

# An Intelligent Optimization-Based Deep Belief Network for Fraud Detection in Financial Transaction Systems

## Hafis Hajiyev

Department of Finance and Audit, Azerbaijan State University of Economics (UNEC), Baku, Azerbaijan  
hafiz\_hajiyev@unec.edu.az (corresponding author)

## Emil Hajiyev

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

## Mirzobek Avezov

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

## Samariddin Makhmudov

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

## Dilora Abdukhalikova

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

Received: 6 October 2025 | Revised: 28 October 2025, 8 November 2025, and 11 November 2025 | Accepted: 15 November 2025

Licensed under a CC-BY 4.0 license | Copyright (c) by the authors | DOI: <https://doi.org/10.48084/etasr.15346>

## ABSTRACT

Financial fraud is one of the most crucial challenges in the digital economy, with growing cutting-edge attacks threatening the security of online transactions. Since conventional fraud detection models are often inadequate in identifying advanced fraud schemes, advanced fraud detection approaches are required to prevent and recognize fraud in real time. In recent years, the progression of AI methods has received considerable attention in the financial sector, specifically in Financial Fraud Detection (FFD). Furthermore, Explainable AI (XAI) has become a prerequisite for building trust and driving acceptance of AI methods in high-stakes domains, namely credit risks, financial crime, and healthcare, which require reliability, fairness, and safety. This study presents an Optimization-Based Deep Belief Network for Fraud Detection in Financial Transaction Systems (ODBN-FDFTS) approach, aiming to develop a reliable system for detecting financial transaction fraud. The ODBN-FDFTS approach begins with data preprocessing using a standard scaler to normalize financial transaction records and enhance data quality. The Artificial Rabbit Optimization (ARO) technique is employed for Feature Selection (FS), and a Deep Belief Network (DBN) is used for the financial fraud classification process, tuning its hyperparameters using the Butterfly Optimization Algorithm (BOA). LIME is integrated to provide transparency and interpretability in the fraud detection process. The comparison study of the ODBN-FDFTS model showed a superior accuracy of 97.95% over other methods on the FFD dataset.

*Keywords-financial fraud; explainable artificial intelligence (XAI); financial transactions; artificial rabbit optimization; deep learning*

## I. INTRODUCTION

Financial fraud is the act of employing fraudulent and illegal approaches to acquire financial advantages in various sectors, namely the taxation, corporate, insurance, and banking sectors [1]. Recently, money laundering, financial transaction fraud, and other types of financial fraud have become a growing problem [2]. Financial fraud causes significant economic damage for governments, particular individuals, and businesses [3]. With the improvement of AI methods, Data Mining (DM) and ML are utilized to identify fraudulent behaviors in the financial domain [4]. Classification techniques are a very common approach for identifying financial fraudulent transactions [5]. Explainable AI (XAI) techniques can achieve both explainability and important predictive efficiency [6]. Furthermore, DL is considered the most promising solution for handling fraud in financial transactions [7]. DL is a general term that relates to ML employing a deep multilayer Artificial Neural Network (ANN) [8]. Deep Neural Networks (DNNs) have received particular focus [9], improving accuracy and precision in several domains, including FFD.

This paper presents an Optimization-Based Deep Belief Network for Fraud Detection in Financial Transaction Systems (ODBN-FDFTS) model with the following contributions:

- Initially, preprocessing is performed for cleaning, normalizing, and structuring financial transactions to improve the reliability of subsequent analysis and FFD. It also ensures that the model receives relevant and well-prepared inputs for accurate classification.
- The AOR method is used to detect and choose the most relevant features, mitigating dimensionality and improving computational efficiency and crucial pattern detection. The DBN is used to precisely classify transactions, utilizing the optimized feature set for improved detection performance.
- BOA is employed to fine-tune the DBN hyperparameters, improving learning efficiency and accuracy for detecting fraudulent financial transactions, while XAI with LIME provides transparency, illustrating the key features and reasoning behind each classification to assist informed decision-making.
- A novel hybrid approach incorporates ARO and BOA with DBN to optimize FS and hyperparameter tuning. Coupled with LIME-based XAI, it achieves high accuracy while providing clear interpretability of fraud detection decisions. This framework ensures an effective and transparent FFD.

