An Explainable AI-based Fraud Detection System Using Recursive Feature Elimination and Waterwheel Plant Optimization for Financial Transactions

Hafis Hajiyev
Department of Finance and Audit, Azerbaijan State University of Economics (UNEC), Baku AZ1001, Azerbaijan
afiz_hajiyev@unec.edu.az (corresponding author)

Emil Hajiyev
Department of Business Management, Azerbaijan State University of Economics (UNEC), Baku AZ1001, Azerbaijan
hajiyev.emil@unec.edu.az

Mirzobek Avezov
Department of Business and Management, Urgench State University, Urgench 220100, Uzbekistan
avezov.mirzobek@urdu.uz

Samariddin Makhmudov
Department of Finance and Tourism, Termez University of Economics and Service, Termez 190111, Uzbekistan | Department of Finance, Alfraganus University, Tashkent 100000, Uzbekistan | Department of Economics, Mamun University, Khiva 220900, Uzbekistan
s.maxmudov@afu.uz

Dilora Abdukhalikova
Department of Exact Sciences, Kimyo International University in Tashkent, Tashkent 100000, Uzbekistan
abdukhalikova.d@kiut.uz

E. Laxmi Lydia
Department of Computer Science and Engineering, Vignan's Institute of Engineering for Women, Visakhapatnam, Andhra Pradesh 530046, India
elaxmi2002@yahoo.com

Received: 13 July 2025 | Revised: 25 July 2025, 5 August 2025, and 21 August 2025 | Accepted: 26 August 2025

 DOI: https://doi.org/10.48084/etasr.13350

ABSTRACT

Fraudulent transactions and the methods to detect them are an an important issue for financial organizations globally. The requirement for progressive fraud detection systems to protect properties and maintain customer trust is predominant for financial organizations, but particular factors make the development of efficient and effective fraud detection models a challenge. Deep Learning (DL) has greatly improved fraud detection accuracy by detecting intrinsic patterns, whereas interpretability techniques improve transparency and build trust by making predictions understandable to experts. This study presents a Fraud Detection System using Recursive Feature Elimination and Waterwheel Plant Optimization (FDS-RFEWPO) model for financial transactions. The aim is to perform a comprehensive evaluation of fraud detection in high-dimensional financial transactions using advanced techniques.

Initially, the FDS-RFEWPO technique follows min-max-based data pre-processing to normalize the input data. For the feature selection process, the FDS-RFEWPO model employs the Recursive Feature Elimination (RFE) technique to select the most relevant features from the dataset. Furthermore, the Variational Autoencoder/Wasserstein Autoencoder (VAE/WAE) model is employed for fraud detection and classification. To further enhance model performance, the Waterwheel Plant Optimization (WPO) technique is employed for hyperparameter tuning, ensuring the selection of optimal parameters that contribute to improved accuracy. Finally, the Explainable Artificial Intelligence (XAI) technique applies Local Interpretable Model-Agnostic Explanations (LIME) to improve the transparency, interpretability, and trustworthiness of Artificial Intelligence (AI) methods by making their decision-making procedures clear to humans. To evaluate the performance of the FDS-RFEWPO model, a comprehensive experimental analysis is conducted using a financial fraud detection dataset. The comparison study of the FDS-RFEWPO model demonstrates a superior accuracy of 97.41% over existing techniques.

Keywords-Explainable Artificial Intelligence (XAI); fraud detection; Recursive Feature Elimination (RFE); Waterwheel Plant Optimization (WPO); financial transactions

I. INTRODUCTION

The internet has expanded rapidly with evolving technologies such as big data, Software-Defined Networking (SDN), and Cloud Computing (CC) [1]. However, major cybersecurity threats accompany these innovations, heavily affecting critical infrastructure. Conventional defense strategies have had difficulty keeping pace with the complexity of modern cyber threats [2], as they depend on static defense tools, such as intrusion prevention and fraud detection systems [3]. Fraudulent activities, namely credit card fraud, identity misuse, insurance fraud, and cybercrimes, have become more widespread across multiple sectors [4].

