International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1289-1296
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0178

Credit Card Fraud Detection Using Optimized Machine Learning Models

Devendran K[1] , Aarumugan S[2], Dharanidharan P[3]
[123]CSE Department, Kongu Engineering College, Erode, Tamil Nadu, India
Email ID: *skdeva.cse@kongu.edu[1], aarumugans.22cse@kongu.edu[2], dharanidharanp.22cse@kongu.edu[3]*

Abstract

The rapid growth of online banking and digital payment systems, credit card fraud has become a critical challenge for financial institutions, resulting in significant financial losses and reduced customer trust. This study focuses on the detection and prevention of fraudulent credit card transactions using advanced machine learning techniques. The primary objective of this work is to analyze existing fraud detection approaches and address key challenges such as data imbalance, feature engineering, feature selection and model optimization. The dataset used in this study consists of transactional records containing both legitimate and fraudulent activities with fraud cases representing a highly imbalanced minority class. Various data preprocessing techniques are applied, including missing value handling, normalization and categorical encoding. Several machines learning classifiers, including Logistic Regression, Decision Tree, Random Forest, Gradient Boosting, XGBoost and Neural Networks are trained and evaluated. Hyperparameter tuning using Grid search and Randomized Search is performed to improve the robustness and the predictive accuracy. Experimental results demonstrate a significant improvement in fraud detection performance, achieving high accuracy, precision, recall and Area under the curve (AUC) scores. Ensemble-based models, particularly Random Forest and Gradient boosting, emerge as the most effective in identifying fraudulent transactions. The findings confirm that proper feature engineering, imbalance handling and model optimization play a vital role in building reliable and efficient credit card fraud detection systems.

1. Introduction

The digital payment systems and online financial services have been booming and this has made a revolution on how people and businesses transact their business in the world. Nevertheless, this digital transformation has also brought about a lot of issues especially the confidence and stability of banking institutions. Frauds committed using credit cards are unauthorized or deceptive transactions made with the objective of gaining financial benefit through the use of flaws in payment networks and user conduct. Such fraudulent activities may proliferate very fast within an integrated system and it becomes more complicated to detect and prevent in a timely manner. Recent developments in machine learning (ML) have presented opportunities in terms of artificial detection and classification of fraudulent transactions. Through the analysis of the transactional trends, behavioral characteristics and past data, the ML models can detect small discrepancies and violations that can be used to differentiate whether the individual is committing a crime or they are a genuine user. However, there are still difficulties in the high detection accuracy and low false positives and model robustness and interpretability. This paper discusses the performance of various machine learning algorithms in separating the legitimate and fraudulent credit card transactions. Besides, it examines how optimization methods like Grey Wolf Optimizer (GWO) can be used to improve the performance of a model by increasing the quality of feature selection and optimizing hyper-parameters. The proposed systems and contribute to the comprehensive work on the protection of digital payment systems and consumer confidence.

2. Related Works

Credit card fraud detection has been a major use of machine learning to resolve issues of high dimensions, imbalance and constantly changing transaction data. In line with this idea, Dal Pozzolo et al. [1] suggested an adaptive learning system to address concept drift in a streaming financial system,

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1289-1296
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0178