## II. EXISTING RESEARCH ON FRAUD DETECTION IN FINANCIAL TRANSACTIONS

This section presents a brief synthesis of the literature on fraud detection in financial transactions. In [10], generative methods were employed, utilizing a transformer-driven classification (LayoutLM) for FFD, enhanced with XAI methods for interpretability. In [11], an actual fraud detection structure integrated Federated Learning (FL) and adaptive Graph NNs (GNNs) to address these restrictions. In [12], a novel ML technique was combined with an XAI model. In

[13], a model utilized Node2Vec graph embedding and DNN for scalable parallel processing. The study in [14] explored the utilization of actual ML methods in transforming fraud detection. In [15], SHAP was employed to enhance the transparency of methods in the domain of FFD. Despite these merits, existing studies face limitations in scalability, interpretability, and real-time adaptability, indicating a research gap in developing unified, explainable, and efficient FFD models.

## III. PROPOSED MODEL

The proposed ODBN-FDFTS approach involves input data processing, ARO-based feature reduction, DBN-based classification, BOA-based tuning, and XAI using LIME. Figure 1 illustrates the flow of the ODBN-FDFTS model.

### A. Data Preprocessing

Data preprocessing is performed using a standard scaler method to normalize financial transaction records and boost the quality of input data [16]. The dataset covers numerous features that may have dissimilar measures. If every feature is not scaled in a normal way, the model will provide high significance to larger-scale attributes, making it demanding for the model to predict appropriately. To resolve this issue, numerical attributes are scaled utilizing the StandardScaler to ensure equality.

$$z = \frac{x - \mu}{\sigma} \quad (1)$$

where  $x$  denotes an original value,  $\mu$  denotes the mean,  $\sigma$  is the standard deviation, and  $z$  represents the standardized value.

### B. Feature Reduction Using ARO

The ARO approach is employed for the feature reduction process to identify the most crucial and relevant features [17]. This approach exhibits an effective exploration of the search space, mitigating dimensionality without losing critical data. This model provides faster convergence and better optimization performance compared to conventional methods, thus improving the accuracy of the model and computational efficiency. ARO is a meta-heuristic model based on the behavioral habits of rabbits. In ARO, the dual behaviors that rabbits have are defined according to their energy, and the changeover among the behaviors is made dependent on energy shrinkage. The ARO model simulates rabbit behavior using detour foraging and random hiding, regulated by an energy shrink factor. The early stages explore through detour foraging, later shifting to random hiding for exploitation as defined in

$$A(T) = 4 \left(1 - \frac{t}{T}\right) \ln \frac{1}{r} \quad (2)$$

where  $r \in [0,1]$  is a random number,  $t$  is the current iteration, and  $T$  is the overall iterations. During detour foraging, rabbits update their positions to explore the search space globally as

$$\begin{aligned} \vec{v}(r+1) &= \vec{x}(r) + R \cdot (\vec{x}(r) - \vec{x}(r)) + \\ &\text{round}(0.5 \cdot (0.05 + r_1)) \cdot n_{12} \\ i, j &= 1, \dots, n \text{ and } j \neq i \end{aligned} \quad (3)$$

here,  $\vec{x}_i(t)$  is the current position of the  $i$ -th rabbit,  $n_1 \sim N(0,1)$ ,  $r_1 \in [0,1]$  is random,  $R = L \cdot C$  defines the movement operator, and  $L$  determines the run length based on iteration progress and randomness. In the random hiding phase, rabbits dig multiple tunnels and select one randomly to reduce predation risk, which enables local exploitation. The position update is given by

$$\vec{v}_i(r+1) = \vec{x}_i(r) + R \cdot (r_4 \cdot \vec{b}(t) - \vec{x}(r)) \quad (4)$$

where  $i = 1, \dots, n$ ,  $\vec{b}(t)$  is a randomly preferred hiding location,  $r_4 \in [0,1]$ ,  $R$  is the running operator, and  $H$  is the hiding parameter. The new position is accepted only if it improves fitness, as demonstrated in:

$$\vec{x}_i(t+1) = \begin{cases} \vec{x}_i(t) & f(\vec{x}_i(t)) \leq f(\vec{v}_i(t+1)) \\ \vec{v}_i(t+1) & f(\vec{x}_i(t)) > f(\vec{v}_i(t+1)) \end{cases} \quad (5)$$

