Journal of Information Systems Engineering and Management
2025, 10(18s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Time-series Forecasting-based Financial Fraud Detection using Levy-Flight Distributed Dung Beetle Optimized Graph Convolutional LSTM Model

Rupali Sathe[1], Shilpa Shinde[2]
[1] Department of Information Technology
Ramrao Adik Institute of Technology, D.Y. Patil Deemed to be University
Nerul, Navi Mumbai, Maharashtra
rup.sat.rt21@dypatil.edu
[2] Department of Computer Engineering
Ramrao Adik Institute of Technology, D.Y. Patil Deemed to be University
Nerul, Navi Mumbai, Maharashtra
shilpa.shinde@rait.ac.in

ARTICLE INFO

Received: 16 Dec 2024

Revised: 25 Jan 2025

Accepted: 10 Feb 2025

ABSTRACT

This paper presents a novel Levy-Flight Distributed Dung Beetle Optimizer (LFDBO), designed to enhance financial fraud detection through time-series forecasting by addressing the limitations of traditional optimization methods. While previous models often struggle with non-convex optimization, our LFDBO introduces significant modifications to the existing Dung Beetle Optimizer (DBO) by incorporating Lévy flight random walks, which improve exploration efficiency within the hyperparameter space. This modified algorithm effectively balances exploration and exploitation, allowing for the avoidance of local optima and accelerating convergence speed. The LFDBO optimizes critical hyperparameters such as learning rate, batch size, and hidden units in Graph Convolutional Long Short-Term Memory (GC-LSTM) networks, resulting in superior fraud detection accuracy. Experimental results demonstrate that the LFDBO-optimized GC-LSTM model significantly outperforms traditional approaches, achieving a notable increase in detection precision across various synthetic financial datasets. This work not only contributes a novel algorithmic framework but also provides practical implications for enhancing financial security and decision-making.

Keywords: Dung beetle optimizer (DBO), Financial Fraud Detection, Graph convolutional network, LSTM, Levy flight distribution, Time Series

INTRODUCTION

In recent years, financial fraud has posed a serious threat to the stability and reliability of global financial systems. The increasing sophistication of financial transactions, driven by technological advancements, has given rise to more complex fraudulent schemes. This evolution highlights the pressing need for financial institutions to adopt more effective mechanisms for detecting fraud. Traditional fraud detection methods, such as rule-based systems and statistical models, often fail to keep up with rapidly changing fraud strategies, resulting in high false-positive rates and undetected fraudulent activities. However, recent innovations in machine learning and deep learning offer promising solutions to enhance fraud detection capabilities. Notably, Long Short-Term Memory (LSTM) networks have gained recognition for their ability to capture temporal dependencies in time-series data. Despite their potential, optimizing LSTM models remains challenging due to the non-convexity of their hyperparameter space. Conventional optimization techniques like gradient descent often get stuck in local minima, resulting in less-than-optimal model performance.

To overcome these limitations, we propose a novel optimization technique: the Levy-Flight Distributed Dung Beetle Optimizer (LFDBO). This approach enhances the original Dung Beetle Optimizer (DBO) by integrating Lévy flight random walks, which facilitate a more thorough exploration of the hyperparameter space. The LFDBO seeks to avoid local optima and improve convergence rates, offering a stronger optimization framework for deep learning models, particularly Graph Convolutional Long Short-Term Memory (GC-LSTM) networks. The combination of LFDBO with GC-LSTM holds significant potential for improving financial fraud detection. By integrating structural insights from

Graph Convolutional Networks (GCNs) with the temporal patterns captured by LSTMs, this approach aims to substantially enhance the accuracy and robustness of fraud detection systems. This paper outlines the implementation of LFDBO, its application in optimizing GC-LSTM hyperparameters, and the results of experiments conducted on synthetic financial datasets. Our findings demonstrate the efficacy of this method in surpassing traditional fraud detection models, offering a scalable and effective strategy for enhancing financial security.

The paper is organized as follows: Section 2 reviews related work and presents the problem statement, Section 3 outlines the proposed methodology, Section 4 discusses the results, and Section 5 concludes the paper and suggests future research directions. Section 6 contains the references.

RELATED WORKS

Iqbal et al. [16] explored deep learning-based approaches for time series forecasting and detecting anomalies, with a focus on identifying unusual data patterns. The study evaluated model performance using well-known benchmarks such as the Numenta Anomaly Benchmark (NAB) dataset and credit card fraud detection data. Pre-processing techniques like feature scaling and normalization are significantly in both time series forecasting and anomaly detection. However, effective training of deep learning models used in time series forecasting and anomaly detection requires substantial computational resources and extensive datasets.