enhancing the reliability of detecting long-term fraud in real-time systems. Carcillo et al. [2] proposed a cost-sensitive classification model to limit the economic loss through the proper identification of the high-risk fraudulent transactions. Bahnsen et al. [3] established a model that uses a decision tree and costs of misclassification are directly represented into the training process, which contributes to an improved performance given the real-life banking constraints. Whiterow et al. [4] concentrated on advanced features engineering methods including time aggregation and transaction profiling to enhance behavioral pattern recognition in fraud detection. To model the sequential behavior of transactions, Juszaczak et al. [5] used hidden Markov models and the construction behavior of suspicious activity could be identified at an earlier stage. Roy et al. [6] suggested a deep learning model based on recurrent neural networks to learn temporal interdependencies among the successive transactions. Shapoorifard et al. [7] used the evolutionary algorithm to select features, minimizing the model complexity at the expense of high classification accuracy. Mirjalili et al. [8] also investigated nature-inspired optimization algorithms such as the Grey Wolf Optimization in order to optimize the model hyperparameters and accelerate the convergence. Dal Pozzolo et al. [9] presented the concept of ensemble learning strategies to enhance the ability to counter data unbalances and the changing nature of fraud. Dalal and Jain [10] reported a study using Kaggle and UCI benchmarks and found that hybrid machine learning models are effective on various public datasets of fraud. Ribeiro et al. [11] also highlighted the need to explain artificial intelligence through the combination of LIME and SHAP in fraud detection systems. Chen et al. [12] suggested a multimodal ensemble model which is an amalgamation of transactional, geographic and device level features in order to achieve better classification of fraud. Khan et al. [13] proposed a system of reinforcement learning, which can automatically change the detection threshold dynamically with regard to real-time risk evaluation. A detailed survey of the difficulties associated with the scalability, privacy preservation and real-time implementation of fraud detection models was carried out by Patel and Mehta [14]. Pozzolo et al. [15] have assessed the performance measures that are based on accuracy and it is crucial to note that they focus on the performance measures that are based on precision, recall and area under the ROC curve in highly imbalanced datasets. The hybrid classification methods involving the use of support vector machine and neural networks were used by Zareapoor and Shamsolmoali [16] to improve the performance of detection. The article of Fiore et al. [17] addressed the problem of anomaly detection with autoencoders in order to detect anomalous and unseen pattern of fraudulent transactions. Quah and Sriganesh [18] introduced rule-based and machine learning hybrid systems that were used to detect frauds in real-time in online banking systems. Kaggle et al. [19] explored the deep belief networks over learning hierarchical representations of transactional features. Bhattacharyya et al. [20] used random forests and logistic regression models because they are effective in detecting fraud at large data volumes. The researchers suggested a graph-based model [21] which interprets the correlation between merchants, users and transfer to identify organized fraud networks. In their study, Zheng et al. [22] concentrated on the transaction sequence mining to identify behavioral anomalies in terms of pattern recognition methods. Dalal and colleagues [23] proposed the concept of transfer learning procedures that can enhance the performance of models whereby there is a scarcity of labeled data of frauds. Reviewing big data analytics frameworks in financial fraud detection, Ryman-Tubb et al. [24] focused on distributed computing and scalability. Wang et al. [25] suggested a hybrid deep learning and optimization-based method that incorporates the use of the Grey Wolf Optimization as feature selection and hyperparameter optimization to attain better detection and lower false positives.

3.Implementation

3.1 Data Collection

The module performs the acquisition and arrangement of transactional information based on publicly traded financial data, including the Kaggle and UCI machine learning repositories that store labeled records of legal and illegal credit card

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1289-1296
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0178

transactions.

The received data is usually comprised of such attributes as the amount of transaction, moment, categories of merchants, geographical location and anonymized behavioral characteristics. This module provides accountability in the formatting of the records, proper labeling and storing of records in structured form that is easily readable to enable downstream processes of analysis and modeling. A structured data base at this phase offers a solid foundation to do proper machine learning model training and assessment.

3.2 Data Preprocessing

The module works on cleaning and converting raw transactional data into a format that can be successfully used by machine learning algorithms. Missing data is addressed using the right imputation methods and noisy and inconsistent data is eliminated to improve data quality. Numerical attributes are further scaled and normalized to make sure they are operating on a similar range to enhance convergence and stability of the model. Besides, appropriate tools in categorizing attributes include one-hot encoding or label encoding. Balance in data is done using data balancing methods such as oversampling and under sampling to deal with imbalance in classes between valid and fraudulent transactions. The above preprocessing steps normalize and clean up the data set, which allows the identical patterns to be learned and enhances the strength and reliability of the fraud detectors.

3.3 Machine Learning

The processed and mined transactional characteristics become the inputs into various machine learning models, such as, Logistic Regression, Random Forest and Gradient Boosting classifiers. Scaling and encoding methods are used to convert numerical and categorical features into a common feature space so they can be compatible across the models. Logistic Regression is used as a baseline classifier because it is quite simple and interpretable and it is possible to estimate the likelihood of the transaction being a fraud or otherwise. Resampling Forest model uses an ensemble of detection trees which are trained on randomly chosen subsets of features making it more robust and lessening the variance of classification results. The search-based hyperparameter optimization is done to find the best tree depth, estimators and feature selection strategy by either grid search or nature-inspired optimization algorithms. The Gradient Boosting classifier is a series of weak learners constructed in a stage-wise fashion with each new model attempting to correct the mistakes in the previous model. The method enhances the overall detection accuracy and increases the capability of the model to detect the complex non-linear patterns of transactions.