Fraud causes significant financial losses, damages reputation, and erodes client trust. Conventional detection methods depend on detecting patterns and deviations but often face difficulty in distinguishing true causes from mere statistical outliers, restricting their efficiency [5, 6]. Financial fraud detection has become a crucial concern and one of the most important research challenges [7]. The imbalance in data is a primary challenge in fraud detection, as most financial transactions do not involve fraud [8]. To create an efficient fraud detection model, addressing this data imbalance issue is essential [9]. Artificial Intelligence (AI), particularly Machine Learning (ML) and Deep Learning (DL), exhibits robust outcomes in cybersecurity. However, Explainable Artificial Intelligence (XAI) has gained renewed focus to address transparency, ethics, and bias concerns [10].

Authors in [11] presented an audit fraud detection technique using EfficientNet. However, with the continual upgrading of financial fraud systems, classical recognition techniques relying on ML and rule matching have inadequate performance in intricate and high-dimensional financial data settings. Authors in [12] proposed a credit card anomaly detection model depending on hierarchical multisource data feature fusion. The system integrates transaction features with hierarchical fusion and dropout to improve anomaly detection and model generalizability. Authors in [13] discussed AI techniques for fraud detection. Using ML, DL, and data analysis techniques, AI improves the speed, precision, and efficiency of fraud detection.

Authors in [14] introduced Self-Attention Generative Adversarial Networks (SAGANs) for credit card fraud detection. SAGANs utilize self-attention and Generative Adversarial Networks (GANs) to improve fraud detection by detecting key patterns and generating realistic fraudulent behavior. Authors in [15] combined DL with Particle Swarm Optimizer (PSO) to improve accounting fraud detection. By optimizing DL parameters, the hybrid model improves fraud detection precision. Authors in [16] emphasized the need for improved security using ML methods, including logistic regression, AdaBoost, and Random Forest (RF), to build a strong hybrid approach.

Existing models improve fraud detection but still face challenges such as data imbalance, false positives, and lack of explainability. They often lack integrated frameworks and real-time adaptability for dynamic financial environments.

This study proposes a Fraud Detection System using Recursive Feature Elimination and Waterwheel Plant Optimization (FDS-RFEWPO) model for financial transactions. The major contributions of the FDS-RFEWPO model are:

- The FDS-RFEWPO method applies min-max normalization to scale features within a defined range, improving convergence during training and preventing bias caused by differing feature magnitudes, which enhances learning efficiency and performance.
- The FDS-RFEWPO model uses the Recursive Feature Elimination (RFE) technique to select the most influential features by recursively removing less important ones, reducing dimensionality and computational overhead while improving model generalization.
- The FDS-RFEWPO approach integrates a Variational Autoencoder (VAE) and a Wasserstein Autoencoder (WAE) to capture complex data patterns for robust fraud detection, whereas the Waterwheel Plant Optimization (WPO) model fine-tunes hyperparameters to improve accuracy, training efficiency, and adaptability.
- The FDS-RFEWPO technique incorporates Local Interpretable Model-Agnostic Explanations (LIME) to improve the interpretability and transparency of DL and ML predictions, allowing users to comprehend model decisions, build trust, and facilitate informed analysis and debugging of complex outputs.

- The novelty of the FDS-RFEWPO model lies in its unique integration of advanced Autoencoder (AE) methods with an efficient optimization algorithm and interpretability techniques. This integration not only improves fraud detection accuracy but also provides clear, transparent explanations of model decisions, addressing both performance and trustworthiness simultaneously.

II. RESEARCH METHOD AND DESIGN

This paper presents an FDS-RFEWPO approach for financial transactions. The aim is to perform a comprehensive evaluation of fraud detection in high-dimensional financial transactions using advanced techniques. Figure 1 illustrates the overall workflow of the FDS-RFEWPO approach.