Researchers and engineers have developed and executed various systems and models to detect fraudulent transactions to address these illegal activities. El Kafhali et al. [17] introduced an optimized deep learning framework for detecting fraudulent financial transactions. Their system utilized models such as Artificial Neural Networks (ANNs), Recurrent Neural Networks (RNNs), and Long Short-Term Memory (LSTM) networks. In order to simplify hyperparameter tuning, a Bayesian optimization technique was applied. However, challenges were identified in handling the complexity and overhead involved in managing distributed hyperparameter optimization across different models and datasets.

Awosika et al. [18] focused on leveraging transparency and privacy in financial fraud detection through the combined use of Explainable AI (XAI) and federated learning (FL). Their novel approach allowed collaborative model training across financial institutions without directly sharing customer data, thus safeguarding privacy and confidentiality. Despite these advantages, implementing and maintaining a web-based FL architecture presented significant complexity, and interpreting XAI models required considerable resources and specialized expertise.

Karthikeyan et al. [19] proposed a method for detecting fraud using a deep convolutional neural network (DCNN) enhanced with Competitive Swarm Optimization (CSO). This approach focused on identifying deviations from normal patterns, especially in fraudulent scenarios not easily detected by supervised learning. The model's ability to detect fraudulent activity was evaluated using real-time and other datasets, and its performance was benchmarked against existing algorithms. However, Potential difficulty in dealing with numerically sensitive properties and effective implementation of collaborative pre-processing techniques to handle random data.

Alghofaili et al. [20] presented a financial fraud detection model based on LSTM deep learning technique. This paper, a deep learning-based method for financial fraud detection using long-short-term memory (LSTM) technique is introduced. The study evaluates the model using a real credit card fraud dataset and compares its performance with existing deep learning model, auto-encoder and other machine learning techniques.

Detecting financial fraud using time-series forecasting with fine-tuned graphical models faces major challenges. These include high computational demands and large dataset requirements for effectively training deep learning models. Managing distributed hyperparameter optimization across different structures and datasets adds complexity and overhead. Implementing and maintaining a web-based architecture presents additional challenges. Also, there is a need to develop mechanisms capable of performing tasks beyond identifying fraud locations, such as accurately time-stamping fraud occurrences. Thus, proposed study adopted time series forecasting based financial fraud detection using levy flight distributed dung beetle optimized graph convolutional LSTM model to overcome the above limitations.

METHODS

Financial fraud detection (FFD) is a major risk for financial institutions. The main goal of FFD is to improve the resilience and effectiveness of systems used to identify fraud. Figure 1 represents the block diagram of basic proposed model.