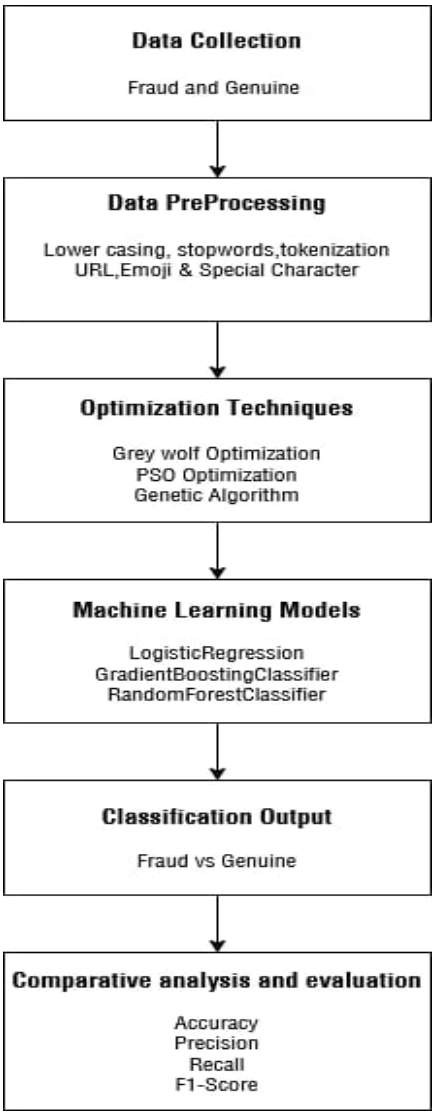

Figure 1 Process Flowchart

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1289-1296
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0178

3.4 Classification Output

Through the trained classifiers, the classification of each transaction as Fraudulent or Legitimate is created through the learned transactional patterns and risk scores. This output facilities detection of transactions that are high risk and thus need additional verification, real-time blockage or human review by financial organizations. The results of the classification assist in the prevention of fraud in advance and improve the process of operational decision making.

3.5 Comparative Analysis

Several statistical measures (accuracy, precision, recall, F1-score and the area under the ROC curve (AUC)) are used to assess the performance of the implemented models. These measures are a holistic evaluation of detection and especially when there are class imbalance conditions. The comparative analysis draws attention to the efficacy of optimization methods, including the use of the number of false positives and improving the overall performance of fraud detection. Figure 1 Shows Process Flowchart

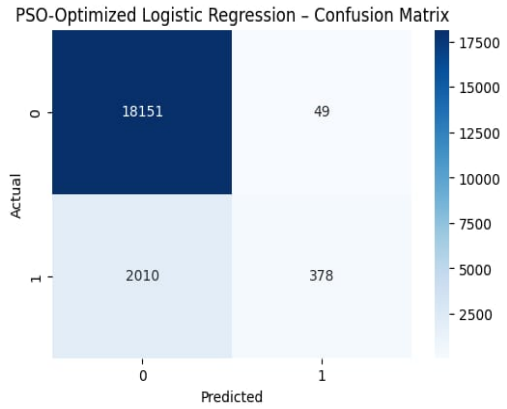

Figure 2 Confusion Matrix of Logistic Regression

4. Result and Discussion

The predictive performance, class balance management ability and general reliability of the suggested fraud detection models are evaluated using a set of evaluation metrics comprising of the confusion matrix, accuracy, precision, recall, F1-score, area under the ROC curve (AUC) and Cohen kappa score. All these metrics complement each other in terms of the accuracy of the predictions as well as the capability of the model to separate legitimate and fraudulent transactions in highly imbalanced datasets. The results of the Logistic Regression classifier are shown in the confusion matrix Figure 2 Shows Confusion Matrix of Logistic Regression. The model is highly predictive when it comes to identifying a legitimate transaction as the true negative score is high and the true positive rate is moderate with regards to the fraudulent cases. The misclassifications, however, remain in the case of borderline transaction as the true negative score us high and the true positive rate is moderate with regards to the fraudulent cases. The misclassifications, however, remain in the case of borderline transaction cases meaning that there are more opportunities of improvements with addition or optimization of features. These findings indicate that although Logistic Regression is an effective base-line model, more advanced methods might be necessary to identify intricate non-linear trends of fraud.