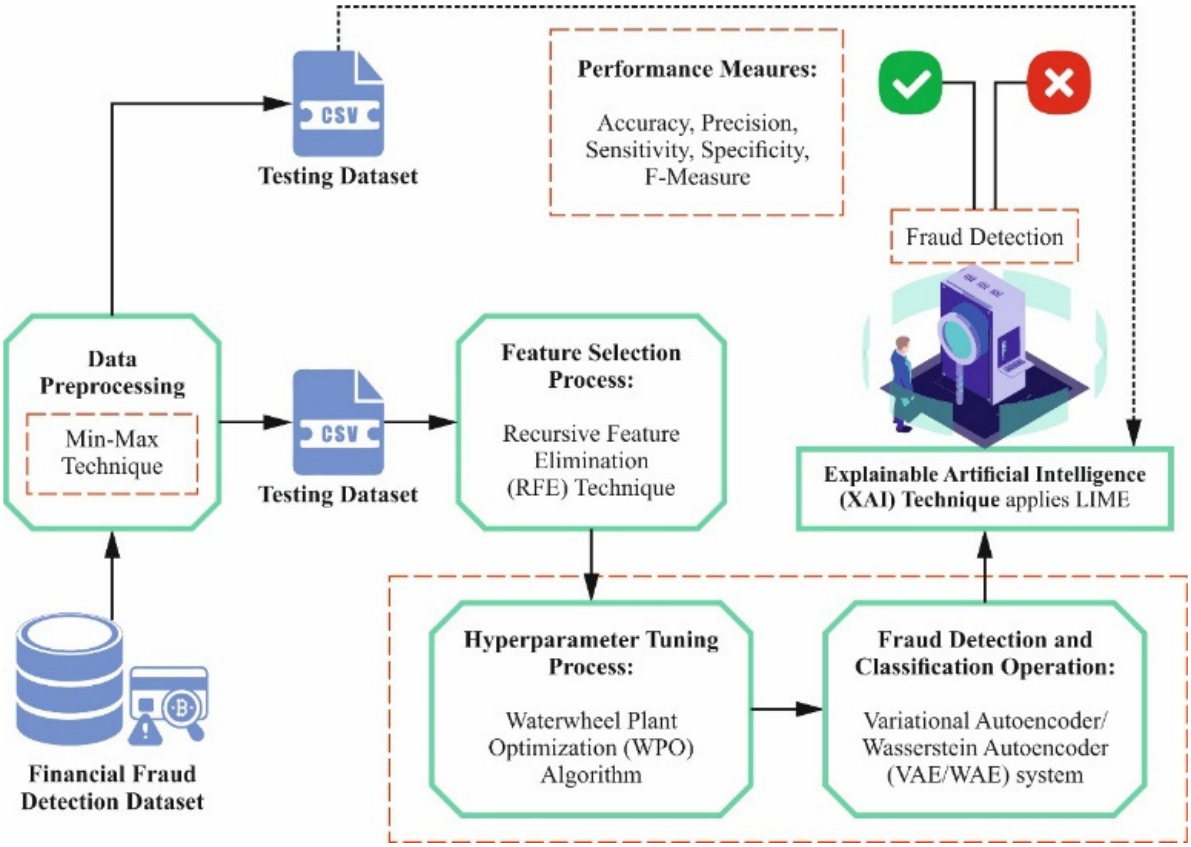

Fig. 1. Overall workflow of the FDS-RFEWPO method.

A. Data Scaling Using the Min-Max Technique

As a primary step, the FDS-RFEWPO technique applies min-max normalization to transform the input data [17]. This model is chosen for its efficiency in scaling features to a fixed range withing [0, 1], preserving the original distribution's shape without distorting relationships between values. Min–max scaling is simple and effective, maintaining positive, bounded values, which is ideal for neural networks by preventing feature dominance and improving training stability and convergence. Min-max normalization standardizes numerical features to a predetermined range, typically between zero and one, ensuring that every feature contributes equally to the learning process. It also increases the speed of convergence and stability in DL approaches. Min–max normalization is defined in (1):

$$x' = \frac{x - x_{min}}{x_{max} - x_{min}} \quad (1)$$

where x_{max} and x_{min} refer to the maximum and minimum values of the feature column, x indicates the original value, and x' denotes the normalized value.

B. Feature Subset Optimization with Recursive Feature Elimination

For the feature selection process, the FDS-RFEWPO model employs the RFE technique to select the most relevant features [18]. RFE is efficient in systematically detecting the most relevant features by recursively removing less crucial ones based on model weights. This technique enhances model performance by reducing dimensionality, mitigating overfitting, and lowering computational cost while using the learning algorithm to select the most relevant features for enhanced accuracy and interpretability.