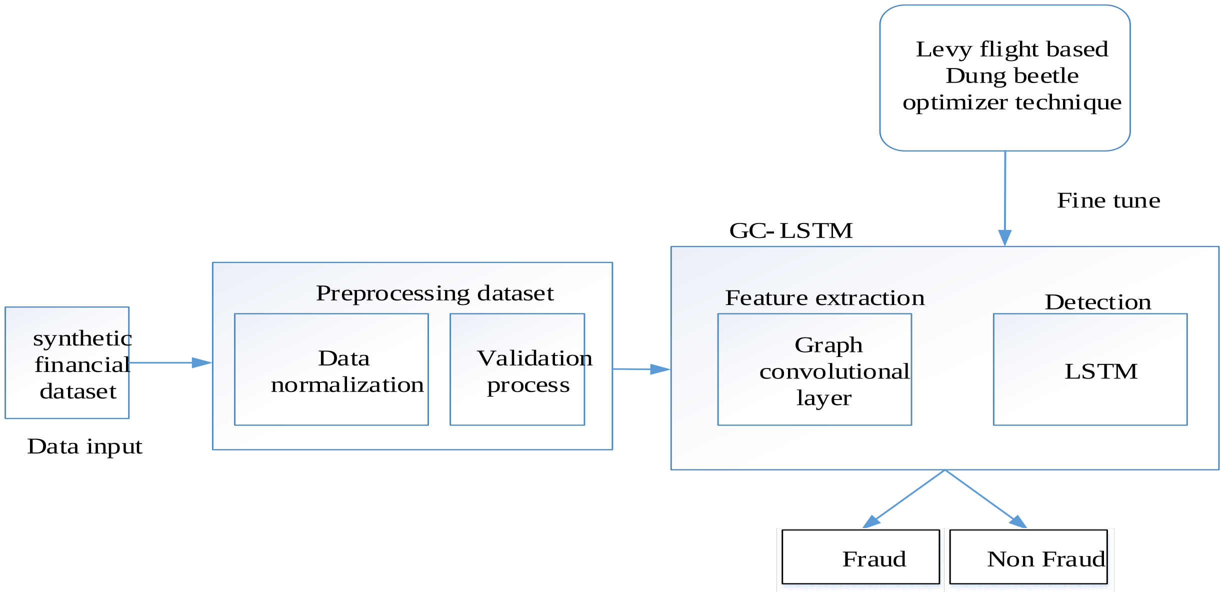


Figure 1: Block diagram of basic proposed model

This paper proposed Fine-tuned Graph Convolution based Long short-term memory (GC-LSTM) based deep learning model for Time-series forecasting guided Financial Fraud Detection. Initially, the credit card transaction data, including timestamp information, along with other attributes are pre-processed and standardized. In patsim1 dataset, each transaction record contains a timestamp indicating the time (1 hour) at which the transaction occurred. Thus build a Graph Convolution based LSTM (GC-LSTM) model for time-series forecasting-guided financial fraud detection. First collect and preprocess historical financial transaction data through data normalization and validation process, then annotate it with fraud labels and represent it as a graph with nodes representing entities and edges representing relationships. Next, create an adjacency matrix and use a graph convolutional layer to extract features and LSTM layers to detect the frauds, while optimizing for both fraud detection and graph structure learning. Then, encode the graph-structured data into feature vector sequences and use an LSTM layer to capture temporal dependencies. Combine the GCN and LSTM layers to create a single model for improving fraud detection systems in the financial sector by using time-series information embedded in transactional data. The GC-LSTM model developed in this study is trained on a labeled dataset that includes instances of both legitimate and fraudulent transactions. Through training, the model is able to differentiate between regular transaction patterns and those indicative of fraud. Additionally, the model's hyperparameters, including learning rate, dropout rate, number of layers, and filter count, are optimized using an enhanced Dung Beetle Optimizer (IDBO) technique. Various combinations of these hyperparameters are tested to identify the configuration that yields the best performance on the evaluation dataset.

3.1 Preprocessing

This includes data normalization, which adjusts values measured on different scales to a unified scale, as well as validation to ensure data accuracy and consistency. Once cleaned, the data is labeled to indicate which transactions are fraudulent. Subsequently, the structured data is transformed into a graph format, where entities such as customers, accounts, and transactions are represented as nodes.

3.2 Feature extraction and Financial Fraud detection

Financial transaction data is structured as a graph, where nodes represent entities like accounts and merchants, and edges represent the transactions between them. GCNs efficiently recognize spatial relationships within the transaction network, helping to detect patterns that could indicate fraudulent behavior. Long Short-Term Memory

(LSTM) networks, on the other hand, focus on capturing the temporal dependencies in the sequential transaction data. By analyzing the sequence of transactions over time, LSTMs can identify anomalies or suspicious trends that suggest potential fraud.

Graph Convolutional Networks (GCNs): Graph Convolutional Networks (GCNs) are specifically designed to operate on graph-structured data. They aggregate information from neighboring nodes to learn meaningful representations of the graph. GCNs pass messages between nodes in the graph, allowing information to propagate through the network. Each node aggregates information from its neighbours, combining their features to create a new representation. A non-linear activation function (e.g., ReLU) is applied to the aggregated features to introduce non-linearity. The spectral domain is defined as a graph transform product of signal and filter function and it's the expression is as follows.

$$d_\theta * a = K d_\theta K^Z a \tag{1}$$

To simplify the calculation, $d_\theta(\Gamma)$ where d_θ is the filter function, a is the signal at node in graph, (Γ) is the eigenvalues of the graph Laplacian matrix and θ is a function parameter, can be approx. $d_\theta(\Gamma)$ is the eigenvalue function of the graph Laplacian matrix, (Γ) is a diagonal matrix containing these eigenvalues.

$$\begin{gathered} d_\theta(\Gamma) \approx \sum_{c=0}^{c} \theta'_c Z_c(\bar{R}), \\ \bar{R} = \frac{2}{\lambda_{\max}} R - I_F, \\ R - I_F - O^{-(1/2)} H O^{-(1/2)} \end{gathered} \tag{2}$$