This mechanism assists ARO in balancing exploration and exploitation, avoiding local optima and improving global search. The fitness function balances minimizing selected features and maximizing classification performance.

$$Fitness = \alpha \gamma_R(D) + \beta \frac{|R|}{|C|} \quad (6)$$

where  $\gamma_R(D)$  denotes the error rate classification of the specified classifier,  $|R|$  signifies the cardinality of the chosen subset,  $|C|$  represents the overall feature counts in the dataset, and  $\alpha$  and  $\beta$  refer to dual parameters equivalent to the substance of classification quality and subset length.

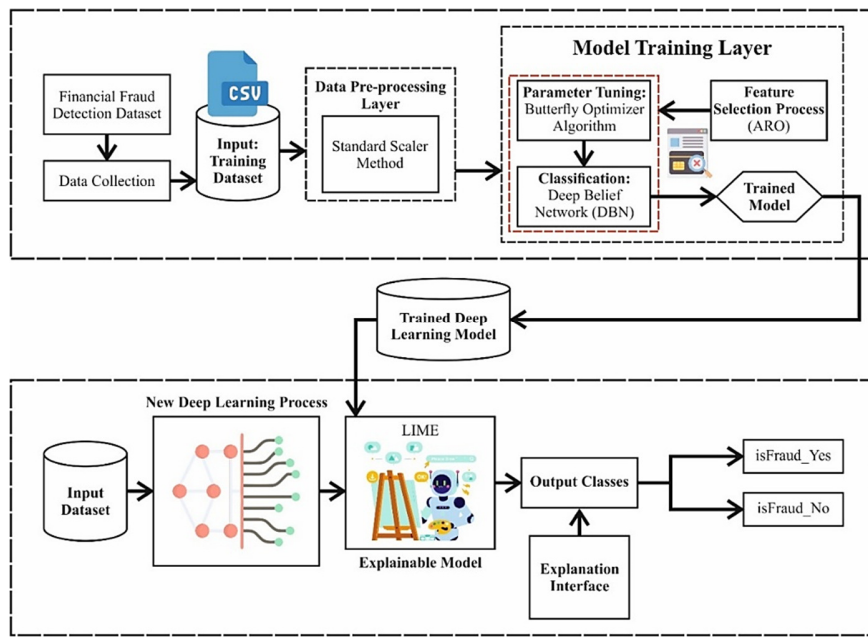


Fig. 1. Overall workflow of the ODBN-FDFTS model.

### C. Financial Fraud Classification Using DBN

A DBN model is employed to accurately detect FFD [18]. This model was selected for its ability to automatically learn hierarchical feature representations, capturing intrinsic patterns in transactional data. This technique presents high accuracy, robustness to noisy data, and improved generalization compared to conventional classifiers, making it appropriate for detecting subtle fraudulent activities. The DBN is molded by stacking three Restricted Boltzmann Machine (RBM) layers with 128, 64, and 32 nodes, followed by a Backpropagation (BP) layer for supervised fine-tuning, forming a joint probabilistic model. Key hyperparameters are tuned using BOA to optimize performance. Every RBM contains a visible layer  $u$  and a hidden layer (HL)  $h$ , with the system state expressed by an energy function.

