Journal of Adaptive Learning Technologies
ISSN **2997-3902** (Online)
Vol. 3, No. 3, Mar 2026,
Available online at: https://scientificbulletin.com/index.php/JALT

Article

Optimization-Based Machine Learning Models for Credit Card Fraud Detection: A Systematic Review with Emphasis on Cuckoo Optimization Algorithm

Ban Hamed Al-miyahi[1], Sarah Hassan Awad Al-taee[2], Melad Jameel Hamoud[3]
1General Directorate of Education, Baghdad, Al-Rusafa First, Department of Preparation and Training, Iraq
ban8kut3@gmail.com
2Ministry of Education, Wasit Education Directorate, Iraq
sawad@uowasit.edu.iq
3Wasit University, Department of Computer Science, Iraq
mieladjameel@uowasi.edu.iq
Article information:
Manuscript received: 30 January 2026; **Accepted:** 05 February 2026; **Published:** 28 March 2026

Abstract: Detection of credit card fraud has become a major concern in the contemporary financial structures with the fast development of online payment systems and electronic transactions. Conventional methods of fraud detection are not usually very accurate in case of the large scale datasets that are highly unbalanced. Optimization algorithms have recently gained popularity to be used together with machine learning models to enhance detection performance, feature selection, and classification accuracy. The paper has carried out a methodical review of optimization-based methods in credit card fraud detection systems with particular consideration of Cuckoo Optimization Algorithm (COA). The general search of the literature was carried out in the key scientific databases such as Scopus, IEEE Xplore, ScienceDirect, etc.

Keywords: Credit Card Fraud Detection, Optimization Algorithms, Machine Learning Models, Cuckoo Optimization Algorithm (COA), Feature Selection

1. Introduction

Background of Credit Card Fraud Detection

Development of e-commerce has created credit card transactions and credit card fraud. It is a type of fraud that utilizes card information unauthorized to commit acquisitions or withdrawals at the detriment of consumers and banking institutions as well as compromising trust in payment systems. According to [1], criminals of fraud are ever improving their methods to identify newer vulnerabilities.

Conventional methods of fraud detection are based on statistical method and rule-based detection. These techniques are not always effective with multifaceted patterns of transactions. According to [2], scaling and adaptation are challenging due to the fact that fixed rules may not detect new threats.

To solve this, it is now possible to use machine learning techniques to analyze large volumes of transaction data in real time. According to [3], the models assist in isolating legitimate transactions and suspicious transactions.

With the development of fraud detection, optimization algorithms and machine learning are more effective at detecting fraud and addressing such problems as imbalances in the training set.

Importance of Optimization in Fraud Detection

Optimization makes a big difference in machine learning models for credit card fraud detection As fraud techniques evolve, fraud detection systems have to evolve rapidly to

keep pace with the changes and minimize the false positives. The detection tools can be used on high-dimensional and complicated data by using optimization algorithms that update model parameters at a rapid rate. Rule-based systems sleepwalk traditional rule-based systems wake lag: as rules have to be updated constantly, they are not always scalable. These advanced optimization algorithms in a machine learning environment make it flexible and reduce manual optimization. They reduce the processing power even further since the Particle Swamp Optimization and the Cuckoo Optimization Algorithm (COA) enable the financial institutions [5] to reap the rewards of utilization of the resources. In general, not only can we sharpen the fraud detection with the aid of a powerful optimization, but also we can create a more confident environment towards consumers and stakeholders.

Overview of Machine Learning Techniques in Fraud Detection

Machine learning has transformed credit card fraud detection to learn intricate patterns through transaction data. Such supervised algorithms as Support Vector Machines (SVM), Random Forest (RF), and ensemble methods can be used to make a distinction between fraudulent and legitimate transactions. Anomalies in unlabeled data are commonly identified by using unsupervised and semi-supervised methods, such as autoencoders. Long Short-Term Memory (LSTM) networks, deep learning architectures, learn time-dependent relationships, whereas Convolutional Neural Networks (CNNs) and Graph Neural Networks (GNNs) learn spatial and relational characteristics. To enhance the accuracy and resilience to the changing fraud patterns, hybrid models that combine various techniques are becoming more popular [3], [5], [6].

