Enhancing Fraud Detection in Credit Card Transactions using Optimized Federated Learning Model

Mustafa Abdul Salam[1]*, Doaa L. El-Bably[2], Khaled M. Fouad[3], M. Salah Eldin Elsayed[4]
Faculty of Computers and Artificial intelligence, Benha University, Egypt[1, 2, 3, 4]
Department of Computer Engineering and Information, College of Engineering, Wadi Ad Dwaser, Prince Sattam Bin Abdulaziz University, Al-Kharj 16273, Saudi Arabia[1]
Faculty of Computer Science and Engineering, New Mansoura University, Mansoura, Egypt[1]
Higher Institute for Computers & Information Technology, ElShorouk, Cairo, Egypt[4]

***Abstract*—In recent years, credit card transaction fraud has inflicted significant losses on both consumers and financial institutions. To address this critical issue, we propose an optimized framework for fraud detection. This study deals with non-identically independent distributions (IIDs) involving different numbers of clients. The proposed framework empowers banks to construct robust fraud detection models using their internal training data. Specifically, by optimizing the initial global model before to the federated learning phase, the suggested optimization technique accelerates convergence speed by reducing communication costs when moving forward with federal training. The optimization techniques using the three most recent metaheuristic Optimizers, namely: An improved gorilla troops optimizer (AGTO), Coati Optimization Algorithm (CoatiOA), Coati Optimization Algorithm (COA). Furthermore, credit card data is highly skewed, which makes it challenging to predict fraudulent transactions. The resampling strategy is used as a preprocessing step to improve the outcomes of unbalanced or skewed data. The performance of these algorithms is documented and compared. Computation time, accuracy, precision, recall, F-measure, loss, and computation time are used to assess the algorithms' performance. The experimental results show that AGTO and (CoatiOA) exhibit higher accuracy, precision, recall, and F1 scores compared to the baseline FL Model. Additionally, they achieve lower loss values.**

***Keywords*—Credit card fraud detection (CCFD); federated learning; optimization algorithms; identically independent distributions (IIDs); metaheuristic optimization techniques**

I. Introduction

Credit card transactions have increased dramatically in recent years due to the rapid development of electronic services such as e-commerce, electronic banking, mobile payments, and the widespread use of credit cards. According to data, Visa [1] and Mastercard [2] issued 2023 million credit cards globally in 2022. Visa issued 1249 million cards worldwide, whereas MasterCard issued 1047 million. By mid-2023, the number of credit cards issued in the United States had increased by more than 30 million compared to the same period in 2022. These statistics indicate how card-based transactions grew popular among end customers.

Billions of dollars in credit card fraud losses will occur from widespread credit card use, a range of transaction circumstances, and weak verification and management. It is challenging to determine the loss exactly. The Nilson Report study (Dec 2022) [3] states that Mastercard faces a significant fraud risk due to the fact that it has 2.5 billion payment cards in more than 200 countries and territories worldwide. Credit card theft cost over $32 billion in 2021—roughly 6.6 cents for every $100 transaction. By 2027, card fraud will result in approximately $40 billion in gross losses worldwide. Two ways that fraudulent transactions could be carried out are using a stolen card that was obtained from either internal or external sources, or using credit card information that was obtained fraudulently [4].

Federated learning (FL) is a machine learning paradigm in which multiple clients collaborate to train a model while being managed by a central server [5]. FL never allows the server or other clients access to raw client data. Hyperparameter optimization poses new challenges in the FL setting and is a prominent open research area [6]. The level of communication influences how effectively a machine learning model performs. We examined a communication-efficient hyperparameter optimization strategy, a local hyperparameter optimization method that allows us to tune the hyperparameters before to the federation phase, to reduce communication costs, which are a significant barrier in FL [7]. Our offer comprehensive and reliable empirical benchmarks for federated optimization strategies that use metaheuristic optimization so that they can be compared. This study presents the following contributions:

- The Synthetic Minority Oversampling Technique (Smote) was used as a resampling method for unbalanced data.
- The conventional federated learning model has been utilized for Non-IID (Identical Independent Distribution) with different numbers of clients.
- Three metaheuristic optimization techniques were used to improve the initial model and reduce communication on a federated learning platform.
- To evaluate the effectiveness of the optimized models with the Federated Learning problem, the learning

process was repeated multiple times using the optimized global model.

