Clean Energy and Smart Technology
Volume 03, Number 02, April 2025
DOI : https://doi.org/10.58641/
e-ISSN : 2964-2647

THE APPLICATION OF XGBOOST CLASSIFICATION FOR FRAUD DETECTION IN CREDIT CARD TRANSACTIONS

Muhamad Fuat Asnawi[1)*], Nur Fitriyanto[2)], M. Agoeng Pamoengkas[3)]
[1)] Universitas Sains Al-Qur'an, Indonesia
[2) 3)] Universitas Amikom Yogyakarta, Indonesia
[1)]fuatasnawi@unsiq.ac.id, [2)]nur.fitriyanto@students.amikom.ac.id, [3)]agoeng@students.amikom.ac.id

* fuatasnawi@unsiq.ac.id

Submitted :16 April 2025 | **Accepted** : 25 April 2025 | **Published** : 30 April 2025

Abstract: Credit card fraud detection remains a critical challenge due to the inherent imbalance in transaction datasets, where fraudulent transactions are significantly fewer than normal ones. This study investigates the application of the XGBoost classification algorithm to address this issue using the publicly available Kaggle Credit Card Fraud Detection dataset. The research incorporates data preprocessing techniques such as normalization and SMOTE to handle the dataset's imbalance. Hyperparameter tuning using GridSearchCV optimizes the model's parameters, enhancing its performance. The results indicate that the model achieves an Area Under the Curve (AUC) of 0.97, demonstrating its high accuracy in distinguishing between fraudulent and normal transactions. The evaluation metrics reveal an F1-score of 0.77 for fraudulent transactions, showing the model's reasonable effectiveness in detecting fraud. While the model performs exceptionally well in identifying normal transactions, reducing false negatives remains a challenge. This study underscores the potential of combining advanced machine learning techniques with preprocessing and optimization strategies to develop robust fraud detection systems.

Keywords: Credit card fraud, XGBoost, Machine learning, Imbalanced dataset, SMOTE, Fraud detection

1. INTRODUCTION

The exponential growth of digital transactions has brought significant advancements in global financial systems, yet it has also introduced unprecedented challenges, particularly in combating fraud. Credit card fraud, one of the most pervasive forms of financial crime, has resulted in billions of dollars in losses annually, affecting both consumers and financial institutions (Raval et al., 2023; Salekshahrezaee et al., 2023). In 2022, global losses from credit card fraud were estimated to exceed $32 billion, with a projected increase in the coming years (Gupta et al., 2022; Hilal et al., 2022; Kumar et al., 2022; Langevin et al., 2022). Detecting credit card fraud is a complex challenge due to the highly imbalanced nature of the datasets, where fraudulent transactions constitute only a small fraction of the total (Chang et al., 2022; Cherif et al., 2023; Mishra & Pandey, 2021). The Credit Card Fraud Detection dataset from Kaggle, for example, contains 284,807 transactions, with only 0.17% labeled as fraudulent (Salekshahrezaee et al., 2023). This imbalance significantly hampers the performance of traditional machine learning models, which often exhibit biases toward the majority class (Dantas et al., 2022).

Clean Energy and Smart Technology
Volume 03, Number 02, April 2025
DOI : https://doi.org/10.58641/
e-ISSN : 2964-2647

Machine learning (ML) has emerged as a powerful tool for fraud detection, offering capabilities to identify subtle patterns in transaction data. Among various ML algorithms, ensemble methods like Extreme Gradient Boosting (XGBoost) have demonstrated exceptional performance due to their ability to handle large, complex datasets with imbalanced classes (Sharma et al., 2021). XGBoost, with its gradient boosting framework, iteratively reduces classification errors and ranks feature importance effectively, making it a popular choice for fraud detection (Trisanto et al., 2021). Addressing data imbalance is a critical aspect of fraud detection systems. Techniques such as Synthetic Minority Oversampling Technique (SMOTE), SMOTE Tomek, and Random Oversampling have been widely adopted to enhance model performance by balancing the dataset (Salekshahrezaee et al., 2023; Sharma et al., 2021). Moreover, advanced feature engineering methods, including Principal Component Analysis (PCA) and autoencoders, further improve the discriminatory power of ML models by reducing dimensionality and retaining essential features (Gupta et al., 2022; Salekshahrezaee et al., 2023).