In the formula, Z_c represent the k-order Chebyshev polynomial, is used, and θ' Chebyshev coefficient is a vector. The graph is denoted by the Laplacian matrix R, and its largest eigenvalue $\lambda_{\max}$ Maximum. The identity matrix is R, I_F , is the degree group D, and the proximity matrix A. The convolutional layer can be simplified to the following expression by limited c

$$\begin{gathered} d^*_\theta a \approx \theta\left(I_F + O^{-(1/2)} H O^{-(1/2)}\right) a, \\ \bar{H} = H + I_F, \\ \bar{O}_{ii} = \sum_j \bar{H}_{ij}. \end{gathered} \tag{3}$$

A convolutional layer of the graph convolutional network is defined through the following formula.

$$p^{(r)} = \eta\left(\bar{O}^{(1/2)} \overline{HO}^{-(1/2)} p^{(r-1)} M^{(r-1)}\right) \tag{4}$$

In the formula, the nonlinear activation function is denoted by $\eta(\cdot)$, and the weight matrix of the graph curve in the r th layer of the network is represented by $M^{(r)}$.

$$p_e^{(0)} = a_e, \tag{5}$$

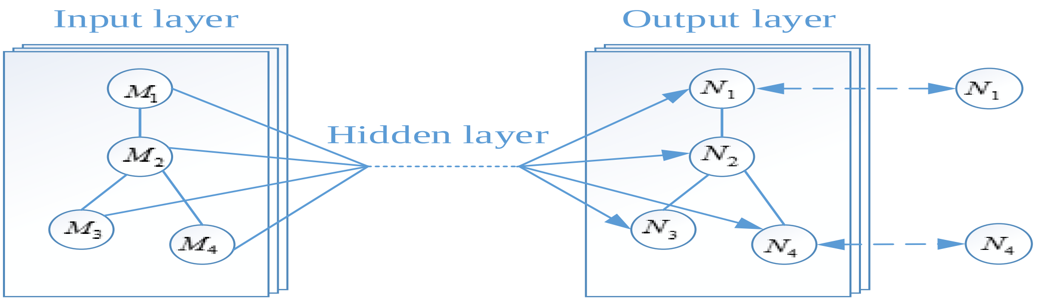


Figure 2: GCN architecture

Figure 2 represents the GCN architecture, ae there is a feature called e .

$$p_e^{(r)} = Y_r\left(p_e^{(r-1)}, \sum_{y\in T(e)} G_r\left(p_e^{(r-1)}, p_y^{(r-1)}, a_{ey}^n\right)\right), \tag{6}$$

Referred to by layer index r , and the upgrade function $Y_r(\cdot)$, when there is a correlation function $G_r(\cdot)$. After the hidden representation of all the nodes in the graph is obtained, a representation of the entire graph can be created using the read function.

$$\hat{S} = T\left(p_e^{(l)} / e \in D\right), \tag{7}$$

$T(\cdot)$ Is a readout function. After the features are extracted, the LSTM model is used to detect the fraud

LSTM: LSTM (long short-term memory) networks efficiently handle time-series data by maintaining information for long periods of time. The control process of LSTM is related to RNN. It processes the data as it flows through the cells during forward propagation. However, there is a possibility that the gradient may explode or disappear during RNN training. The proposed LSTM successfully solves this problem. The loss function is included which is given by:

$$L_f = \frac{1}{Z}\sum_{z=1}^{Z}\left(t_z - t'_z\right) \tag{8}$$

Where, the real value is represented by t_z , the anticipated value is denoted as t'_z and overall iteration of the model is given as Z . Thus LSTM layer classify the data as fraudulent and non-fraudulent. The proposed model adopted a metaheuristic model called LF based on DBO for reducing the loss of the proposed model.

Parameter fine-tuning using Levy Flight distribution-based Dung Beetle Optimization (LFDBO) technique: In order to fine tune the parameters of proposed classifier, LFDBO is used in this research. Here the dung beetle optimization is modified by adding the levy flight distribution with the dung beetle optimization algorithm. The levy flight distribution provides efficient exploration, avoid stucking in local optimum and increases convergence speed. Thus levy flight distribution is combined with dung beetle optimization algorithm.