This paper's remaining sections are organized as follows: Section 2 includes a comprehensive review of the existing literature. Section 3 outlines the methodologies taken and demonstrates each phase of the proposed federated paradigm. In Section 4, we examine and explain the experimental data, as well as compare the suggested method to previous research. Finally, Section 5 of the paper looks at prospective future research directions.

II. Related Works

The traditional machine learning approach, implicitly or explicitly, assumes the data distribution is identically independent. This scenario is suitable for collecting all data and then training in a distributed way. However, data is collected from various devices or institutions. Besides, there’s maybe a huge variety of data sizes in different nodes, thereby not following Identically Independent Distribution (IID). some research studies related to credit card fraud detection that specifically consider IID (Identically Distributed) datasets [8:10]. To address imbalanced credit card fraud detection datasets, the researchers [8] propose a novel approach that combines autoencoder (AE) and fully connected deep networks (FCDN) models. The process is divided into three stages: training an AE on fraudulent transactions, dimensionality reduction with another AE, and using encoded representations for FCDN classification. The model's performance is improved further by including an additional FCDN trained on preprocessed data using the synthetic minority oversampling technique (SMOTE). The integrated model architecture detects credit card fraud with high accuracy.

The study [9] employs machine learning algorithms to predict both legitimate and fraudulent credit card transactions. They assess algorithm performance using accuracy, sensitivity, specificity, Matthew's Correlation Coefficient, and Receiver Operating Characteristic (ROC) Area rates. The study applies the Synthetic Minority Oversampling Technique (SMOTE) to an imbalanced dataset and optimizes algorithms using feature selection methods. The study [10] suggests using an autoencoder-based classification scheme to extract credit card fraud characteristics from a European credit card dataset. They use encoded features to compare various machine learning algorithms in terms of classification consistency. The results indicate high accuracy, precision, recall, and F1 score.

Federated learning optimization is a demanding and active research subject with the goal of developing efficient and effective algorithms for learning models from decentralized data sources. Federated programming is a distributed learning paradigm in which multiple clients work together with a central server to build a model without providing their own training data1. This approach ensures data privacy, reduces communication costs, and enhances security by keeping sensitive information localized [11].

Federated learning tackles challenges by creating efficient algorithms for model learning from decentralized data sources. In this collaborative paradigm, multiple clients (such as banks or institutions) build a model without sharing raw training data with a central server.

Communication Bottlenecks in Federated Learning: Communication plays a pivotal role in federated learning, but it presents challenges: firstly, Limited Bandwidth: clients often face restricted communication bandwidth, hindering frequent data exchanges. Secondly, Compression Techniques: researchers explore compression communication techniques to efficiently transmit model updates to the central server. In the context of credit card fraud detection, federated learning holds promise. However, understanding the trade-offs between communication efficiency, model accuracy, and privacy preservation remains an active area of research.

In Fl, communication is regarded as a significant obstacle. Because clients often have limited communication bandwidth, limiting the quantity of communication or using compression communication techniques for model modifications to the central server becomes more important [12].

There are various previous works focused on credit card fraud detection problems. Table I elicits and summarizes these works.