RFE iteratively trains a model, ranks feature importance based on performance, and removes the least significant features in each cycle until the optimal subset is identified.

Feature importance can be calculated depending on the method used. For example, in linear models:

$$Feature\ Importance = |\beta_i| \quad (2)$$

where β_i is the coefficient of feature i in the linear model. For Support Vector Machines (SVM), feature importance is derived from the decision hyperplane weights:

$$Feature\ Importance = |w_i| \quad (3)$$

where w_i represents the weight associated with feature i in the decision hyperplane.

C. Fraud Detection Using the Variational Autoencoder and Wasserstein Autoencoder Models

The FDS-RFEWPO method employs the VAE and WAE models for fraud detection [19]. These models are chosen for their ability to learn intrinsic data distributions and detect anomalies by reconstructing input data. They are effective at identifying subtle anomalies and handling class imbalance in fraud datasets. By reducing the Wasserstein distance, WAE improves stability and reconstruction quality, enhancing detection accuracy and reducing false positives.

The VAE consists of two main components: an encoder $q_\varphi(z|x)$, which maps input x to a latent representation z, and a decoder $p_\theta(x|z)$ which reconstructs the input from z. The training objective is to maximize the Evidence Lower Bound (ELBO), given in (4):

$$\mathcal{L}(\theta, \varphi; x) = \mathbb{E}_{q_\varphi(Z|X)}[logp_\theta(x|z)] - D_{KL}(q_\varphi(z|x)\|p(z)) \quad (4)$$

Here, x denotes the input data, z is the latent variable capturing the encoded representation of x, $q_\varphi(z|x)$ is the encoder estimating the posterior of z, $p_\theta(x|z)$ is the decoder reconstructing x, $p(z)$ is the prior distribution of z, $\mathbb{E}_{q_\varphi(Z|X)}[logp_\theta(x|z)]$ is the reconstruction loss, and $D_{KL}(q_\varphi(z|x)\|p(z))$ is the Kullback-Leibler (KL) divergence.

One limitation of VAE is posterior collapse, where the latent space fails to capture meaningful variation in input data. To address this, WAE introduces a regularization term to align the latent distribution $q_\varphi(z)$ with the prior $p(z)$ using the Maximum Mean Discrepancy (MMD), formulated in (5):

$$\mathcal{L}_{WAE} = \mathbb{E}_{q_\varphi(z|x)}[logp_\theta(x|z)] + \lambda \cdot MMD\left(q_\varphi(z), p(z)\right) \quad (5)$$

Here, $MMD(q_\varphi(z), p(z))$ measures the variance between the prior $p(z)$ and the latent distribution $q_\varphi(z)$, and λ is a hyperparameter balancing the trade-off between latent space smoothness and reconstruction accuracy.

D. Parameter Optimization Using Waterwheel Plant Optimization

The WPO approach is used for parameter tuning to ensure that the optimal parameters are selected for improved accuracy [20]. This approach is chosen for its effective global searching capability and low computational complexity. It balances exploration and exploitation through dynamic parameter adjustment, enabling faster convergence and improved accuracy when tuning intrinsic ML and DL models.

WPO is a population-based stochastic optimizer inspired by the natural foraging behavior of waterwheel plants. It iteratively explores solution spaces by mimicking how water plants locate and capture prey, guiding the model toward optimal solutions. The representation of waterwheel positions is given in (6):

$$O = \begin{bmatrix} o_{1,1} & \cdots & o_{1,i} & \cdots & o_{1,n} \\ o_{2,1} & \cdots & o_{2,i} & \cdots & o_{2,n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ o_{j,1} & \cdots & o_{j,i} & \cdots & o_{j,n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ o_{M,1} & \cdots & o_{M,i} & \cdots & o_{M,n} \end{bmatrix} \quad (6)$$

Here, M and n denote the number of waterwheels and variables, respectively. Each component is computed as:

$$o_{j,i} = l_{ai} + q_{j,i} \cdot (u_{ai} - l_{ai})$$

where $j = 1, \ldots, M$ and $i = 1, \ldots, n$, and $q_{j,i}$ is a uniformly distributed random number between 0 and 1. The upper and lower limits of the i-th variable are u_{ai} and l_{ai}, respectively. The o_j represents the j-th waterwheel, and O represents the population matrix that encodes all waterwheel positions.