2. Methodology

This systematic review is conducted in line with the principles of undertaking systematic literature reviews in software engineering [19]. The content of the major scientific databases, i.e., Scopus, IEEE Xplore, ScienceDirect, SpringerLink, and Google Scholar was searched systematically. The search query was formulated based on the combination of terms to do with credit card fraud (credit card fraud, fraud detection, financial fraud) with optimization algorithms (cuckoo optimization, COA, particle swarm optimization, genetic algorithm, grey wolf optimizer, ant colony optimization, differential evolution) and machine learning (machine learning, deep learning, SVM, neural network). Articles published in English between 2015 and 2026 were included. We removed duplicates, screened titles and abstracts, and examined full texts of potentially relevant studies. We included studies that proposed or evaluated an optimization based machine learning model for credit card fraud detection. Data extracted from each study included optimization algorithm, machine learning classifier, dataset, performance metrics and key findings. Narrative and tabular summaries of the extracted information were used to highlight trends and comparative performance.

Literature Review

ML has brought significant changes in the credit card fraud detection, and it gives better results than the traditional rules based methods which are described in 2.1. Such traditional systems are outdated very quickly, as machine learning models adapt to the most recent fraudulent behaviour and anomalies. This is necessary, as the fraud situation is constantly evolving, in order to be detected at an earlier stage.

So methods like Support Vector Machines (SVM) can be used to classify fraud from high dimensional data. Since they are based on decision trees, Random Forests are considered more trustworthy, as they limit the overfitting. Long Short-Term Memory (LSTM) networks have been used to recognize temporal dependencies in a sequence of transactions, which is important as fraudulent activities evolve over time.

Convolutional neural networks (CNNs) and graph neural networks (GNNs) as hybrid models can successfully capture the intricate relationships of the structured and unstructured data, which are usually missed by the traditional methods. Furthermore, an optimization algorithm can also optimize model parameters and reduce the size of the feature space, increasing precision and recall as seen in Section 6.2. See references [1], [2] and [5].

Traditional Fraud Detection Methods

The conventional methods of fraud detection are primarily based on statistical and rule-based methods. Systems based on rules are dependent on pre-determined rules developed by specialists and directed at the detection of certain fraud activities such as inflated income or fabricated expense claims. These rules are effective in detecting well known fraud patterns, but in most cases they are rigid and require regular modifications to match emerging fraud patterns. According to [6], this reliance on manual updates renders them less appropriate to the dynamic financial environment.

Statistical methods, in their turn, use regression and cluster analysis techniques to reveal abnormalities in past data. The methods are effective in identifying trends using historical trends but tend to fail in situations where there is a complicated transactional data with non-linear associations and numerous variables [6]. Besides, they are more dependent on historical data and this can lead to failure in detecting new fraud schemes that do not correspond to the old trends through the use of statistical approaches. As a result, the rule-based and the statistical methods are not able to keep up with the increased complexity of credit card fraud.

Limitations of Traditional Methods

The traditional fraud detection techniques such as rule-based and statistical systems have significant defenses against the contemporary credit card fraud. Rule based systems are based on set rules which are easily overtaken by the fraudsters who adapt to new tricks. This will have to be done manually and this has the risk of missing threats and time wasted [6]. They find it hard to scale as fraud trends change as well. Statistical techniques suppose that the data should be of linear or normal distribution, whereas the financial operations are complicated and non-uniform. Such models are very reliant on historical data, and they do not work with fresh cases of fraud that do not follow the same pattern as in the past [7]. Besides, they also require substantial resources to work with large datasets. Due to these limitations, conventional methods fail to respond and identify the changing fraud. All in all, they lag behind in dealing with the continuously increasingly sophisticated fraud.

Introduction to Optimization Algorithms

Optimization algorithms are important in enhancing credit card detection of fraud by optimizing the model parameters and features. Conventional approaches have issues with multi-dimensional and multi-dimensional datasets and optimization algorithms are required. These algorithms apply mathematical techniques to search large sets of solutions, and trade off exploration of promising solutions with exploitation of new ones.

Particle Swamp Optimization, Genetic Algorithms, and the Cuckoo Optimization Algorithm (COA) which are bio-inspired have been useful in solving complex searches. As discussed in section 4.1, they enhance model accuracy and solve other problems such as class imbalance and identifying significant features.

In section 3.2, the authors point out the importance of feature selection in narrowing down model inputs, which enhances ease of computation and increases transparency. More recent developments encompass hybrid solutions that involve both optimization and deep learning that can offer greater capabilities to fight developing frauds in financial institutions. See references [3], [4], and [6].