Deep learning architectures, such as Long Short-Term Memory (LSTM) networks and Graph Neural Networks (GNN), have recently gained traction in credit card fraud detection. These models analyze temporal and spatial dependencies in transaction data, providing a more comprehensive understanding of fraudulent patterns (Cheng et al., 2022; Raval et al., 2023). For instance, the spatial-temporal attention-based GNN framework has been shown to outperform traditional methods by leveraging temporal aggregation and spatial features to detect fraud effectively (Cheng et al., 2022). Explainable AI (XAI) has further enhanced the usability of ML models in fraud detection by providing interpretability for decision-making processes. This transparency is critical for building trust in high-stakes applications such as financial systems (Almazroi & Ayub, 2023; Raval et al., 2023). Studies integrating XAI with LSTM and GNN models have demonstrated improved accuracy and user trust by elucidating the features that influence fraud classification (Raval et al., 2023).

This research focuses on developing an optimized credit card fraud detection framework leveraging XGBoost, integrated with data balancing. The framework will be evaluated on the Kaggle Credit Card Fraud Detection dataset to address challenges such as data imbalance, adaptive fraud patterns, and model scalabilitys (Salekshahrezaee et al., 2023). By benchmarking its performance against traditional and advanced ML models, this study aims to contribute to the ongoing development of robust, efficient, and interpretable fraud detection systems. The detection of credit card fraud has been a critical research area due to the financial and reputational risks it poses to consumers and institutions. Several studies have focused on addressing the challenges of imbalanced datasets, adaptive fraud patterns, and model scalability(Afriyie et al., 2023; Hashemi et al., 2023; Mehbodniya et al., 2023; Singh, Ranjan, et al., 2022).

Raval proposed a trusted explainable LSTM model, RaKShA, to classify fraudulent patterns in credit card transactions. The model combines Long Short-Term Memory (LSTM) networks with explainable AI (XAI) to improve both prediction accuracy and interpretability. By integrating XAI, the model identifies the most influential features used in classification, making it more transparent and trustworthy. The results demonstrated an accuracy of 99.8% with a significant improvement in user trust due to its interpretable decision-making process (Raval et al., 2023). Salekshahrezaee investigated the impact of feature extraction and data sampling techniques on credit card fraud detection. They evaluated four ensemble classifiers, including XGBoost, Random Forest, LightGBM, and CatBoost, on an imbalanced dataset. The study implemented data-level methods such as Random Undersampling (RUS) and SMOTE Tomek, alongside feature extraction techniques like Principal Component Analysis (PCA) and Convolutional Autoencoders (CAE). Their findings showed that combining RUS with CAE led to the best performance, achieving a high F1 score and AUC, particularly with XGBoost (Salekshahrezaee et al., 2023).

Cheng introduced a spatial-temporal attention-based graph neural network (STAGN) for credit card fraud detection. The model leverages graph representations of transaction data to capture spatial and temporal aggregation patterns of fraudulent activities. By employing 3D convolutional layers with spatial-temporal attention mechanisms, STAGN outperformed traditional models in both AUC and precision-recall metrics. The study also highlighted the model's adaptability in detecting evolving fraud patterns in real-world datasets (Cheng et al., 2022). These studies underscore the importance of combining advanced machine learning algorithms with explainability techniques to tackle the complexities of fraud detection (Alarfaj et al., 2022; E et al., 2022; Khan et al., 2022; Mehbodniya et al., 2023; Tanouz et al., 2021). While ensemble models like XGBoost have proven effective in addressing imbalanced datasets, the integration of deep learning and attention mechanisms has further enhanced the detection of nuanced fraud patterns, ensuring better adaptability and scalability. These advancements lay the groundwork for developing robust and interpretable fraud detection systems.

Clean Energy and Smart Technology
Volume 03, Number 02, April 2025
DOI : https://doi.org/10.58641/
e-ISSN : 2964-2647

2. METHOD

Research flow

The research flow begins with selecting the Credit Card Fraud Detection dataset from Kaggle, which provides a highly imbalanced dataset for analysis. In the data preprocessing phase, techniques like SMOTE are applied to balance the dataset, while scaling ensures numerical consistency across features. The dataset is then split into training (70%) and testing (30%) subsets to evaluate the model's performance (Błaszczyński et al., 2021; Esenogho et al., 2022; Gupta et al., 2022; Li et al., 2021). Hyperparameter tuning is performed to optimize parameters for the XGBoost model, enhancing its predictive accuracy (Wang et al., 2022). The model is then developed using XGBoost, a robust algorithm known for its ability to handle imbalanced data effectively. Finally, the model is evaluated using performance metrics to ensure its reliability in detecting fraudulent transactions. The process concludes with a thorough assessment of results to validate the methodology(Trisanto et al., 2021).