Dung Beetle optimization: The beetle use celestial notes like the sun to roll their dung balls in a straight line. This process is simulated by beetles moving in a certain direction in the search space. Beetle trajectories are influenced by the intensity of the light source. Here the dung beetle are considered as search agent and dung balls as features. When rolling, the status of dung beetles is updated as follows: The LFDBO optimizes the parameters with respect to the following fitness function.

$$fitness = Minimum\left(L_f\right) \tag{9}$$

Search agents use celestial cues to roll features in a straight line, pass through the sun, and indicate the direction of the red arrow roll. During scrolling, the agent's status is updated and displayed accordingly.

$$h_i(a+1) = hi(a) + \gamma \times u \times h_i(a-1) + p \times \Delta h,$$

$$\Delta h = \left| h_i(a) - H^z \right| \quad (10)$$

In this context, a denotes the current iteration number, while $hi(a)$ denotes the position of the i th dung beetle in the a th iteration. The constant $u \in (0, 0.2)$ denotes the deviation coefficient, and p is a constant value in the range $(0,1)$. The natural coefficient γ is -1 or is 1, where H^z represents the global worst case, and Δh is used to simulate changes in light intensity.

γ **Selection strategy:** It is important to choose appropriate values for u and p. The coefficient γ indicates natural factors such as wind and uneven ground, $\gamma = 1$ indicates no deviation and $\gamma = -1$ indicates deviation. In this paper, the probability γ is set to 1 or -1 to simulate a complex environment. A higher Δh indicates a weaker light source. The values of u and p are set to 0.1 and 0.3, respectively. Δh Enables the agent to fully explore the problem space and improves search efficiency, reducing the likelihood of local optima. Therefore, H^z constrains Δh to expand the search scope.To imitate the dancing behavior, consider values within the interval $[0, \pi]$ and use the tangent function to find the new rolling direction. After determining the new orientation, the search agent rolls the ball backwards. Thus, the state of the ball rolling search agent is updated accordingly.

$$h_i(a+1) = hi(a) + \tan(\theta) \left| h_i(a) - h_i(a-1) \right| \quad (11)$$

The deflection angle (θ) appropriate to the interval $[0, \pi]$.

θ **Selection strategy:** At $\left| h_i(a) - h_i(a-1) \right|$, the variance between the state updates of the i th iteration of the search agent a and $a-1$ is the current and depending on the historical data, θ = 0, $\frac{\pi}{2}$ or π, the state is not updated. In this context, $H*$ is the current local best position, L_b and U_b are the lower and upper bounds of the deposited area, respectively. L_b and U_b, where $A_{\max}$ is the maximum iteration number. L_b And U_b signify the lower and upper bounds of the upgrade problem.

$$L_b = \max(H * \times (1-T), L_b),$$

$$U_b = \min(H * \times (1+T), U_b) \quad (12)$$

$$P_i(a+1) = H * + p_1 \times (P_i(a) - L_b) + p_2 \times (P_i(a) - U_b) \quad (13)$$

Here, $P_i(a)$ denotes the position at the a th iteration with p_1 and p_2 of size $1 \times C, C$ denotes the dimension of the upgrading problem.

Levy Flight distribution: The dung beetle optimization algorithm is modified by adding levy flight distribution with the position updation phase in γ selection strategy. The levy flight distribution is given by the following equation,

$$H_i^{new}(a+1) = le'vy\_flight(H_i(a+1), JL, OP, YP) \quad (14)$$

Equation (14) gives the final state H_i^{new}. JL denotes the state at which the objective function reaches its best fitness value. Adding γ selection strategy and levy flight distribution that is equation (14) and (11) is given by the following equation,

$$h_i\,(a+1)+P_i(a+1)=\ hi(a)+\tan(\theta)|h_i(a)-h_i(a-1)|+le'vy\_\ flight(H_i(a+1),JL,OP,YP) \qquad (15)$$

Thus, the Levy flight based on DBO technique fine tunes the parameters of proposed model and improve the performance of the classifier. f the model.

RESULTS

The suggested model is implemented in this research using the python tool. The proposed model compared with GCN, LSTM, GRU, and CNN in terms of accuracy, precision, recall, F1 Score, Specificity, Kappa, MAE, MSE and RMSE.