3. Results and Discussion

Machine Learning Models for Fraud Detection

Overview of Popular Machine Learning Models

Machine learning identifies credit card frauds through the analysis and classification of transactions. Support Vector Machines (SVM) are also well able to process high dimensional data and divide fraudulent and legitimate transactions with a hyperplane which is best. Random Forest (RF) enhances the accuracy through numerous decision tree building and minimizing overfitting. Long Short-term memory (LSTM) networks perform well when it comes to identifying patterns of time in transaction streams. LSTM is capable of winning over other models such as RF when it comes to offline transactions with [2] observing that. Similar approaches, which are hybrid models of Convolutional Neural Network (CNN) and Graph Neural Network (GNN), also aim at retrieving spatial attributes and processing

relational data of fraud detection. Advanced techniques combine deep learning and quantum optimization to make training quicker and more efficient. This integration is promising in integrating classical machine learning with new computational technologies that could be used in solving financial fraud problems. See also [3], [6], and [8]

Role of Feature Selection in Model Performance

Selecting the appropriate characteristics is critical towards enhancing machine learning models to identify credit card frauds. The choice of key variables has a huge influence on the accuracy of the model and it avoids issues such as overfitting and expensive computation as observed in [4]. The ability to highlight critical characteristics eases the modeling, reduces the training duration, and boosts interpretability.

The aspect of class imbalance that feature selection tackles is the fact that there are few instances of fraud. Other methods such as SMOTE can be used to balance the proportion of classes, which decreases bias and gives fraud characteristics a higher chance of being identified by the model, as explained by [6].

Optimization algorithms are also used to enhance additional feature selection, which enhances the accuracy of classification. Bio-inspired techniques effectively identify meaningful feature subsets and do not fall into the same pitfalls as overfitting as outlined in [3], and leave models reliable and useful.

Optimization Algorithms Used in Credit Card Fraud Detection

Commonly Used Optimization Algorithms

Optimization algorithms play a significant role in enhancing machine learning models to detect credit card fraud. The methods have gained popularity due to their ability to address such issues as high dimensionality and imbalanced classes in data. Particle Swarm Optimization (PSO), Genetic Algorithms (GA), and the Ant Colony Optimization (ACO) are common algorithms used. PSO is naturally motivated hence navigates the space of solutions with ease, and this will go a long way in the selection of features to be used in fraud models.

Genetic Algorithms are the use of the principle of natural selection and genetics to find the optimal subsets of features by competing with a large number of solutions simultaneously. They are particularly useful when working with complicated datasets that can be derailed by standard methods. Ant Colony Optimization is inspired to emulate the foraging behavior of the ants so as to determine optimal paths and is useful in some routing problems in data.

In addition, a combination of different metaheuristic approaches which are known as hybrid has proved to be a powerful force in enhancing the accuracy of fraud detection. Indicatively, a combination of PSO and other algorithms may result in significant enhancement of the classification results as indicated in [7]. These optimization methods are useful not only in refining the feature selection process, but also in making the model more resistant to fraud.

For further insights, see [8].

Genetic Algorithm in Fraud Detection

One of the oldest optimization approaches in the system that is used to detect fraud is the Genetic Algorithm (GA). GA follows the natural evolutionary and selection processes where the candidate solutions are enhanced by the crossover and mutation processes.

Scholars have applied GA to the selection of features and optimization of parameters of machine learning models. It was observed that, GA with Support Vector machine and random forest gave high accuracy in detecting credit card frauds [9].

GA can be used to search large solution spaces, and it can be more computationally intensive than other optimization algorithms.

Particle Swarm Optimization in Fraud Detection

Particle swarm optimization (PSO) is a swarm intelligence algorithm based on the motion of birds and fish. PSO is popularly used for the optimization of neural network and SVM parameters.

Multiple studies claimed that the PSO-based models are much more accurate and fast-convergent than the conventional machine learning approaches. PSO has been applied to detect fraud successfully by enhancing the performance of classification and false positive minimization [10].

Nevertheless, PSO can occasionally coincide to local optimum in case the data set is highly intricate.

Ant Colony Optimization and Grey Wolf Optimizer

Fraud detection has been implemented using ACO to create rules and select features. The ACO based models prove to be helpful in classification problems whereby the best possible rules need to be derived out of the transaction data [11].

Grey Wolf Optimizer (GWO) is a comparatively new optimization algorithm, where the wolves are simulated to hunt. GWO has demonstrated good performance in the machine learning applications, such as fraud detection. Researchers have found that GWO in combination with Random Forest and Neural Networks was highly accurate in credit card fraud datasets [12].

