud detection: A deep learning approach to imbalanced datasets. *International Journal of Electrical and Computer Engineering*, *14*(4), 4802–4814. https://doi.org/10.11591/ijece.v14i4.pp4802-4814

Ojugo, A. A., Akazue, M. I., Ejeh, P. O., Ashioba, N. C., Odiakaose, C. C., Ako, R. E., & Emordi, F. U. (2023). Forging a user-trust memetic modular neural network card fraud detection ensemble: A pilot study. *Journal of Computational Theory and Applications*, *1*(2), 50–60. https://doi.org/10.33633/jcta.v1i2.9259

Akazue, M. I., Ojugo, A. A., Yoro, R. E., Malasowe, B. O., & Nwankwo, O. (2022). Empirical evidence of phishing menace among undergraduate smartphone users in selected universities in Nigeria. *Indonesian Journal of Electrical Engineering and Computer Science*, *28*(3), 1756–1765. https://doi.org

Akazue, M. I., Ahweyevu, K. O., Ogeh, C. O., & Asuai, C. (2024). Development of a real-time phishing detection website via a triumvirate of information retrieval, natural language processing, and machine learning modules. *International Journal of Trend in Research and Development*. http://www.ijtrd.com

Ojugo, A. A., Eboka, A. O., Okonta, O. E., Yoro, R. E., & Aghware, F. O. (2012). Genetic algorithm rule-based intrusion detection system (GAIDS). *Journal of Emerging Trends in Computing and Information Sciences*. http://www.cisjournal.org

Ojugo, A. A., & Ekurume, E. (2021). Deep learning network anomaly-based intrusion detection ensemble for predictive intelligence to curb malicious connections: An empirical evidence. *International Journal of Advanced Trends in Computer Science and Engineering*, *10*(3), 2090–2102. https://doi.org/10.30534/ijatcse/2021/851032021

Ojugo, A. A., Akazue, M. I., Ejeh, P. O., Odiakaose, C. C., & Emordi, F. U. (2023). DeGATraMoNN: Deep learning memetic ensemble to detect spam threats via a content-based processing. *Kongzhi yu Juece (Control and Decision)*. https://www.researchgate.net/publication/374874600_DeGATraMoNN_Deep_learning_memetic_ensemble_to_detect_spam_threats_via_a_content-based_processing

Yoro, R. E., Ojugo, A. A., Akazue, M. I., Ejeh, P. O., Odiakaose, C. C., Aghware, F. O., Emordi, F. U., & Okpor, M. D. (2025). Adaptive DDoS detection model in software-defined SIP-VoIP using transfer learning with boosted meta-learner. *PLOS ONE*, *20*(6), e0326571. https://doi.org/10.1371/journal.pone.0326571

Akazue, M. I., Ojugo, A. A., Ejeh, P. O., Odiakaose, C. C., Aghware, F. O., Emordi, F. U., Yoro, R. E., & Ako, R. E. (2024). Handling transactional data features via associative rule mining for mobile online shopping platforms. *International Journal of Advanced Computer Science and Applications*, *15*(3). https://doi.org/10.14569/IJACSA.2024.0150354

Deborah, O., Maureen, A., & Anthony, I. (2023). A framework for feature selection using data value metric and genetic algorithm. *International Journal of Computer Applications*, *184*(43), 14–21. https://doi.org/10.5120/ijca2023922533

Akazue, M. I., Debekeme, I. A., Edje, A. E., Asuai, C., & Osame, U. J. (2023). Unmasking fraudsters: Ensemble feature selection to enhance Random Forest fraud detection. *Journal of Computational Theory and Applications*, *1*(2), 201–211. https://doi.org/10.33633/jcta.v1i2.9462