Each waterwheel evaluates its objective function as in (7):

$$e_j = \begin{bmatrix} e(Y_1) \\ e(Y_2) \\ \vdots \\ e(Y_n) \end{bmatrix} \quad (7)$$

where e_j is the calculated value for the j-th waterwheel and e denotes the vector of objective function values. Higher values indicate better solutions, whereas lower values indicate worse ones.

The position of each waterwheel is updated iteratively to search for optimal solutions:

$$Z = q_1 \cdot (O(s) + 2L),\ O(s+1) = O(s) + [Z + (2L + q_2)] \quad (8)$$

where $L \in [0,1]$ is an exponentially distributed random variable, $q_1 \in [0,2]$, and $q_2[0,1]$ are random numbers, and the vector Z represents the waterwheel's circular searching area. The updated position can also be expressed as:

$$O(s+1) = Gaussian(\mu_0, \sigma) + \left(\frac{q_1(O(s)+2L)}{Z}\right) \quad (9)$$

Furthermore, waterwheels are guided toward the best position found so far:

$$Z = q_3 \cdot \left(L_{best}(s) + q_3 O(s)\right),\ O(s+1) = O(s) + LZ \quad (10)$$

where $q_3 \in [0,2]$ and L_{best} is the best solution identified up to the current iteration. If no improvement is observed after three consecutive iterations, a mutation procedure is applied to avoid local minima traps:

$$O(s+) = (q_1 + L)sin\left(\frac{e(\theta)}{D}\right) \quad (11)$$

To ensure robust parameter tuning, the WPO method uses precision as the primary criterion for designing the fitness function, which is defined in (12)–(13):

$$Fitness = max(P) \quad (12)$$

$$P = \frac{TP}{TP+FP} \quad (13)$$

where TP and FP denote true positives and false positives, respectively.

With its low computational cost, WPO dynamically balances exploration and exploitation, adapts to challenges, handles noise effectively, and excels in complex optimization tasks. Its fitness-based hyperparameter selection improves model performance, making it an effective and scalable solution for real-world applications.

E. Explainable AI Using Local Interpretable Model-Agnostic Explanations

LIME is used to explain the predictions made by complex DL and ML techniques [21]. LIME builds a simple, interpretable model around a single prediction instance to highlight the features that most influenced the outcome. It generates synthetic data points around the instance x and uses a surrogate model $L(x)$ to approximate the behavior of the global model $M(x)$ in a defined neighborhood N:

$$L(x) \approx M(x), \quad x \in N \quad (14)$$

The goal is to develop a locally faithful approximation $L(x)$ that accurately reflects $M(x)$'s behavior near x, helping users understand the model's reasoning and increasing transparency and trust.

III. RESULT ANALYSIS AND VALIDATION

The performance analysis of the FDS-RFEWPO model is evaluated using a publicly available financial fraud detection dataset [22]. The dataset contains 10,000 instances classified into two classes: isFraud_Yes and isFraud_No, with 5,000 instances in each class. It includes 11 features, namely step, type, amount, nameOrig, oldbalanceOrg, newbalanceOrig, nameDest, oldbalanceDest, newbalanceDest, isFraud, and isFlaggedFraud. Of these, 9 features were selected for analysis, excluding the target variable isFraud and the flag isFlaggedFraud, which are used only for labeling and validation.

Figure 2 illustrates the correlation matrix generated by the FDS-RFEWPO model. The results demonstrate that the model successfully detects and identifies each class.

Table I presents a comparative analysis of the FDS-RFEWPO model against existing methods [23-25]. The baseline models include Artificial Neural Network (ANN), Quadratic Discriminant Analysis (QDA), DL, RF, Fuzzy Logic (FL), Hierarchical Temporal Memory–Cortical Learning Algorithm (HTM-CLA), and Long Short-Term Memory–ANN (LSTM-ANN). The results show that the FDS-RFEWPO model achieves the highest accuracy, precision, recall, and F-measure, with values of 97.41% for all four metrics.