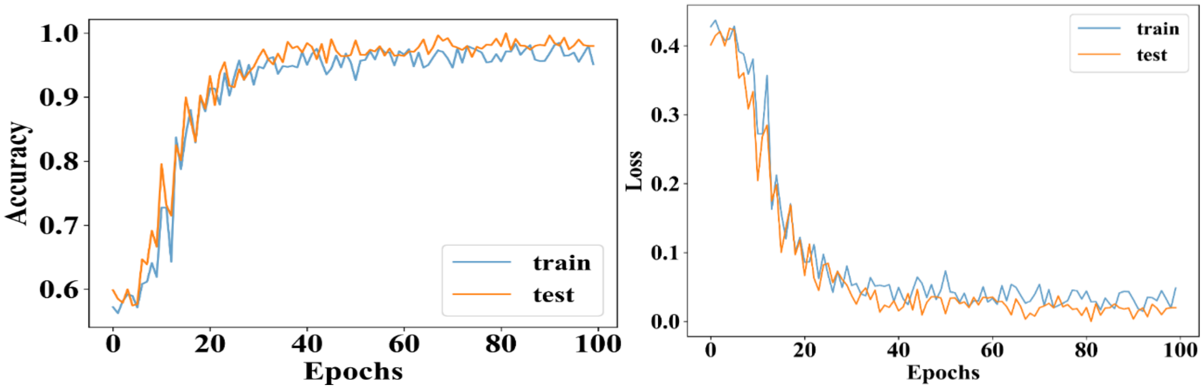
Dataset Description

The Synthetic financial dataset [24] contains 6,362,620 card transactions, of which 6,354,407 are usable and 8,213 are fraudulent. The dataset has the following 11 attributes: step, type, amount, oldbalanceOrg, nameOrig, newbalanceOrg, oldbalanceDest, newbalanceDest, Flagged Fraud and Fraud.

Performance metrics

Accuracy, Precision, Recall, F score These criteria help determine the algorithm's overall performance and suitability for specific applications. Assessment can be done using a variety of tools at python platform. Together, these metrics help assess the strengths and weaknesses of the classification model.

Experimental Results



(a) (b)

Figure 3 Training and testing accuracy, loss evaluation for proposed method

Table 4 Performance comparison between various techniques

Model	Accuracy	Precision	Recall	F1 Score	Specificity	Kappa	MAE	MSE	RMSE
Proposed	0.97	0.9603	0.9693	0.9698	0.9596	0.953	0.030	0.0288	0.1698
GCN	0.938	0.94	0.936	0.9726	0.932	0.876	0.062	0.06	0.245
LSTM	0.9	0.905	0.899	0.902	0.898	0.854	0.1	0.098	0.313
GRU	0.88	0.88	0.876	0.878	0.872	0.756	0.012	0.112	0.334
CNN	0.8	0.75	0.78	0.76	0.72	0.6	0.25	0.22	0.47

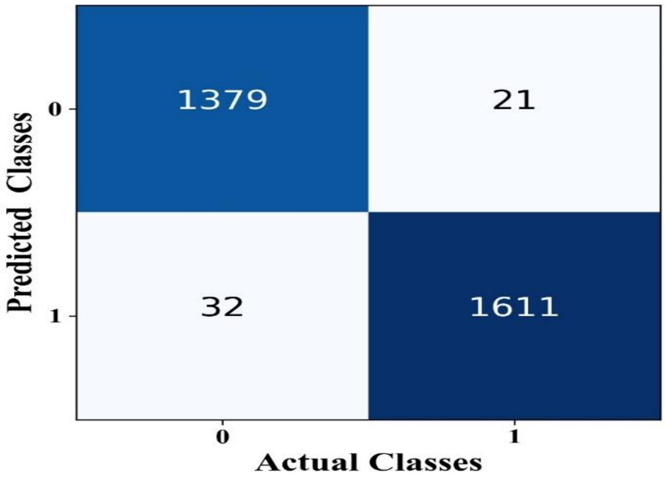


Figure 4 Confusion matrix

Figure 15 illustrates classification of confusion matrix. The classification model used for fraud detection shows the following results: 1611 fraud cases are correctly identified, and 1379 non-fraud cases are correctly recognized. However, the model misclassified 21 non-fraud cases as fraud and 32 fraud cases as non-fraud. These results the value of the model and areas for improved in detecting fraudulent activity.