$$E(u, h|\theta) = -\sum_{i=1}^n a_i v_i - \sum_{j=1}^m b_j h_j - \sum_{i=1}^n \sum_{j=1}^m w_{ij} v_i h_j \quad (7)$$

where  $\theta = (a, b, w)$  signifies the model parameter,  $a_j$  corresponds to the bias of the visible layer,  $b_j$  is the bias of HL, and  $w_{ij}$ ,  $u_j$ , and  $h_j$  represents a connection weight. The joint probability follows the Boltzmann distribution

$$P(v, h|\theta) = \frac{1}{Z(\theta)} e^{-1j(v, h|\theta)} \quad (8)$$

where  $Z(\theta) = \sum_{v, h} e^{-E(v, h|\theta)}$  represents a normalization factor. Based on the conditional independence theory, an activation probability of HL is expressed as

$$p(h_j = 1|v) = \sigma(b_j + \sum_{i=1}^n w_{ij} v_i) \quad (9)$$

On the other hand, the reconstruction probability of the visible layer is given by

$$p(v_i = 1|h) = \sigma(a_i + \sum_{j=1}^m w_{ij} h_j) \quad (10)$$

where  $\sigma(x) = 1/(1 + e^{-x})$  signifies the Sigmoid function.

The training objective is to enlarge the likelihood of the visible layer, given by:

$$\ln(p(V)) = \ln\left(\sum_{v,h} e^{-E(v,h)}\right) - \ln\left(\sum_h e^{-E(v,h)}\right) \quad (11)$$

Contrastive Divergence (CD) with Gibbs sampling updates visible and hidden layers for efficient parameter estimation.

$$\Delta w_{ij} = \frac{\partial \ln(p(V))}{\partial w_{ij}} = p(h_j = 1|V)v_i - \sum_v p(v)p(h_j = 1|v)v_i$$

$$\Delta w_i = \frac{\partial \ln(p(V))}{\partial a_i} = V_i - \sum_v p(v)v_i \quad (12)$$

$$\Delta b_j = \frac{\partial \ln(p(V))}{\partial h_j} = p(h_j = 1|V) - \sum_v p(v)p(h_j = 1|v)$$

It is worth noting that DBN has been employed in similar applications due to its capability to model deep hierarchical features from raw data.

#### D. BOA-Based Optimization Process

BOA is used for optimal hyperparameter tuning [19]. This method illustrates efficiency in global search capability and fast convergence toward optimal solutions compared to conventional methods. This approach also improves model accuracy, mitigates training time, and effectively balances exploration and exploitation, enhancing the performance of the DBN in FFD.

BOA-based hyperparameter optimization starts by defining bounds, dimensionality ( $D$ ), iterations, and population ( $N$ ). Each butterfly depicts a candidate hyperparameter set, with initial solutions generated randomly as

$$X_i = \{L_R, B_S, N_F, E, D_R\}_i, i = 1, 2, \dots, N \quad (13)$$

where  $X_i$  denotes the location of the  $i^{th}$  butterfly. The fitness of each solution is then evaluated using classification accuracy:

$$Fitness = \text{Max} \left( \frac{TP+TN}{TP+TN+FP+FN} \right) \quad (14)$$

The solution with the highest fitness is considered the best candidate. The update phase uses two strategies: fragrance and butterfly movement. Fragrance is computed using

$$fr = mI^p \quad (15)$$

where  $I$  is stimulus intensity,  $m$  is the sensory modality, and  $p$  is the power exponent. Butterflies move globally toward the best solution  $f$  and locally, as indicated in

$$d_i^{t+1} = d_i^t + (r^2 \times f - d_i^t) \times fr_i \quad (16)$$

$$d_i^{t+1} = d_i^t + (r^2 \times d_j^t - d_k^t) \times fr_i \quad (17)$$

where  $d_j^t$  and  $d_k^t$  are random butterflies, and  $r$  is a random number in  $[0,1]$ . The process repeats until the optimal hyperparameters are found, maximizing DBN performance.

Fitness selection is a significant factor inspiring the execution of the BOA approach. The parameter selection contains the solution encoder model to compute the candidate solution efficiency.

$$Fitness = \max(P) \quad (18)$$

$$P = \frac{TP}{TP+FP} \quad (19)$$

where TP and FP denote the true and false positive rates.