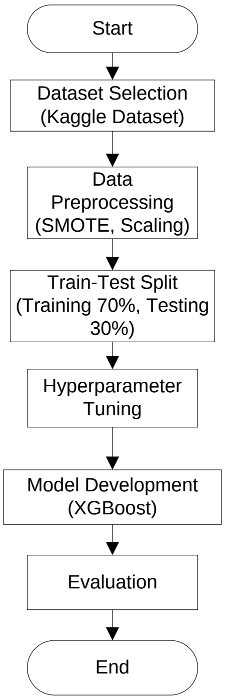

Fig. 1. Research flow

XGBoost Classification

The XGBoost classification algorithm is an ensemble learning method that uses gradient boosting on decision trees (Chen & Guestrin, 2016). The process involves building a series of trees, where each subsequent tree focuses on correcting the errors of the previous ones. XGBoost optimizes the objective function, which combines the loss function and a regularization term to improve the model's generalization and prevent overfitting. Its iterative approach ensures that tSShe model learns residuals effectively and enhances prediction accuracy, especially for imbalanced datasets (Trisanto et al., 2021).

The objective function in XGBoost is:

$$\mathcal{L}(\Theta) = \sum_{i=1}^{n} \ell(y_i, \hat{y}_i) + \sum_{k=1}^{K} \Omega(f_k)$$

3. RESULT AND DISCUSSION

Clean Energy and Smart Technology
Volume 03, Number 02, April 2025
DOI : https://doi.org/10.58641/
e-ISSN : 2964-2647

Dataset

The dataset used in this study is the publicly available Credit Card Fraud Detection dataset from Kaggle. It consists of 284,807 transactions, out of which only 492 (0.17%) are classified as fraudulent. The class distribution chart clearly shows a significant imbalance, with the vast majority of transactions being normal (Ahmad et al., 2023; Benchaji et al., 2021; Dileep et al., 2021; Sanober et al., 2021; Singh, Jain, et al., 2022). This imbalance reflects real-world scenarios where fraudulent transactions are rare but critical to detect. The dataset is widely used in fraud detection research due to its realistic representation of imbalanced data, making it an ideal benchmark for evaluating machine learning algorithms in this domain.

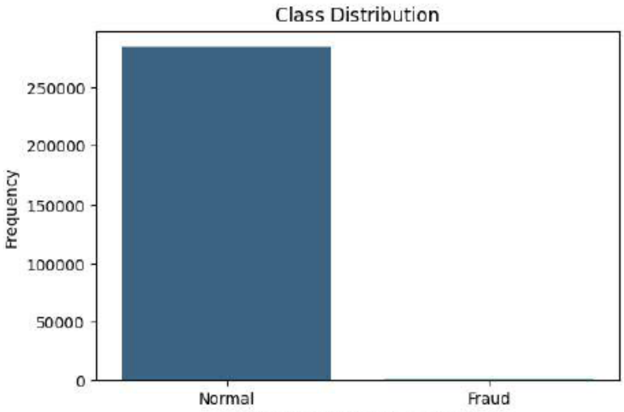

Fig. 2. Dataset Class Distribution

1. *Data Preprocessing*

The preprocessing phase begins with normalizing the Time and Amount columns using StandardScaler to ensure that these numerical features are standardized, having a mean of 0 and a standard deviation of 1. This normalization helps eliminate any disproportionate influence of these features on the model. Additionally, the Synthetic Minority Oversampling Technique (SMOTE) is applied to address the imbalance in the dataset by generating synthetic samples for the minority class (fraudulent transactions). This process ensures a more balanced representation of classes, improving the model's ability to detect fraudulent patterns effectively.