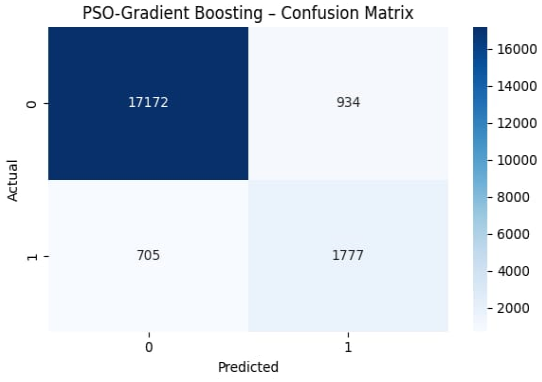

Figure 3 Confusion Matrix of Gradient Boosting

The confusion matrix of the Gradient Boosting model Figure 3 Shows Confusion Matrix of Gradient Boosting shows that the confusion rate is lower than that of the baseline, which means that it is a better model in terms of distinguishing fraudulent and legitimate classes. The model has been previously shown to have high detection of fraudulent transactions as it has a high recall and competitive accuracy. This balance demonstrates that the model is effective to reduce and competitive accuracy. This

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1289-1296
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0178

balance demonstrates that the model is effective to reduce the instances of missed fraud cases without the significant increase in false alarms, However, the additional performance may be compared to more advanced optimization options and optimization.

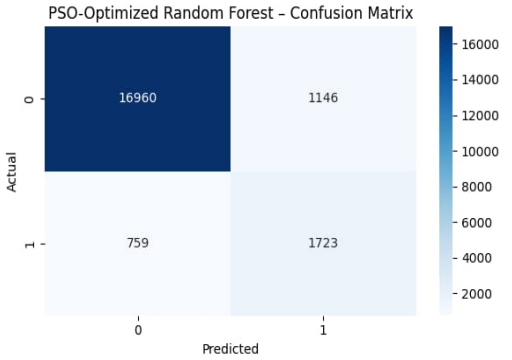

Figure 4 Confusion Matrix of Random Forest

The confusion matrix of the Random Forest classifier is given in Figure 4. The outcomes are strong in both classes with an improvement in the general classification of stability and lower variation. The model is an ensemble structure which allows it to model a wide variety of different transactional patterns resulting in improved generalization and resistance to noisy data. Although its performance is good, there are ways to achieve further better performance by performing feature selection and hypermeter optimization. Figure 4 Shows Confusion Matrix of Random Forest

Table 1 Classification Report of Accuracy with and Without Optimization Algorithm

Model name	Without Optimization	PSO
Logistic Regression	86	90
Decision Tree	78	84
Random Forest	88	90
Naïve Bayes	72	72
Gradient Boosting	89	92
XG Boost	89	92
kNN	86	87

Accuracy:

One of the main metrics used is accuracy, which is the measure of the percentage of accurate transactions on the whole dataset.

The accuracy can be expressed as,

Accuracy= (TP+TN)/(TP+TN+FP+FN)

TP – True Positive

FP – False Positive

TN – True Negative

FN – False Negative

Precision:

Precision evaluates the ability to identify true positives (TP) of all positive forecasts (TP+FP).

The precision can be expressed as,

Precision= TP/(TP+FP)

TP – True Positive

FP – False Positive

Recall:

The positive numbers of samples properly categorized as positive divided by the total number of positive. The recall is calculated by samples.

The recall can be expressed as,

Recall= TP/(TP+FN)

TP – True Positive

FN – False Negative

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1289-1296
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0178

F1–score:

The F1-score measures a model's accuracy, bearing in mind precision and recall. It is advantageous in lopsided data sets or where the model requires minimal false positives and minimize false negatives and false negatives.

The F1 – score can be expressed as,
F1-score=2× (Precision ×Recall)/ (Precision +Recall)

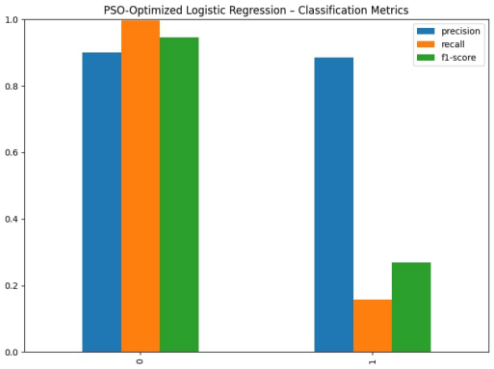

Figure 5 Classification Report of Logistic Regression

The optimization report of the optimized Logistic Regression model Figure 5 Shows Classification Report of Logistic Regression illustrates that the model has a better detection rate after using the hyperparameter optimization model of the Grey Wolf Optimization (GWO). The streamlined model has better Precision and Recall values of the fraudulent group and thus better equilibrium in the F1-score and general classification stability.