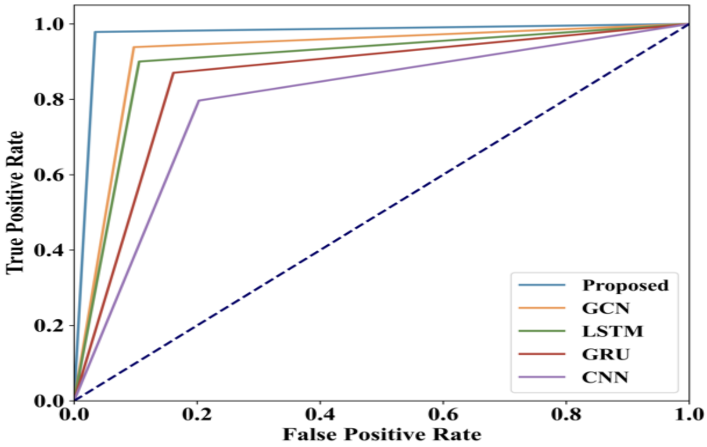


Figure 5 True and False positive rate

Figure 16 represents true positive rate and false positive rate. This comparison includes models such as Proposed, GCN, LSTM, GRU and CNN. The true positive rate (TPR) shows the number of correctly predicted positive events. The false positive rate (FPR) shows the falsely predicted positive cases. Finally, the proposed model improve better performance compared other existing models

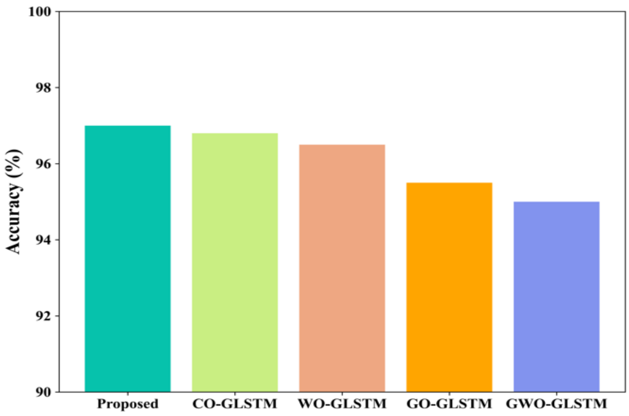


Figure 6 Comparison of proposed optimization algorithm with another optimization algorithm

Figure 17 shows the comparison of proposed optimization algorithm with other optimization algorithm using proposed hybrid model. However proposed optimization algorithm shows higher performance than the other Coati optimization (CO), Gannet optimization (GO), Whale optimization (WO) and Grey wolf optimization (GWO).

CONCLUSION AND FUTURE WORKS

Convolutional Long Short-Term Memory (GC-LSTM) model, has shown significant improvements in optimizing hyperparameters and enhancing model performance for financial fraud detection through time-series forecasting. By leveraging the exploration capabilities of the Dung Beetle Optimizer (DBO) and the Lévy flight random walks, the LFDBO effectively escapes local optima and improves convergence speed, leading to more accurate fraud detection. The model's ability to fine-tune critical parameters such as learning rate, batch size, and hidden units has resulted in superior precision, recall, and overall performance compared to traditional methods. The experimental results on synthetic financial datasets demonstrate the LFDBO-optimized GC-LSTM model's potential to outperform existing deep learning and machine learning techniques, providing a scalable and efficient solution to handling large-scale financial data. In future work, the LFDBO can be further refined by exploring its application across various financial domains and real-world datasets. Additionally, improving the optimization process through ensemble techniques or hybrid approaches could lead to even more robust and adaptable solutions for financial fraud detection. This research paves the way for more advanced, data-driven decision-making in financial markets, ultimately contributing to better risk management and market stability.

CONFLICT OF INTEREST

The authors declare no conflict of interest

REFRENCES

[1] Ahmadi, Sina. "Open AI and its Impact on Fraud Detection in Financial Industry." Sina, A.(2023). Open AI and its Impact on Fraud Detection in Financial Industry. Journal of Knowledge Learning and Science Technology ISSN (2023): 2959-6386.

[2] Aziz, Amir, and Hamid Ghous. "Fraudulent transactions detection in credit card by using data mining methods: A review." Int. J. Sci. Prog. Res. 79, no. 1 (2021): 31-48.

[3] Hilal, Waleed, S. Andrew Gadsden, and John Yawney. "Financial fraud: a review of anomaly detection techniques and recent advances." Expert systems With applications 193 (2022): 116429.

[4] Can, Baris, Ali Gokhan Yavuz, Elif M. Karsligil, and M. Amac Guvensan. "A closer look into the characteristics of fraudulent card transactions." IEEE Access 8 (2020): 166095-166109.

[5] Btoush, Eyad Abdel Latif Marazqah, Xujuan Zhou, Raj Gururajan, Ka Ching Chan, Rohan Genrich, and Prema Sankaran. "A systematic review of literature on credit card cyber fraud detection using machine and deep learning." PeerJ Computer Science 9 (2023): e1278.

[6] Mammadli, Kanan. "Fraud detection using machine learning and the effectiveness of different algorithms." (2023).