#### E. LIME

The last stage integrates LIME to present interpretability in the FFD process [20]. The integration of LIME ensures that the decisions are transparent and interpretable, allowing users to comprehend how predictions are made. This improves system trust and assists fairness by underscoring the features driving each classification. LIME highlights key factors influencing classification by approximating complex methods with simpler, interpretable models, making predictions easier to understand and explaining feature impact clearly. To attain this, LIME decreases the following function:

$$\varepsilon(x) = \text{argmin}_{g \in G} [\mathcal{L}(f, g, \pi_x) + \Omega(g)] \quad (20)$$

where  $f$  is the original model,  $g$  the interpretable one,  $x$  the input, and  $\pi_x$  denotes the variations.  $\mathcal{L}(f, g, \pi_x)$  shows how well  $g$  mimics  $f$ , while  $\Omega(g)$  reflects model complexity, highlighting key features driving fraud detection.

## IV. RESULTS AND DISCUSSION

The proposed ODBN-FDFTS was evaluated on the FFD dataset [21], which contains 16,000 examples, evenly split between fraudulent (isFraud\_Yes) and non-fraudulent (isFraud\_No) cases, with 11 features: step, type, amount, nameOrig, oldbalanceOrg, newbalanceOrg, nameDest, oldbalanceDest, newbalanceDest, isFraud, and isFlaggedFraud. Using the ARO approach, step and isFlaggedFraud were eliminated, which reduced training time, slightly improved accuracy, and improved model interpretability by focusing on the most relevant transaction features. Figure 2 shows the classification analysis of the ODBN-FDFTS method.

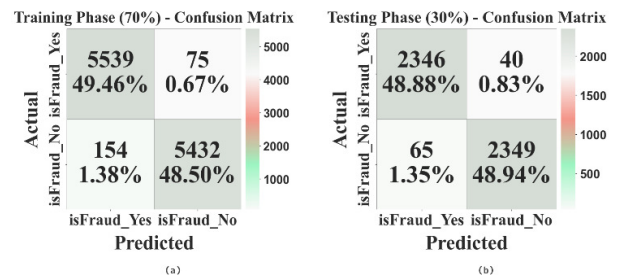


Fig. 2. Classification analysis.

Table I illustrates the comparative study of ODBN-FDFTS with [21, 22] under various measures. Based on  $accuracy$ , the ODBN-FDFTS model reached the highest  $accuracy$  of 97.95%. In addition, the ODBN-FDFTS model achieved the lowest Computational Time (CT) of 10.09 s, showing its high efficiency for the FFD process.

TABLE I. COMPARATIVE STUDY OF ODBN-FDFTS MODEL WITH EXISTING APPROACHES

Model	Accur <sub>y</sub>	Preci <sub>n</sub>	Recal <sub>l</sub>	F1 <sub>score</sub>	CT
Stacking Model [21]	95.00	96.34	93.00	94.00	20.31
AIDE Model [22]	96.26	90.37	86.78	90.85	24.39
FT [22]	96.50	81.15	96.45	89.19	24.75
ODBN-FDFTS (Proposed)	97.95	97.97	97.95	97.96	10.09

Table II depicts the ablation analysis of the ODBN-FDFTS technique. The proposed DBN, enhanced with FS using ARO and further tuned using BOA, exhibited robust performance, achieving accur<sub>y</sub> of 97.95%, preci<sub>n</sub> of 97.97%, recal<sub>l</sub> of 97.95%, and F1<sub>score</sub> of 97.96%, illustrating that integrating these strategies significantly improves fraud detection performance.

TABLE II. ABLATION STUDY-BASED COMPARATIVE ANALYSIS OF THE ODBN-FDFTS TECHNIQUE

Technique	Accur <sub>y</sub>	Preci <sub>n</sub>	Recal <sub>l</sub>	F1 <sub>score</sub>
DBN	95.95	95.97	95.62	96.19
DBN+ARO (with FS without parameter tuning)	96.46	96.56	96.41	96.84
DBN+BOA (with parameter tuning without FS)	97.22	97.34	97.15	97.34
ODBN-FDFTS (DBN with FS and parameter tuning)	97.95	97.97	97.95	97.96

Table III shows that the ODBN-FDFTS approach required higher inference time, FLOPs, and GPU memory in terms of computational efficiency over conventional models such as CNN, XGB, RF, ADA, and DT [23]. The ODBN-FDFTS model is significantly more efficient, attaining the lowest inference time of 0.0352 s, minimal FLOPs of 0.34 G, and GPU usage of 783 M, emphasizing its suitability for fast and resource-efficient fraud detection.