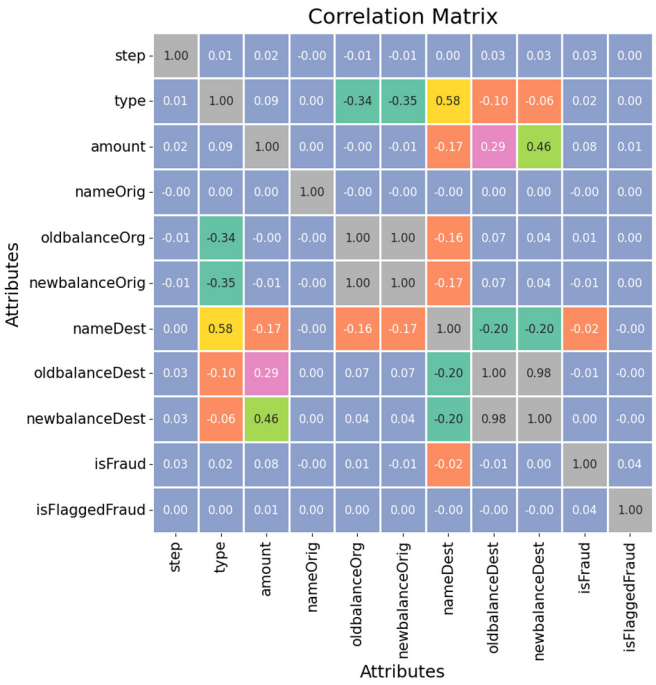

Fig. 2. Correlation matrix of the FDS-RFEWPO model for numerical features.

TABLE I. COMPARATIVE ANALYSIS OF THE FDS-RFEWPO MODEL AGAINST EXISTING METHODS

Method	Accuracy (%)	Precision (%)	Recall (%)	F-measure (%)
ANN	96.14	95.74	96.55	95.50
QDA	93.74	95.04	96.20	90.81
DL	86.06	94.73	89.42	93.88
RF	90.80	87.14	96.70	89.99
FL	95.36	91.49	91.30	96.79
HTM-CLA	93.59	88.61	93.71	96.54
LSTM-ANN	87.51	89.83	97.30	93.92
FDS-RFEWPO	97.41	97.41	97.41	97.41

IV. CONCLUSION

In this article, a Fraud Detection System using Recursive Feature Elimination and Waterwheel Plant Optimization (FDS-RFEWPO) for financial transactions is presented. The study aimed to perform a comprehensive evaluation of fraud detection in high-dimensional financial transaction data using advanced techniques.

Initially, the FDS-RFEWPO approach applies min-max normalization to scale and standardize input features. For feature selection, the Recursive Feature Elimination (RFE) technique is employed to identify the most relevant features. Fraud detection is performed using the Variational Autoencoder/Wasserstein Autoencoder (VAE/WAE) model, whereas the Waterwheel Plant Optimization (WPO) method is used to fine-tune model hyperparameters and ensure optimal performance. Finally, Explainable Artificial Intelligence (XAI) techniques, specifically Local Interpretable Model-Agnostic Explanations (LIME), are applied to improve transparency, interpretability, and trustworthiness of the predictive model.

The experimental analysis on a financial fraud detection dataset demonstrates that the FDS-RFEWPO model achieves superior performance, reaching an accuracy of 97.41%, outperforming existing techniques.

The limitations of the FDS-RFEWPO model include limited generalizability across diverse financial institutions due to dataset constraints and potential biases in class distributions. The system may also face challenges in adapting to evolving fraud tactics and rare fraud scenarios. Future work should explore integrating adaptive learning strategies and incorporating domain-specific contextual understanding to enhance robustness and applicability in real-world financial environments.

REFERENCES

[1] W. Min, W. Liang, H. Yin, Z. Wang, M. Li, and A. Lal, "Explainable Deep Behavioral Sequence Clustering for Transaction Fraud Detection." arXiv, Jan. 12, 2021, https://doi.org/10.48550/arXiv.2101.04285.