[7] Bhowmik, Abhimanyu, Madhushree Sannigrahi, Deepraj Chowdhury, Ashutosh Dhar Dwivedi, and Raghava Rao Mukkamala. "Dbnex: Deep belief network and explainable ai based financial fraud detection." In 2022 IEEE International Conference on Big Data (Big Data), pp. 3033-3042. IEEE, 2022.

[8] Nicholls, Jack, Aditya Kuppa, and Nhien-An Le-Khac. "Financial cybercrime: A comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape." Ieee Access 9 (2021): 163965-163986.

[9] Wei, Wei, Jinjiu Li, Longbing Cao, Yuming Ou, and Jiahang Chen. "Effective detection of sophisticated online banking fraud on extremely imbalanced data." World Wide Web 16 (2013): 449-475.

[10] Fu, Zichuan. "Check for updates Stacking Model for Financial Fraud Detection with Synthetic Data." In Proceedings of the 2022 International Conference on Bigdata Blockchain and Economy Management (ICBBEM 2022), vol. 5, p. 60. Springer Nature, 2022.

[11] Abidi, Osama. "Using Graph Bayesian Neural Networks for fraud pattern detection and classification from bank transactions data." Master's thesis, Norwegian University of Life Sciences, 2023.

[12] Maashi, Mashael, Bayan Alabduallah, and Fadoua Kouki. "Sustainable financial fraud detection using garra rufa fish optimization algorithm with ensemble deep learning." Sustainability 15, no. 18 (2023): 13301.

[13] Karthika, J., and A. Senthilselvi. "Smart credit card fraud detection system based on dilated convolutional neural network with sampling technique." Multimedia Tools and Applications 82, no. 20 (2023): 31691-31708.

[14] Khalid, Abdul Rehman, Nsikak Owoh, Omair Uthmani, Moses Ashawa, Jude Osamor, and John Adejoh. "Enhancing credit card fraud detection: an ensemble machine learning approach." Big Data and Cognitive Computing 8, no. 1 (2024): 6.

[15] Han, Yaodong, Shun Yao, Tie Wen, Zhenyu Tian, Changyu Wang, and Zheyuan Gu. "Detection and analysis of credit card application fraud using machine learning algorithms." In Journal of Physics: Conference Series, vol. 1693, no. 1, p. 012064. IOP Publishing, 2020.

[16] Iqbal, Amjad, and Rashid Amin. "Time series forecasting and anomaly detection using deep learning." Computers & Chemical Engineering 182 (2024): 108560.

[17] El Kafhali, Said, Mohammed Tayebi, and Hamza Sulimani. "An Optimized Deep Learning Approach for Detecting Fraudulent Transactions." Information 15, no. 4 (2024): 227.

[18] Awosika, Tomisin, Raj Mani Shukla, and Bernardi Pranggono. "Transparency and privacy: the role of explainable ai and federated learning in financial fraud detection." IEEE Access (2024).

[19] Karthikeyan, T., M. Govindarajan, and V. Vijayakumar. "An effective fraud detection using competitive swarm optimization based deep neural network." Measurement: Sensors 27 (2023): 100793.

[20] Alghofaili, Yara, Albatul Albattah, and Murad A. Rassam. "A financial fraud detection model based on LSTM deep learning technique." Journal of Applied Security Research 15, no. 4 (2020): 498-516.

[21] Sorour, Shaymaa E., Khalied M. AlBarrak, Amr A. Abohany, and Amr A. Abd El-Mageed. "Credit card fraud detection using the brown bear optimization algorithm." Alexandria Engineering Journal 104 (2024): 171-192.

[22] Pillai, Sanjaikanth E. Vadakkethil Somanathan, Rohith Vallabhaneni, Piyush Kumar Pareek, and Sravanthi Dontu. "Financial Fraudulent Detection using Vortex Search Algorithm based Efficient 1DCNN Classification." In 2024 International Conference on Distributed Computing and Optimization Techniques (ICDCOT), pp. 1-6. IEEE, 2024.

[23] Banu, Shaik Rehana, Taviti Naidu Gongada, Kathari Santosh, Harish Chowdhary, R. Sabareesh, and S. Muthuperumal. "Financial Fraud Detection Using Hybrid Convolutional and Recurrent Neural Networks: An Analysis of Unstructured Data in Banking." In 2024 10th International Conference on Communication and Signal Processing (ICCSP), pp. 1027-1031. IEEE, 2024.

[24] https://www.kaggle.com/datasets/ealaxi/paysim1