TABLE III. COMPUTATIONAL EFFICIENCY COMPARISON OF DIVERSE MODELS FOR FRAUD DETECTION

Approach	Inference time (s)	FLOPs (G)	GPU (M)
CNN	2.55	11.91	2677
XGB	0.66	27.77	1811
RF	0.1494	15.01	2348
ADA	0.133	30	1891
DT	0.236	8.95	2245
ODBN-FDFTS	0.0352	0.34	783

## V. CONCLUSION

The proposed ODBN-FDFTS approach involves input data processing, ARO-based feature reduction, DBN-based classification, BOA-based tuning, and XAI using LIME. The comparison study of the ODBN-FDFTS model showed a superior accuracy of 97.95% over other methods on the FFD dataset. Limitations include dependence on a single dataset and a fixed feature set, which may limit the generalizability of the findings to other financial environments. Furthermore, real-time deployment and scalability were not fully explored. In addition, the interpretability was not deeply analyzed, which may affect trust and transparency in practical financial applications.

Future work may focus on investigating the approach on massive and more diverse datasets and incorporating adaptive mechanisms for dynamic fraud patterns. Future studies could also focus on improving model explainability and developing interpretable frameworks to assist decision-making for financial institutions.

## REFERENCES

- [1] T. Madhavappa and B. Sathyanarayana, "An efficient framework based on optimized CNN-RNN for online transaction fraud detection in financial transactions," *International Journal of System Assurance Engineering and Management*, vol. 16, no. 10, pp. 3354–3374, Oct. 2025, <https://doi.org/10.1007/s13198-025-02861-x>.
- [2] M. M. Ismail and M. A. Haq, "Enhancing Enterprise Financial Fraud Detection Using Machine Learning," *Engineering, Technology & Applied Science Research*, vol. 14, no. 4, pp. 14854–14861, Aug. 2024, <https://doi.org/10.48084/etasr.7437>.
- [3] 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>.
- [4] Y. Alghofaili, A. Albattah, and M. A. Rassam, "A Financial Fraud Detection Model Based on LSTM Deep Learning Technique," *Journal of Applied Security Research*, vol. 15, no. 4, pp. 498–516, Oct. 2020, <https://doi.org/10.1080/19361610.2020.1815491>.
- [5] E. P. Galla *et al.*, "Enhancing Performance of Financial Fraud Detection Through Machine Learning Model," *Journal of Contemporary Education Theory & Artificial Intelligence*, 2023.
- [6] Z. Rojan, "Financial Fraud Detection Based on Machine and Deep Learning: A Review," *Indonesian Journal of Computer Science*, vol. 13, no. 3, June 2024, <https://doi.org/10.33022/ijcs.v13i3.4059>.
- [7] I. K. Nti and A. R. Somanathan, "A Scalable RF-XGBoost Framework for Financial Fraud Mitigation," *IEEE Transactions on Computational Social Systems*, vol. 11, no. 2, pp. 1556–1563, Apr. 2024, <https://doi.org/10.1109/TCSS.2022.3209827>.
- [8] T. Karthikeyan, M. Govindarajan, and V. Vijayakumar, "Enhancing Financial Fraud Detection Through Chimp-Optimized Long Short-Term Memory Networks," *Traitement du Signal*, vol. 41, no. 2, pp. 835–845, Apr. 2024, <https://doi.org/10.18280/ts.410224>.
- [9] R. Liu, J. Huang, and Z. Zhang, "Tracking disclosure change trajectories for financial fraud detection," *Production and Operations Management*, vol. 32, no. 2, pp. 584–602, Feb. 2023, <https://doi.org/10.1111/poms.13888>.
- [10] R. Milad, "Real-Time Financial Fraud Detection Using Adaptive Graph Neural Networks and Federated Learning," *International Journal of Management and Data Analytics*, vol. 5, no. 1, pp. 98–110, Mar. 2025, <https://doi.org/10.5281/ZENODO.15107110>.
- [11] 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 *Explainable Artificial Intelligence in the Digital Sustainability Administration*, 2024, pp. 1–25, [https://doi.org/10.1007/978-3-031-63717-9\\_1](https://doi.org/10.1007/978-3-031-63717-9_1).
- [12] H. Zhou, G. Sun, S. Fu, L. Wang, J. Hu, and Y. Gao, "Internet Financial Fraud Detection Based on a Distributed Big Data Approach With Node2vec," *IEEE Access*, vol. 9, pp. 43378–43386, 2021, <https://doi.org/10.1109/ACCESS.2021.3062467>.
- [13] R. T. Potla, "AI in fraud detection: Leveraging real-time machine learning for financial security," *Journal of Artificial Intelligence Research and Applications*, vol. 3, no. 2, pp. 534–549, 2023.
- [14] P. Fukas, J. Rebstadt, L. Menzel, and O. Thomas, "Towards Explainable Artificial Intelligence in Financial Fraud Detection: Using Shapley Additive Explanations to Explore Feature Importance," in *Advanced Information Systems Engineering*, 2022, pp. 109–126, [https://doi.org/10.1007/978-3-031-07472-1\\_7](https://doi.org/10.1007/978-3-031-07472-1_7).