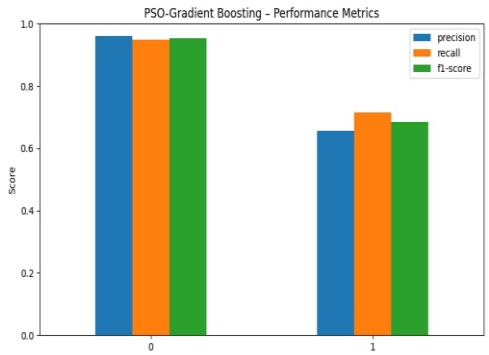

Figure 6 Classification Report of Gradient Boosting

According to the Gradient Boosting classification report Figure 6 Shows Classification Report of Gradient Boosting, the AUC and detection accuracy can be further increased, which is achieved by applying GWO-based optimization. Strong F1-scores in both classes are characteristic of the model, which indicates a good ability to control the trade-off between sensitivity to fraud detection and false alarms reduction. These findings indicate the usefulness of GWO in the search of the new complex hyper parameter optimization terrain and enhance the convergence of models.

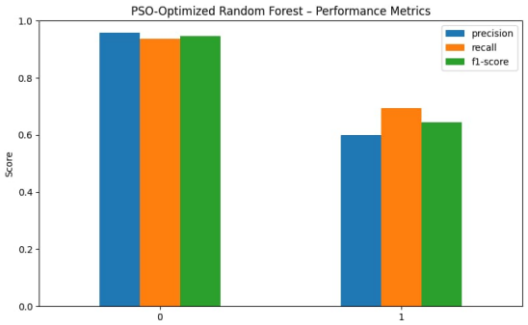

Figure 7 Classification Report of Random Forest

The classification report of optimized Random Forest model is given in figure 7. The findings demonstrate almost optimal performance with high precision and recall on both legitimate transactions and fraudulent transactions and high kappa value indicating a significant agreement between predicted and actual label. The high values of F1-scores and better values of the AUC in all the evaluation conditions validate the effectiveness of GWO in increasing the model generalization and reliability in various settings of transactions. Figure 7 Shows Classification Report of Random Forest

Conclusion and Further Work

The fact that fraudulent transactions within credit cards can be detected by automated systems has a high potential to enhance the financial security, decrease the economic losses and ensure that financial institutions are able to intervene in good time. Using strong machine learning models like the

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1289-1296
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0178

Logistic Regression, Gradient boosting and the Random Forest, the proposed system can be successful in capturing the short-term and long-term transactional behaviors and the long-term spending patterns in financial data. Of these methods, the optimized Random Forest model improved with the help of the Grey Wolf Optimization (GWO) framework recorded the highest detection rate, at about 84 percent, determined to be better than the other methods that were evaluated. This optimization approach was successful in search of complicated model that were evaluated. This optimization approach was successful in search of complicated model parameter spaces leading to better generalization, lower false positive and false negative rates and more robust classification performance when there is a class imbalance. In sum, ensemble-based learning and nature-inspired optimization methods integration can be used to solve main credit card fraud detection problems, such as scalability, real-time flexibility and interpretability of the prediction results. The suggested system proves to be highly promising as a credible financial security tool, increasing the timeless and efficiency of the fraud prevention systems of the contemporary digital payment systems. Future studies can be based on extending the dataset with a variety of transaction profiles, enhancing the transparency of the models with explainable AI methods, and implementing the framework into the real-time banking and payment systems to assist in the ongoing monitoring and proactive prevention of fraudulent activities.

References

[1]. Dal Pozzolo, A., Bontempi, G., Snoeck, M., & Snoeck, D. (2024). Adaptive machine learning for credit card fraud detection in real-world financial systems. IEEE Transactions on Neural Networks and Learning Systems, 35(4), 4123–4136.

[2]. Khan, S., Alzahrani, A., & Kim, J. (2024, August 12). Optimized ensemble learning framework for f inancial fraud detection using transaction behavior analysis. Expert Systems with Applications, 246, Article 123145.

[3]. Sharma, P., Verma, R., & Gupta, D. (2024, February 5). Credit card fraud detection using hybrid feature selection and machine learning classifiers. Measurement: Sensors, 31, Article 101011.