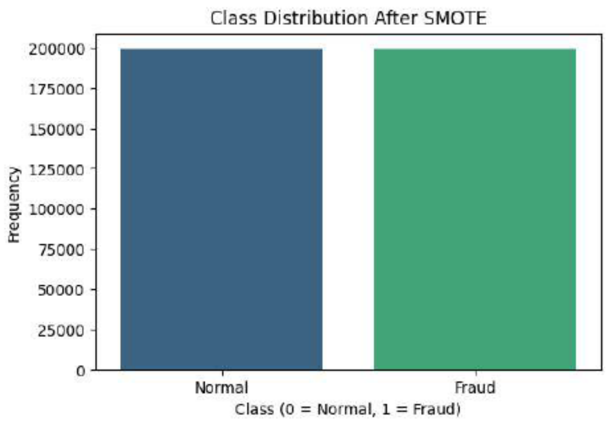

Fig. 3.Class Distribution After SMOTE

2. *Train-Test Split*

The train-test split step divides the dataset into two subsets, with 70 percent of the data allocated for training and 30 percent for testing. The training set is used to train the machine learning model, allowing it to learn patterns and relationships within the data, while the testing set is reserved for evaluating the model's performance on unseen data. This process ensures that the model's predictive capabilities are assessed objectively and helps prevent overfitting, ensuring it generalizes well to new data. Stratification is typically applied to maintain the same class

Clean Energy and Smart Technology
Volume 03, Number 02, April 2025
DOI : https://doi.org/10.58641/
e-ISSN : 2964-2647

distribution in both subsets, which is particularly important for imbalanced datasets like the one used in this research.

3. Hyperparameter Tuning

The hyperparameter tuning process employs GridSearchCV to optimize the XGBoost classifier's performance by systematically testing different combinations of hyperparameters. The parameters explored include max_depth (values of 3, 5, and 7), learning_rate (0.01, 0.1, 0.2), n_estimators (100, 200, 300), and scale_pos_weight (1, 10, 20), which are crucial for controlling model complexity, learning speed, and addressing class imbalance (Trisanto et al., 2021). The search uses 3-fold cross-validation with the scoring metric set to "ROC AUC" to identify the best configuration. After evaluating 243 combinations, the optimal parameters are identified as learning_rate of 0.2, max_depth of 7, n_estimators of 300, and scale_pos_weight of 20. This tuned model is expected to deliver improved accuracy and robustness for the imbalanced fraud detection dataset.

```
# Hyperparameter tuning with GridSearchCV
param_grid = {
    'max_depth': [3, 5, 7],
    'learning_rate': [0.01, 0.1, 0.2],
    'n_estimators': [100, 200, 300],
    'scale_pos_weight': [1, 10, 20]
}

xgb = XGBClassifier(random_state=42, eval_metric='logloss')
grid_search = GridSearchCV(estimator=xgb, param_grid=param_grid, scoring='roc_auc', cv=3, verbose=1, n_jobs=-1)
grid_search.fit(X_train_smote, y_train_smote)

Fitting 3 folds for each of 81 candidates, totalling 243 fits
    GridSearchCV
    best_estimator_: XGBClassifier
        XGBClassifier

# Best parameters
print("Best Parameters:", grid_search.best_params_)

Best Parameters: {'learning_rate': 0.2, 'max_depth': 7, 'n_estimators': 300, 'scale_pos_weight': 20}
```

Fig. 4. Hyperparameter tuning

4. Evaluation

The evaluation results demonstrate the performance of the XGBoost model in detecting fraudulent and normal transactions. For the majority class (normal transactions), the model achieves perfect precision, recall, and F1-score, indicating that it correctly identifies all normal transactions without false positives or negatives. For the minority class (fraudulent transactions), the model achieves a precision of 0.72, a recall of 0.82, and an F1-score of 0.77, showing reasonable effectiveness in identifying fraud despite the dataset's imbalance. The overall accuracy is 100%, but the macro average F1-score of 0.88 highlights the model's balanced performance across both classes. These metrics indicate the model is effective, though there is room for improvement in detecting fraudulent transactions.

```
Classification Report:
              precision    recall  f1-score   support

           0       1.00      1.00      1.00     85295
           1       0.72      0.82      0.77       148

    accuracy                           1.00     85443
   macro avg       0.86      0.91      0.88     85443
weighted avg       1.00      1.00      1.00     85443
```

Fig. 5. Evaluation Result

Clean Energy and Smart Technology
Volume 03, Number 02, April 2025
DOI : https://doi.org/10.58641/
e-ISSN : 2964-2647