[2] A. Ali *et al.*, "Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review," *Applied Sciences*, vol. 12, no. 19, Oct. 2022, Art. no. 9637, https://doi.org/10.3390/app12199637.

[3] S. S. Taher, S. Y. Ameen, and J. A. Ahmed, "Advanced Fraud Detection in Blockchain Transactions: An Ensemble Learning and Explainable AI Approach," *Engineering, Technology & Applied Science Research*, vol. 14, no. 1, pp. 12822–12830, Feb. 2024, https://doi.org/10.48084/etasr.6641.

[4] E. Parkar, S. Gite, S. Mishra, B. Pradhan, and A. Alamri, "Comparative study of deep learning explainability and causal ai for fraud detection," *International Journal on Smart Sensing and Intelligent Systems*, vol. 17, no. 1, Aug. 2024, Art. no. 23, https://doi.org/10.2478/ijssis-2024-0023.

[5] A. A. J. Al-hchaimi, M. F. Alomari, Y. R. Muhsen, N. B. Sulaiman, and S. H. Ali, "Explainable Machine Learning for Real-Time Payment Fraud Detection: Building Trustworthy Models to Protect Financial Transactions," in *Proceedings of the 2nd International Conference on Explainable Artificial Intelligence in the Digital Sustainability Administration*, Basrah, Iraq, 2024, pp. 1–25, https://doi.org/10.1007/978-3-031-63717-9_1.

[6] A. A. Alhashmi, A. M. Alashjaee, A. A. Darem, A. F. Alanazi, and R. Effghi, "An Ensemble-based Fraud Detection Model for Financial Transaction Cyber Threat Classification and Countermeasures," *Engineering, Technology & Applied Science Research*, vol. 13, no. 6, pp. 12433–12439, Dec. 2023, https://doi.org/10.48084/etasr.6401.

[7] A. K. M. Emran and M. T. H. Rubel, "Big Data Analytics And Ai-Driven Solutions For Financial Fraud Detection: Techniques, Applications, And Challenges," *Frontiers in Applied Engineering and Technology*, vol. 1, no. 1, pp. 269–285, Dec. 2024, https://doi.org/10.70937/faet.v1i01.40.

[8] Y. Zhang, Y. Li, G. Zhang, Z. Ding, Y. Wu, and Y. Peng, "Application of Ensemble Learning Based on High-Dimensional Features in Financial Big Data," in *Artificial Intelligence Security and Privacy: Second International Conference*, Guangzhou, China, 2025, pp. 117–130, https://doi.org/10.1007/978-981-96-1148-5_10.

[9] A.-A. Al-Maari, M. Abdulnabi, Y. Nathan, A. Ali, U. Ali, and M. Khan, "Optimized Credit Card Fraud Detection Leveraging Ensemble Machine Learning Methods," *Engineering, Technology & Applied Science Research*, vol. 15, no. 3, pp. 22287–22294, Jun. 2025, https://doi.org/10.48084/etasr.10287.

[10] D. A. Pustokhin and I. V. Pustokhina, "Statistical Machine Learning Model and Commodity Futures Volatility Information for Financial Stock Market Forecasting," *American Journal of Business and Operations Research*, vol. 7, no. 2, pp. 32–40, Aug. 2022, https://doi.org/10.54216/AJBOR.070203.

[11] X. Du, "Audit Fraud Detection via EfficiencyNet with Separable Convolution and Self-Attention," *Transactions on Computational and Scientific Methods*, vol. 5, no. 2, Feb. 2025, Art. no. 14912715, https://doi.org/10.5281/zenodo.14912715.

[12] J. Wang, "Credit Card Fraud Detection via Hierarchical Multi-Source Data Fusion and Dropout Regularization," *Transactions on Computational and Scientific Methods*, vol. 5, no. 1, Jan. 2025, Art. no. 14979821, https://doi.org/10.5281/zenodo.14979821.