Another optimization technique that has been applied to enhance neural network training is the Differential Evolution (DE). DE is good in continuous optimization and has been used in fraud detection to help optimize the parameters of classifiers [13].

Cuckoo Optimization Algorithm in Fraud Detection

The Cuckoo Optimization Algorithm (COA) has recently been in the limelight as it has a good global search capacity and can escape local minima. COA has also been applied in machine learning models in feature selection and parameter tuning.

A number of studies have indicated that COA-based models were more accurate than GA and PSO in certain problems of fraud detection. COA is also effective when the dataset is large in terms of features and needs the best selection to enhance the performance of classification [14].

The new models of combining COA and neural networks, as well as support vectors machine, have already demonstrated promising outcomes in more recent studies.

Summary of Previous Studies

Table 1 presents a summary of selected studies that used optimization algorithms in credit card fraud detection systems.

Table 1. Optimization algorithms used in fraud detection

Reference	Algorithm(s)	Model / Approach	Dataset / Context	Performance / Notes
Ileberi et al. (2022)	Genetic Algorithm (GA)	ML with GA for Feature Selection	European Credit Card Dataset	Improved detection performance with optimized features
AL-Hammadi (2025)	GA + PSO	SVM with optimization	Credit Card Fraud Dataset	Achieved ≈ 99.99% accuracy using GA + PSO for feature selection and tuning
Sree et al. (2023)	Particle Swarm Optimization (PSO)	PSO-optimized Neural Network	Credit Card Fraud Dataset	PSO improved training performance compared to baseline models
PSO-SVM Hybrid (2024)	PSO	SVM optimized with PSO	European Kaggle Dataset	Improved classification through hyperparameter optimization
PSO-ACO Based ANN (2025)	PSO + ACO	ANN with hybrid optimization	Experimental Credit Card Dataset	Hybrid PSO-ACO outperformed conventional ANN models
CCFD Meta-Heuristics (2024)	PSO, GWO, ABC, SSA	RF & SVM with metaheuristic optimization	Credit Card Fraud Detection tasks	Ensemble metaheuristics improved feature selection and

Reference	Algorithm(s)	Model / Approach	Dataset / Context	Performance / Notes
				classification
Example Hybrid (Review Studies)	GA + PSO + CS	Hybrid optimized ML models	General fraud detection contexts	Hybrid optimization consistently yields higher detection performance

Table 1 is a summary of the recent articles that incorporate optimization algorithms into credit card fraud detection systems. The results suggest that metaheuristic algorithms GA, PSO, and hybrid (e.g. PSO-ACO and GA-PSO) substantially improve the performance of the models. The hybrid optimization methods are always superior to single algorithm models, especially in feature selection and hyperparameter optimization. It is worth pointing out that GA+PSO-based systems provided almost perfect accuracy, which demonstrates the efficiency of integrating various optimization approaches. Moreover, the ensemble metaheuristic models have a good potential of enhancing the robustness and generalization of the fraud detection tasks.

Specific Focus on Cuckoo Optimization Algorithm (COA)

Cuckoo Optimization Algorithm (COA) is based on the behavior of cuckoos that deposit eggs in the places of other bird nests. It maintains a list of candidate solutions, or nests, and searches and exploits the search space completely. COA is used in credit card fraud classification to fine-tune machine learning models to boost accuracy and recall. Research demonstrates that the use of COA in conjunction with classifiers such as Support Vector Machines and the k-Nearest Neighbors is more accurate and less feature based (see section 5.1). The feature selection in COA also does a great job in eliminating irrelevant features and preserving those that are important in detecting fraud as indicated in section 3.2. It has a strong side of striking a balance between exploration and exploitation. COA is also more likely to converge quicker and provide greater accuracy in fraud detection than other techniques such as Particle Swarm Optimization and Genetic Algorithms (see section 5.2). Therefore, COA is an encouraging opportunity in improving credit card fraud detection systems. See references [15] and [16].

Application Scenarios for COA in Fraud Detection Systems

Case Studies Utilizing COA

The Cuckoo Optimization Algorithm (COA) has been used extensively in credit card fraud detection since it enhances the performance of a model by improving the ability to select smart features and refine them. One such application was the use of machine learning classifiers on the Australian credit dataset using COA which was significantly superior to the traditional algorithms. The study increased classification accuracy by 3.83, 10.71 and 11.21 percent using COA with classifiers such as Support Vector Machine (SVM), k-Nearest Neighbor (k-NN) and Xgboost compared to the baseline models. Meanwhile, the feature dimensionality reduced by COA was 53.07, 62.85, and 67.14 and simplified the models without affecting their performance.