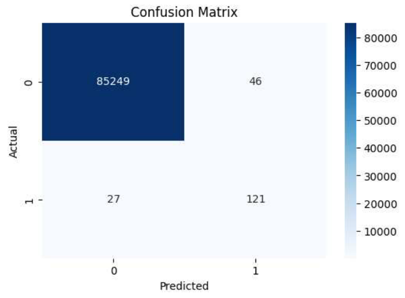

Fig. 6. Confusion Matrix

In Figure 6, the confusion matrix illustrates the classification performance of the XGBoost model. Out of 85,295 normal transactions, the model correctly classified 85,249 as normal, with only 46 misclassified as fraudulent (false positives). For 148 fraudulent transactions, the model accurately identified 121 as fraudulent, while 27 were misclassified as normal (false negatives). These results demonstrate that the model is highly accurate in predicting normal transactions but still faces challenges in detecting all fraudulent cases, primarily due to the dataset's imbalance. The confusion matrix highlights the importance of comprehensive evaluation to assess the model's performance across both classes.

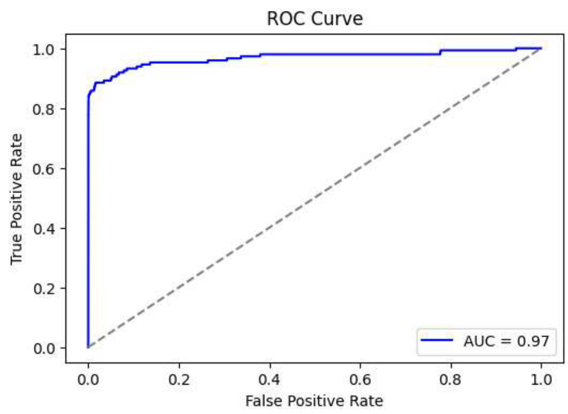

Fig. 7. ROC Curve

In Figure 7, the ROC (Receiver Operating Characteristic) curve evaluates the performance of the XGBoost model in distinguishing between fraudulent and normal transactions. The curve plots the True Positive Rate (TPR) against the False Positive Rate (FPR) at various classification thresholds. A model with perfect performance would have a curve reaching the top-left corner, representing a TPR of 1 and an FPR of 0. The Area Under the Curve (AUC) value of 0.97 indicates that the model performs exceptionally well in distinguishing between the two classes. This high AUC value demonstrates that the model achieves a strong balance between sensitivity and specificity, effectively detecting fraudulent transactions while minimizing false positives. The ROC curve confirms the reliability of the model in handling imbalanced datasets.

4. CONCLUSION

This study demonstrates the effective application of the XGBoost classification algorithm for detecting credit card fraud in an imbalanced dataset. By employing data preprocessing techniques such as normalization and SMOTE, the inherent class imbalance was addressed, ensuring a balanced dataset for training. The hyperparameter tuning process optimized model performance, and the results showcased a high Area Under the Curve (AUC) of 0.97, indicating strong predictive capabilities. Evaluation metrics, including precision, recall, and F1-score, revealed that the model performs exceptionally well in identifying normal transactions while achieving reasonable accuracy in detecting fraudulent transactions. However, challenges remain in further reducing false negatives for improved fraud detection. The findings highlight the importance of combining robust machine learning algorithms like XGBoost with effective preprocessing and optimization techniques to tackle real-world challenges in fraud detection systems.

5. REFERENCES

Afriyie, J. K., Tawiah, K., Pels, W. A., Addai-Henne, S., Dwamena, H. A., Owiredu, E. O., Ayeh, S. A., & Eshun, J. (2023). A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions. *Decision Analytics Journal*, *6*. https://doi.org/10.1016/j.dajour.2023.100163

Ahmad, H., Kasasbeh, B., Aldabaybah, B., & Rawashdeh, E. (2023). Class balancing framework for credit card fraud detection based on clustering and similarity-based selection (SBS). *International Journal of Information Technology (Singapore)*, *15*(1), 325–333. https://doi.org/10.1007/s41870-022-00987-w

Alarfaj, F. K., Malik, I., Khan, H. U., Almusallam, N., Ramzan, M., & Ahmed, M. (2022). Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms. *IEEE Access*, *10*, 39700–39715. https://doi.org/10.1109/ACCESS.2022.3166891

Almazroi, A. A., & Ayub, N. (2023). Online Payment Fraud Detection Model Using Machine Learning Techniques. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.0322000

Benchaji, I., Douzi, S., & El Ouahidi, B. (2021). Credit card fraud detection model based on LSTM recurrent neural networks. *Journal of Advances in Information Technology*, *12*(2), 113–118. https://doi.org/10.12720/jait.12.2.113-118