TABLE I. Comparison of the Recent Previous Works

Research/ Publish Date	Contribution	Datasets	Techniques	Conclusion
[13]/ 2020	The purpose of this study is to provide IBM with a better understanding of federated learning and its potential applications. Specifically, they explore how Federated Averaging, a key technique in federated learning can be applied to address credit card fraud detection within the banking sector. Federated Averaging has been applied to the banking industry, where the aim was to detect credit card fraud.	European Credit Card (ECC) Obtained from Kaggle	SMOTE for oversampling the skewed datasets. PCA for high-dimensional datasets. MLP for centralized detecting fraudulent transactions. Federated Averaging. Mini-batch gradient descent as an optimizer.	Small Dataset Size Lack of Cost-Sensitive Learning Simple Model Updates. The study assumed no faulty nodes, and no missing data. Differential privacy and secure computation techniques were not implemented.

[6] /2019	A framework to train a fraud detection model using behavior features with federated learning, as well as an oversampling approach, is combined with balancing the skewed dataset. The performance evaluation of the credit card FDS with FFD framework on a large-scale dataset of real-world credit card transactions	European Credit Card (ECC) Obtained from Kaggle	A data level method: SMOTE is selected for data rebalancing. PCA Federated Convolutional Neural Network as a suitable ML algorithm for detecting credit card fraud	Small Dataset Size. Privacy concerns related to credit card fraud detection. Lack of Cost-Sensitive Learning.
[14] /2020	This model enables banks to learn fraud detection models with the training data distributed on their own local database.	European Credit Card (ECC) Revolution Analytics (RA) SD and Vesta from Kaggle	Feature extraction model and relation model The deep K-tuplet network as a novel meta-learning-based classifier	The study did not implement differential privacy or other secure computation techniques. These methods are essential for protecting sensitive data during federated learning. Lack of Cost-Sensitive Learning.
[15] /2020	Using under-sampling to balance the dataset because of the high imbalance class, implying skewed distribution. Applying NB, SVM, KNN, and RF to under-sampled class to classify the transactions into fraudulent and genuine, followed by testing the performance measures using a confusion matrix and comparing them. Examining these models against the entire dataset (skewed) using the confusion matrix and AUC (Area Under the ROC Curve) ranking measure to conclude the results to determine which would be the best model for us to use with a particular type of fraud.	dataset for European cardholders (ECC)	Under-sampling was used to remove the observation values from the majority class (genuine) randomly until the dataset reaches the balance because the minority class (fraudulent) is very small in comparison with the majority class. (PCA) to protect the true information from the analyst examining the data by transforming the original variables obtained during the collection of data. - NB, SVM, KNN, and RF to classify the transactions into fraudulent and genuine transaction.	The study focused exclusively on European banks, which may limit the generalizability of its findings to other regions. Lack of Cost-Sensitive Learning The research did not investigate privacy concerns related to credit card fraud detection.

III. Proposed Model

The notion of federated learning (FL) plays a crucial role in the banking industry, particularly in credit card fraud detection. The growth of CCFD systems raises concerns about data security and privacy protection, which FL intends to address. This work uses a federated learning model to detect credit card fraud. In Florida, communication is regarded as a significant obstacle. As a result, we provide thorough and reproducible empirical standards for evaluating federated optimization strategies using metaheuristic optimization techniques. This study presents a federated learning technique for CCFD that addresses data privacy concerns. The classical federated learning model was then applied to the non-IID dataset, which included many clients.

Furthermore, resampling strategies were proposed as a solution to overcome imbalanced class concerns and improve classification accuracy. Finally, optimization can significantly reduce the amount of communication needed to train a model on a federated learning platform.

Standard optimization strategies, such as extended SGD, are typically ineffective in FL and can incur high communication costs. To address this, we developed efficient models that were constantly updated prior to interacting with the server. This drastically reduces the amount of communication required to train a model on a federated learning platform. This study used three metaheuristic algorithms, as stated in Table II.