[13] T. Islam, S. A. M. Islam, A. Sarkar, A. J. M. O. R. Khan, R. Paul, and M. S. Bari, "Artificial Intelligence in Fraud Detection and Financial Risk Mitigation: Future Directions and Business Applications," *International Journal For Multidisciplinary Research*, vol. 6, no. 5, pp. 1–23, Oct. 2024, https://doi.org/10.36948/ijfmr.2024.v06i05.28496.

[14] C. Zhao, X. Sun, M. Wu, and L. Kang, "Advancing financial fraud detection: Self-attention generative adversarial networks for precise and effective identification," *Finance Research Letters*, vol. 60, Feb. 2024, Art. no. 104843, https://doi.org/10.1016/j.frl.2023.104843.

[15] R. Sivarethinamohan, "Integration of Deep Learning and Particle Swarm Optimization for Enhanced Accounting Fraud Detection," in *2023 International Conference on Data Science, Agents & Artificial Intelligence*, Chennai, India, 2023, pp. 1–7, https://doi.org/10.1109/ICDSAAI59313.2023.10452469.

[16] A.-A. Al-Maari and M. Abdulnabi, "Credit Card Fraud Transaction Detection Using a Hybrid Machine Learning Model," in *2023 IEEE 21st Student Conference on Research and Development*, Kuala Lumpur, Malaysia, 2023, pp. 119–123, https://doi.org/10.1109/SCOReD60679.2023.10563915.

[17] R. Mekala, "Hybrid Deep Learning Framework for Securing Cloud E-Commerce Through Big Data-Driven Fraud Detection and User Behavior Analytics," *Journal of Current Science*, vol. 10, no. 2, pp. 19–27, Dec. 2022.

[18] R. Hemnath, "Deep Learning-Based Framework for Smart Vehicular Traffic Management and Cybersecurity," *Indo-American Journal of Life Sciences and Biotechnology*, vol. 21, no. 2, pp. 43–62, Feb. 2024.

[19] F. Ullah *et al.*, "Synergizing Attribute-Guided Latent Space Exploration (AGLSE) with Classical Molecular Simulations to Design Potent Pep-Magnet Peptide Inhibitors to Abrogate SARS-CoV-2 Host Cell Entry," *Viruses*, vol. 17, no. 6, Jun. 2025, Art. no. 828, https://doi.org/10.3390/v17060828.

[20] B. Wu, "Research on the Strategy of Promoting Rural Tourism Development Through IoT Technology in Rural Revitalization," *International Journal of High Speed Electronics and Systems*, Jul. 2025, Art. no. 2540592, https://doi.org/10.1142/S0129156425405923.

[21] Y. Hosain and M. Çakmak, "XAI-XGBoost: an innovative explainable intrusion detection approach for securing internet of medical things systems," *Scientific Reports*, vol. 15, no. 1, Jul. 2025, Art. no. 22278, https://doi.org/10.1038/s41598-025-07790-0.

[22] "Financial Fraud Detection Dataset." Kaggle. [Online]. Available: https://www.kaggle.com/datasets/sriharshaeedala/financial-fraud-detection-dataset.

[23] N. S. Aghili, M. Rasekh, H. Karami, V. Azizi, and M. Gancarz, "Detection of fraud in sesame oil with the help of artificial intelligence combined with chemometrics methods and chemical compounds characterization by gas chromatography–mass spectrometry," *LWT*, vol. 167, Sep. 2022, Art. no. 113863, https://doi.org/10.1016/j.lwt.2022.113863.

[24] S. Othman, N. R. Mavani, M. A. Hussain, N. A. Rahman, and J. Mohd Ali, "Artificial intelligence-based techniques for adulteration and defect detections in food and agricultural industry: A review," *Journal of Agriculture and Food Research*, vol. 12, Jun. 2023, Art. no. 100590, https://doi.org/10.1016/j.jafr.2023.100590.

[25] E. N. Osegi and E. F. Jumbo, "Comparative analysis of credit card fraud detection in Simulated Annealing trained Artificial Neural Network and Hierarchical Temporal Memory," *Machine Learning with Applications*, vol. 6, Dec. 2021, Art. no. 100080, https://doi.org/10.1016/j.mlwa.2021.100080.