Błaszczyński, J., de Almeida Filho, A. T., Matuszyk, A., Szeląg, M., & Słowiński, R. (2021). Auto loan fraud detection using dominance-based rough set approach versus machine learning methods. *Expert Systems with Applications*, *163*. https://doi.org/10.1016/j.eswa.2020.113740

Chang, V., Minh, L., Doan, T., Stefano, A. Di, Sun, Z., & Fortino, G. (2022). Digital Payment Fraud Detection Methods in digital ages and Industry 4.0. *Elsevier, Computers and Electrical Engineering*.

Chen, T., & Guestrin, C. (2016). XGBoost: A scalable tree boosting system. *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, *13-17-August-2016*, 785–794. https://doi.org/10.1145/2939672.2939785

Cheng, D., Wang, X., Zhang, Y., & Zhang, L. (2022). Graph Neural Network for Fraud Detection via Spatial-Temporal Attention. *IEEE Transactions on Knowledge and Data Engineering*, *34*(8), 3800–3813. https://doi.org/10.1109/TKDE.2020.3025588

Cherif, A., Badhib, A., Ammar, H., Alshehri, S., Kalkatawi, M., & Imine, A. (2023). Credit card fraud detection in the era of disruptive technologies: A systematic review. In *Journal of King Saud University - Computer and Information Sciences* (Vol. 35, Issue 1, pp. 145–174). King Saud bin Abdulaziz University. https://doi.org/10.1016/j.jksuci.2022.11.008

Dantas, R. M., Firdaus, R., Jaleel, F., Neves Mata, P., Mata, M. N., & Li, G. (2022). Systemic Acquired Critique of Credit Card Deception Exposure through Machine Learning. *Journal of Open Innovation: Technology, Market, and Complexity*, *8*(4). https://doi.org/10.3390/joitmc8040192

Dileep, M. R., Navaneeth, A. V., & Abhishek, M. (2021). A novel approach for credit card fraud detection using decision tree and random forest algorithms. *Proceedings of the 3rd International Conference on Intelligent Communication Technologies and Virtual Mobile Networks, ICICV 2021*, 1025–1028. https://doi.org/10.1109/ICICV50876.2021.9388431

E, J., T, R., Kharat, R. S., M.R.M, V., Bharathiraja, N., Venkatesan, R., & Marappan, R. (2022). *Cybersecurity Enhancement to Detect Credit Card Frauds in Healthcare Using New Machine Learning Strategies*. https://doi.org/10.21203/rs.3.rs-2278457/v1

Esenogho, E., Mienye, I. D., Swart, T. G., Aruleba, K., & Obaido, G. (2022). A Neural Network Ensemble with Feature Engineering for Improved Credit Card Fraud Detection. *IEEE Access*, *10*, 16400–16407. https://doi.org/10.1109/ACCESS.2022.3148298

Gupta, P., Varshney, A., Khan, M. R., Ahmed, R., Shuaib, M., & Alam, S. (2022). Unbalanced Credit Card Fraud Detection Data: A Machine Learning-Oriented Comparative Study of Balancing Techniques. *Procedia Computer Science*, *218*, 2575–2584. https://doi.org/10.1016/j.procs.2023.01.231

Hashemi, S. K., Mirtaheri, S. L., & Greco, S. (2023). Fraud Detection in Banking Data by Machine Learning Techniques. *IEEE Access*, *11*, 3034–3043. https://doi.org/10.1109/ACCESS.2022.3232287

Clean Energy and Smart Technology
Volume 03, Number 02, April 2025
DOI : https://doi.org/10.58641/
e-ISSN : 2964-2647

Hilal, W., Gadsden, S. A., & Yawney, J. (2022). Financial Fraud: A Review of Anomaly Detection Techniques and Recent Advances. In *Expert Systems with Applications* (Vol. 193). Elsevier Ltd. https://doi.org/10.1016/j.eswa.2021.116429

Khan, S., Alourani, A., Arabia, S., Mishra, B., Ali, A., & Kamal, M. (2022). Developing a Credit Card Fraud Detection Model using Machine Learning Approaches. *IJACSA) International Journal of Advanced Computer Science and Applications*, *13*(3), 2022. www.ijacsa.thesai.org