TABLE II. THE CHRONOLOGICAL TABLE OF USED METAHEURISTIC ALGORITHMS

Name	Abbreviation	Main Category	Subcategory	Year published	Ref.
Giant trevally optimizer.	**GTO**	Nature-inspired	Swarm-based	2022	[16]
An improved gorilla troops optimizer	**AGTO**	Nature-inspired	Swarm-based	2023	[17]
Coati Optimization Algorithm	**COA**	Nature-inspired	Swarm-based	2023	[18]

The Giant Trevally Optimizer (GTO) is a novel metaheuristic algorithm based on the natural hunting behavior of giant trevallies. Giant trevallies eat fish, cephalopods, and seabirds, including sooty terns. Giant trevallies' unique hunting strategies for seabirds have been mathematically modelled and divided into three major steps.

Algorithm Steps:

- Foraging Movement Patterns. The first step simulates giant trevallies' foraging movement patterns.

- Selecting the Right Area: In the second step, giant trevallies choose a food-rich area where they can hunt for prey.
- In the final step, trevallies chase and attack seabirds. When the prey is close enough, the trevallies jump out of the water to attack it in the air or snatch it from the water's surface.

An improved Gorilla Troops Optimizer (AGTO) is an improved for a metaheuristic algorithm inspired by gorillas' collective behavior and social intelligence. Like other metaheuristics, the basic GTO has limitations, particularly when dealing with complex and flexible optimization problems. To address these limitations and improve performance, the Improved Gorilla Troops Optimizer (IGTO) was proposed.

Here are the key enhancements introduced into IGTO:

- IGTO uses Circle Chaotic Mapping to initialize gorilla positions.
- This initialization technique increases population diversity and provides a solid foundation for global search.
- To avoid being trapped in local optima, IGTO uses a lens opposition-based learning mechanism.
- This mechanism broadens the search ranges, enabling the algorithm to investigate a larger solution space.
- IGTO uses a novel local search algorithm called adaptive β-hill climbing.

Combining this technique with GTO improves precision in determining the final β solution.

IGTO Increases exploration and exploitation capabilities and enhances solution quality, local optimum avoidance, and robustness.

Competitive performance on real-world tasks.

The Coati Optimization Algorithm (COA) is a novel bio-inspired metaheuristic that aims to model coatis' natural behaviors. These small mammals, native to Central and South America, exhibit fascinating behaviors that inspire the COA.

COA draws inspiration from coatis' hunting and survival strategies.

It considers both attacking behavior (when coatis hunt for prey) and escape behavior (when they come across predators).

COA mathematically models different stages of exploration and exploitation.

These two phases guide the algorithm's search process, allowing it to explore a wide range of solution spaces while focusing on promising regions.

To address optimization challenges, the Coati Optimization Algorithm (COA) combines natural inspiration and mathematical modeling. Its ability to explore diverse solution spaces while exploiting promising regions makes it a useful tool for both researchers and practitioners.

IV. Experimental Results and Discussion

The experiments in this work have been done using Python programming language (Python 3). In this work, we utilized open-source tools Scikit learn (1.1.3), pandas (1.4.4), NumPy (1.22.3), matplotlib (3.5.3), TensorFlow federated (0.17.0), mealpy 2.5.3, and Imblearn (0.9.1) in this work. The experiment was carried out using a desktop computer with an Intel core i7 1.80 GHz CPU, 16GB of RAM, and Windows 10 64-bit operating system. Wherever Times is specified, Times Roman of Times New Roman may be used. If neither is available on your word processor, please use the font closest in appearance to Times. Avoid using bit-mapped fonts if possible. True-Type 1 fonts are preferred.

A. *Datasets*

The Kaggle dataset [19] used in this study contains real but anonymous, credit card transactions made by European cardholders. The dataset includes 284807 credit card transactions from September 2013. There is no missing data, and just 492 of the 284807 transactions are fake, yielding a highly skewed dataset. Furthermore, it includes 30 properties, just two of which are known: transaction amount and time. See Table III for a summary of the dataset.

TABLE III. Summary of the Dataset Obtained from Kaggle

Total dataset	#fraud	#Not fraud	Label not fraud	Label fraud
284807	492	284315	0	1

B. *Results Analysis*

As a baseline, the experimental results compare the classical simple federated model on non-IID dataset with different number of clients as shown in Table IV.