- [15] V. B. Kamble, K. Pisal, P. Vaidya, and S. Gaikwad, "Enhancing UPI Fraud Detection: A Machine Learning Approach Using Stacked Generalization," *Multidisciplinary on Science and Management*, vol. 2, no. 1, pp. 69–83, 2025.
- [16] S. Alazwari *et al.*, "Artificial rabbits optimization with transfer learning based deepfake detection model for biometric applications," *Ain Shams Engineering Journal*, vol. 15, no. 12, Dec. 2024, Art. no. 103057, <https://doi.org/10.1016/j.asej.2024.103057>.
- [17] G. Yu and Z. Luo, "Financial fraud detection using a hybrid deep belief network and quantum optimization approach," *Discover Applied Sciences*, vol. 7, no. 5, May 2025, Art. no. 454, <https://doi.org/10.1007/s42452-025-06999-y>.
- [18] N. S. Nordin and M. A. Ismail, "A hybridization of butterfly optimization algorithm and harmony search for fuzzy modelling in phishing attack detection," *Neural Computing and Applications*, vol. 35, no. 7, pp. 5501–5512, Mar. 2023, <https://doi.org/10.1007/s00521-022-07957-0>.
- [19] S. J. Chavakula, C. A. J. Albert, E. Ebenezer, M. H. Bhagat, and C. V. Mahamuni, "Explainable AI (XAI) Using SHAP and LIME for Financial Fraud Detection and Credit Scoring," in *2025 International Conference on Advanced Computing Technologies (ICoACT)*, Sivalasi, India, Mar. 2025, pp. 1–8, <https://doi.org/10.1109/ICoACT63339.2025.11005238>.
- [20] "Financial Fraud Detection Dataset." Kaggle, [Online]. Available: <https://www.kaggle.com/datasets/sriharshaedala/financial-fraud-detection-dataset>.
- [21] J. Jin and Y. Zhang, "The analysis of fraud detection in financial market under machine learning," *Scientific Reports*, vol. 15, no. 1, Aug. 2025, Art. no. 29959, <https://doi.org/10.1038/s41598-025-15783-2>.
- [22] M. Binsawad, "Enhanced Financial Fraud Detection Using an Adaptive Voted Perceptron Model with Optimized Learning and Error Reduction," *Electronics*, vol. 14, no. 9, May 2025, <https://doi.org/10.3390/electronics14091875>.
- [23] F. L. Becerra-Suarez, H. Alvarez-Vasquez, M. G. Forero, F. L. Becerra-Suarez, H. Alvarez-Vasquez, and M. G. Forero, "Improvement of Bank Fraud Detection Through Synthetic Data Generation with Gaussian Noise," *Technologies*, vol. 13, no. 4, Apr. 2025, <https://doi.org/10.3390/technologies13040141>.