Kumar, S., Ahmed, R., Bharany, S., Shuaib, M., Ahmad, T., Tag Eldin, E., Rehman, A. U., & Shafiq, M. (2022). Exploitation of Machine Learning Algorithms for Detecting Financial Crimes Based on Customers' Behavior. *Sustainability (Switzerland)*, *14*(21). https://doi.org/10.3390/su142113875

Langevin, A., Cody, T., Adams, S., & Beling, P. (2022). Generative adversarial networks for data augmentation and transfer in credit card fraud detection. *Journal of the Operational Research Society*, *73*(1), 153–180. https://doi.org/10.1080/01605682.2021.1880296

Li, Z., Huang, M., Liu, G., & Jiang, C. (2021). A hybrid method with dynamic weighted entropy for handling the problem of class imbalance with overlap in credit card fraud detection. *Expert Systems with Applications*, *175*. https://doi.org/10.1016/j.eswa.2021.114750

Mehbodniya, A., Alam, I., Pande, S., Neware, R., & Rane, K. P. (2023). Retracted: Financial Fraud Detection in Healthcare Using Machine Learning and Deep Learning Techniques. *Security and Communication Networks*, *2023*, 1–1. https://doi.org/10.1155/2023/9758612

Mishra, K. N., & Pandey, S. C. (2021). Fraud Prediction in Smart Societies Using Logistic Regression and k-fold Machine Learning Techniques. *Wireless Personal Communications*, *119*(2), 1341–1367. https://doi.org/10.1007/s11277-021-08283-9

Raval, J., Bhattacharya, P., Jadav, N. K., Tanwar, S., Sharma, G., Bokoro, P. N., Elmorsy, M., Tolba, A., & Raboaca, M. S. (2023). RaKShA: A Trusted Explainable LSTM Model to Classify Fraud Patterns on Credit Card Transactions. *Mathematics*, *11*(8). https://doi.org/10.3390/math11081901

Salekshahrezaee, Z., Leevy, J. L., & Khoshgoftaar, T. M. (2023). The effect of feature extraction and data sampling on credit card fraud detection. *Journal of Big Data*, *10*(1). https://doi.org/10.1186/s40537-023-00684-w

Sanober, S., Alam, I., Pande, S., Arslan, F., Rane, K. P., Singh, B. K., Khamparia, A., & Shabaz, M. (2021). An Enhanced Secure Deep Learning Algorithm for Fraud Detection in Wireless Communication. *Wireless Communications and Mobile Computing*, *2021*. https://doi.org/10.1155/2021/6079582

Sharma, P., Banerjee, S., Tiwari, D., & Patni, J. C. (2021). Machine learning model for credit card fraud detection-A comparative analysis. *International Arab Journal of Information Technology*, *18*(6), 789–796. https://doi.org/10.34028/iajit/18/6/6

Singh, A., Jain, A., & Biable, S. E. (2022). Financial Fraud Detection Approach Based on Firefly Optimization Algorithm and Support Vector Machine. *Applied Computational Intelligence and Soft Computing*, *2022*. https://doi.org/10.1155/2022/1468015

Singh, A., Ranjan, R. K., & Tiwari, A. (2022). Credit Card Fraud Detection under Extreme Imbalanced Data: A Comparative Study of Data-level Algorithms. *Journal of Experimental and Theoretical Artificial Intelligence*, *34*(4), 571–598. https://doi.org/10.1080/0952813X.2021.1907795

Tanouz, D., Subramanian, R. R., Eswar, D., Reddy, G. V. P., Kumar, A. R., & Praneeth, C. H. V. N. M. (2021). Credit card fraud detection using machine learning. *Proceedings - 5th International Conference on Intelligent Computing and Control Systems, ICICCS 2021*, 967–972. https://doi.org/10.1109/ICICCS51141.2021.9432308

Trisanto, D., Rismawati, N., Mulya, M. F., & Kurniadi, F. I. (2021). Modified Focal Loss in Imbalanced XGBoost for Credit Card Fraud Detection. *International Journal of Intelligent Engineering and Systems*, *14*(4), 350–358. https://doi.org/10.22266/ijies2021.0831.31

Wang, S., Ma, C., Xu, Y., Wang, J., & Wu, W. (2022). A Hyperparameter Optimization Algorithm for the LSTM Temperature Prediction Model in Data Center. *Scientific Programming*, *2022*. https://doi.org/10.1155/2022/6519909