TABLE IV. The Results for the FL_Model When Dealing with Non-IID Data Across Different Client Configurations

Framework	**TensorFlow Federated**					
	FL_Model					
# of Clients	**Accuracy**	**Precision**	**Recall**	**F1-score**	**Loss**	**Time**
2	93.91	91.66	96.61	94.06	0.2602	294
3	93.53	94.17	92.79	93.47	0.2639	268
5	95.49	94.14	95.88	95.50	0.1548	251
10	95.01	98.14	91.77	94.84	0.2641	272

These measurements offer insight into the FL_Model's performance across various client settings. Notably, as the number of clients grows, accuracy stays high, illustrating the efficacy of the federated learning approach. Keep in mind that modest differences in performance measures are to be expected given the FL model's dispersed nature and privacy-preserving mechanisms.

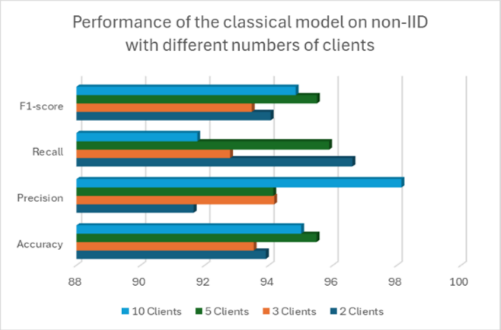

Fig. 1. The Performance parameters of the Classical Model on non-IID with different numbers of clients

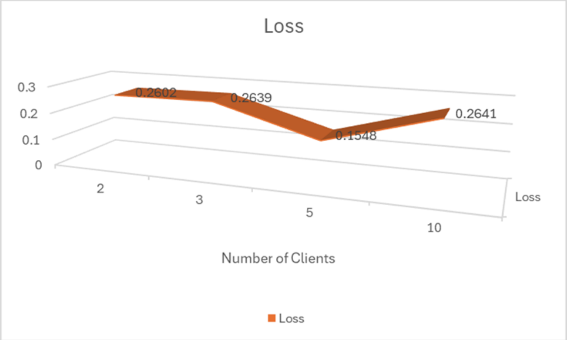

Fig. 2. The Loss values of the Classical Model different numbers of Clients

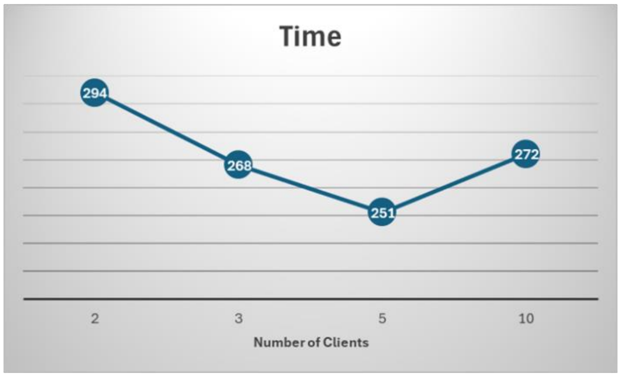

Fig. 3. The Computation Time of the Classical Model different numbers of Clients

As per the graphical representation of these boxplots, shown in Fig. 1 to Fig. 3, the classical federated learning model in combination with different number of clients. For each number of clients, the performance of all cases is presented.

The optimized federated model is compared with the typical simple federated model [20] in the experimental results as a baseline. Table V displays the findings of the experiment. It is evident that any federated model that has been tuned outperforms the basic model in terms of performance. Performance indicators such as accuracy, precision, recall, F score, and loss ratio are the main tools used to assess the efficacy of the suggested model.