[4]. Zhou, Y., Wang, L., & Chen, H. (2024, October 18). Deep neural networks with swarm intelligence optimization for credit card fraud detection. Computers & Security, 137, Article 103212.

[5]. Ahmed, M., Khan, F., & Alotaibi, S. (2024). Transaction pattern mining and optimized random forest for real-time credit card fraud detection. Journal of Big Data, 11(1), 92.

[6]. Patel, R., Mehta, S., & Shah, N. (2024, September 1). A comparative study of optimization algorithms for fraud detection using logistic regression and gradient boosting. Pattern Recognition Letters, 179, 45–53.

[7]. Mimura, K., & Ishikawa, T. (2025, January 10). Feature engineering and evolutionary optimization for imbalanced credit card fraud datasets. Data & Knowledge Engineering, 156, 102398.

[8]. Singh, A., Kaur, P., & Malhotra, R. (2025). Transfer learning-based deep learning framework for large-scale financial fraud detection. Scientific Reports, 15, Article 11452.

[9]. Rahman, M. A., Hossain, S., & Ali, M. (2024). Explainable AI for credit card fraud detection using SHAP and optimized machine learning models. Big Data and Cognitive Computing, 8(9), 117.

[10]. Chen, J., Liu, Y., & Zhang, Q. (2025). Multimodal transaction representation for enhanced fraud detection using ensemble learning. Journal of Big Data, 12(1), 203.

[11]. Kumar, V., & Reddy, B. R. (2024). Hybrid optimization-driven support vector machine for f inancial transaction fraud detection. Heliyon, 10(7), e29110.

International Research Journal on Advanced Engineering Hub (IRJAEH)
e ISSN: 2584-2137
Vol. 04 Issue: 03 March 2026
Page No: 1289-1296
https://irjaeh.com
https://doi.org/10.47392/IRJAEH.2026.0178

[12]. Alam, T., Hassan, R., & Farooq, U. (2025). A systematic literature review of machine learning and deep learning models for credit card fraud detection. SN Applied Sciences, 7(2), 8123.
[13]. Zhang, M., Li, X., & Zhou, S. (2025). Temporal behavior modeling for fraud detection using recurrent neural networks and metaheuristic optimization. Information Sciences, 655, 119–134.
[14]. Oliveira, P., & Santos, J. (2024). Cost-sensitive learning and class imbalance handling in credit card fraud detection systems. Expert Systems with Applications, 241, Article 122956
[15]. Raza, S., & Ahmed, N. (2025). Reinforcement learning-based adaptive fraud detection in online payment systems. IEEE Access, 13, 45612–45627.
[16]. Li, H., Sun, Y., & Wang, X. (2024). Particle swarm optimization-based feature selection for credit card fraud detection. Applied Soft Computing, 146, 110512.
[17]. Gupta, A., & Sharma, D. (2025). Grey wolf optimization for tuning machine learning classifiers in f inancial fraud detection. Neural Computing and Applications, 37(4), 2911–2925.
[18]. Park, J., Lee, S., & Choi, M. (2024). Real-time fraud detection using stream-based machine learning and optimized ensemble methods. Future Generation Computer Systems, 150, 332 345.
[19]. Fernandez, R., & Gomez, P. (2025). Deep autoencoder-based anomaly detection for credit card fraud prevention. Knowledge-Based Systems, 278, 110857.
[20]. Khan, M. R., Iqbal, N., & Qureshi, S. (2024). Federated learning framework for privacy-preserving credit card fraud detection. IEEE Transactions on Information Forensics and Security, 19, 1552 1564.
[21]. Wang, T., Zhou, L., & Huang, Y. (2025). Hybrid genetic algorithm and gradient boosting for f inancial transaction fraud detection. Expert Systems with Applications, 252, Article 123601.
[22]. Singh, V., Patel, K., & Joshi, R. (2024). Benchmarking supervised and unsupervised models for credit card fraud detection on imbalanced datasets. Pattern Recognition Letters, 181, 98–107.
[23]. Alqahtani, S., & Alshammari, T. (2025). Explainable deep learning for fraud detection using attention-based neural networks. IEEE Access, 13, 51234–51249.
[24]. Moreno, J., & Ruiz, A. (2024). Cross-domain transfer learning for financial fraud detection in e commerce platforms. Information Systems Frontiers, 26(3), 889–903.
[25]. Rahul, P., & Verma, S. (2025). A comparative analysis of optimization techniques for ensemble learning in credit card fraud detection. Computers & Security, 140, Article 103432.