TABLE V. COMPARISON RESULTS OF OPTIMIZED FEDERATED LEARNING MODELS WITH THE PREVIOUS WORK [20]

Performance Parameters	Previous Work	Optimized FL Models (Proposed Works)		
	FL Model [20]	GTO_FL	AGTO_Fl	CoatiOA_FL
Accuracy	91.88	95.79	96.83	96.85
Precision	0.8965	0.9379	0.9615	0.9631
Recall	0.9476	0.9807	0.9756	0.9744
F1_Score	0.9213	0.9588	0.9684	0.9687
Loss	0.2804	0.2221	0.2120	0.21088
OP_Time	-	2153	673	721
FL_Time	415	360	303	326

These metrics provide insights into the performance of each model. The AGTO_FL and CoatiOA_FL models exhibit higher accuracy, precision, recall, and F1 scores compared to the baseline FL Model. Additionally, they achieve lower loss values. The optimization strategies employed in AGTO_FL and CoatiOA_FL seem effective in enhancing fraud detection.

In terms of model performance, the AGTO_FL and CoatiOA_FL models outperform the baseline FL Model in terms of accuracy, precision, recall, and F1 score. Both AGTO_FL and CoatiOA_FL achieve higher accuracy (96.83% and 96.85%, respectively) compared to the baseline (91.88%). Precision is significantly improved in AGTO_FL (96.15%) and CoatiOA_FL (96.31%) compared to the baseline (89.65%). Recall values for both advanced models are also impressive (97.56% and 97.44%) compared to the baseline (94.76%). The F1 score, which balances precision and recall, is notably higher in AGTO_FL (96.84%) and CoatiOA_FL (96.87%) than in the baseline (92.13%).

Regarding Loss Minimization, the loss function is crucial for model optimization. Both AGTO_FL and CoatiOA_FL achieve lower loss values (0.2120 and 0.21088, respectively) compared to the baseline (0.2804). This reduction in loss indicates better convergence and improved model performance.

From Computational Efficiency, the optimization strategies employed in AGTO_FL and CoatiOA_FL led to faster convergence. AGTO_FL takes 303 seconds, while CoatiOA_FL takes 326 seconds for federated learning, outperforming the baseline (415 seconds).

V. CONCLUSION

This study was conducted on a non-IID dataset with a large number of clients. This limitation may impact the generalizability of the findings to other scenarios. This paper proposes an optimized federated learning model that employs the most recent metaheuristic CCFD algorithms to detect patterns of fraudulent credit card transactions (GTO, AGTO, COA). The optimization tactics used in AGTO_FL and CoatiOA_FL appear to be effective at improving fraud detection. While the proposed federated learning model employs recent metaheuristic algorithms (GTO, AGTO, COA), it's essential to recognize that these algorithms have their own limitations. In the future, enhancing privacy protection mechanisms within the federated learning model is crucial. Incorporating better gradient privacy techniques can safeguard sensitive data during training. will be optimized by including better gradient privacy protection, and additional comparison analysis and reliability checks against earlier research are advised for a thorough evaluation. Future research should conduct thorough comparison analyses against earlier studies. Additionally, reliability checks such as robustness testing and sensitivity analysis will provide a more comprehensive evaluation of the proposed model.

REFERENCES

[1] Statista, “Visa credit cards in circulation 2023,” Statista, 2023. [Online]. Available: https:// www. stati sta. com/ stati stics/ 618115/ number- of-visa- creditcards-world wide- by- region/. [Accessed 24 Aug 2023].

[2] Statista, “Mastercard: credit cards in circulation 2023,” Statista, 2023. [Online]. Available: https:// www. stati sta. com/ stati stics/ 618137/ number- of- mastercard- credit- cards- world wide- by- region/. [Accessed 24 Aug 2023].

[3] Nilson Report, “Card Fraud Losses (2022),” [Online]. Available: https://nilsonreport.com/mention/1750/1link/. [Accessed 24 Aug 2023].

[4] S. Makki et al., “An experimental study with imbalanced classification approaches for credit card fraud detection,” IEEE Access, vol. 7, pp. 93010-93022, 2019, doi:10.1109/ACCESS.2019.2927899

[5] I. H. Sarker, “AI-driven cybersecurity: an overview, security intelligence modeling and research directions,” SN Computer Science, vol. 2, no. 1, 2021, doi:10.1007/s42979-020-00417-4.

[6] P. Kairouz et al., “Advances and open problems in federated learning,” Foundations and Trends® in Machine Learning, vol. 14, no. 1–2, pp. 1-210, 2021, doi:10.1561/2200000093.

[7] A. Nilsson et al., “A performance evaluation of federated learning algorithms,” in Proceedings of the Second Workshop on Distributed Infrastructures for Deep Learning, 2018, pp. 1-8.

[8] El Hlouli, F. Z., Riffi, J., Mahraz, M. A., Yahyaouy, A., El Fazazy, K., & Tairi, H. (2024). Credit Card Fraud Detection: Addressing Imbalanced Datasets with a Multi-phase Approach. SN Computer Science, 5(1), 173.

[9] Husejinović, A., Kevrić, J., Durmić, N., & Jukić, S. (2023, June). Credit Card Fraud Payments Detection Using Machine Learning Classifiers on Imbalanced Data Set Optimized by Feature Selection. In International Symposium on Innovative and Interdisciplinary Applications of Advanced Technologies (pp. 233-250). Cham: Springer Nature Switzerland.

[10] Sudarshana, K., MylaraReddy, C., & Adhoni, Z. A. (2022). Classification of Credit Card Frauds Using Autoencoded Features. In Intelligent Computing and Applications: Proceedings of ICDIC 2020 (pp. 9-17). Singapore: Springer Nature Singapore.

[11] H. Yuan, “On principled local optimization methods for federated learning,” Ph.D. dissertation, Stanford University, 2022.

[12] J. Konecny, H. B. McMahan, F. X. Yu, P. Richtarik, A. T. Suresh, and D. Bacon, “Federated learning: Strategies for improving communication efficiency,” NIPS Workshop on Private Multi-Party Machine Learning, 2016.

[13] Jansson, M., & Axelsson, M. (2020). Federated learning used to detect credit card fraud. LU-CS-EX.

[14] Zheng, W., Yan, L., Gou, C., & Wang, F. Y. (2021, January). Federated meta-learning for fraudulent credit card detection. In Proceedings of the Twenty-Ninth International Conference on International Joint Conferences on Artificial Intelligence (pp. 4654-4660).

[15] Askari, Q., Saeed, M., & Younas, I. (2020). Heap-based optimizer inspired by corporate rank hierarchy for global optimization. Expert Systems with Applications, 161, 113702.

[16] Sadeeq, H. T., & Abdulazeez, A. M. (2022). Giant trevally optimizer (GTO): A novel metaheuristic algorithm for global optimization and challenging engineering problems. IEEE Access, 10, 121615-121640.

[17] Mostafa, R. R., Gaheen, M. A., Abd ElAziz, M., Al-Betar, M. A., & Ewees, A. A. (2023). An improved gorilla troops optimizer for global optimization problems and feature selection. Knowledge-Based Systems, 269, 110462.

[18] Dehghani, M., Montazeri, Z., Trojovská, E., & Trojovský, P. (2023). Coati Optimization Algorithm: A new bio-inspired metaheuristic algorithm for solving optimization problems. Knowledge-Based Systems, 259, 110011.

[19] Machine Learning Group – ULB, “Credit card fraud detection: Anonymized credit card transactions labeled as fraudulent or genuine,” 2018. [Online]. Available: https://www.kaggle.com/mlg-ulb/creditcardfraud. [Accessed 24 Aug 2023].

[20] Abdul Salam, M., Fouad, K.M., Elbably, D.L., and Salah M. Elsayed. Federated learning model for credit card fraud detection with data balancing techniques. Neural Comput & Applic (2024). https://doi.org/10.1007/s00521-023-09410-2.