In a different study, scholars combined COA with deep learning models to improve the neural networks in fraud detection. This integration was able to optimize the weight parameters across the neural networks, resulting into increased efficiency and reduced false positive in the case of fraud detection..These are examples of how COA can be applied in various ways to improve the accuracy of fraud detection and control the number of computations. See references [3], [4], and [15].

Comparative Analysis with Other Optimization Techniques

A comparison of the Cuckoo Optimization Algorithm (COA) with various other methods of optimizations for credit card fraud detection gives rise to several interesting methods. Indicatively, the Firefly Optimization Algoritm (FOA) with the Support Vector Machines has high potential of enhancing the accuracy of the detection with the least false positives. It takes advantage of the flashing behavior of natural fireflies to obtain (near) optimal solutions more expeditiously as reports [3].

A new sport with Quantum Optimization Algorithms. They rely on the principles of quantum mechanics and allow exploring complex search spaces in a way that would be challenging to the traditional methods like gradient descent, see [6] and frequently result in local optima kompleksaran.

COA has sufficient convergence speed, the cardinality control on the feature subsets, though it can be outperformed by some hybrid methods with the combination of alternative optimization scheme. As an example, the Brown Bear Optimization algorithm has enhanced the classification by making better choices of features compared to COA such as in [4]. These observations may suggest that a combination of various optimization techniques remains a promising road to further development of the systems of fraud detection.

Performance Evaluation Metrics for Fraud Detection Models

Key Metrics Used in Assessing Model Effectiveness

There are varied measures that are required to comprehend the performances of the credit card fraud detection models fully when comparing them.

We tend to seek accuracy on the one hand to find out the number of the predictions that were correct. It is however problematic especially in fraud detection when the data is usually unbalanced that is, there are many more legitimate transactions as compared to fraudulent ones.

The following are some other metrics that you need to take into consideration in your evaluations:

Precision (or Positive Predictive Value) informs us of many of the transactions that are claimed to be fraudulent are in fact fraudulent. This enables us to observe the degree of reliability of the model as it screams fraud.

Recall (also known as True Positive Rate or sensitivity) is a percentage of real fraudulent transactions that the model identifies. High recall implies that the model is effective in detecting fraud.

F1-score is a harmonic average of precision and recall and it gives a fairer picture which may be invaluable especially on imbalanced data sets.

Specificity = TN/(TN+FP) informs us of the quality of the model to identify non-fraud cases correctly and provides an approximate information on how the model performs on legitimate transaction. In addition, the Receiver Operating Characteristic (ROC) curve (see Section 4.2) and its area under the curve (AUC) gives an excellent graphical representation of the model performance in terms of the different values of the threshold, and gives a trade-off between sensitivity and specificity (or false positive rate).

Taken all together, these metrics will provide a very comprehensive view of the effectiveness of the fraud detection systems in question, in the sense that we can obtain a fair idea on which ones are the most well-balanced in terms of their strengths and weaknesses.. See [3], [5], and [6].

Impact of Optimization on Model Performance Metrics

Optimization algorithms have a significant impact on the main evaluation metrics of models for fraud detection. Optimization increases precision and recall by fine tuning hyperparameters and choosing informative features which leads to higher F1 scores even on highly imbalanced datasets. It has been shown that the neural network that has been optimized through PSO and hybrid systems of GA PSO provides accuracy nearly equal to perfect with decreasing false positive rate [9], [10]. COA based feature selection enhances the AUC ROC by further eliminating the irrelevant variables and concentrating the model on those patterns of fraud that discriminate [14]. In addition, optimization can minimize the time spent in training, the cost of computation and enables real time detection without compromising on reliability [5], [6]. Therefore, when optimization is included into the modeling piping, it results in stronger, efficient and robust fraud detection systems.

4. Results and Discussion

The systematic review indicates that optimization algorithms have emerged to be important in enhancing the performance of machine learning models in detecting credit card fraud. The existing challenges are high dimensionality, class imbalance and model tuning. These issues are addressed by bio-inspired algorithms as a form of GA, PSO, ACO, GWO

and COA. Table 1 results indicate that the hybrid methods (such as GA+PSO, PSO+ACO) are always better than the single-algorithm models with accuracy levels of up to 99.99% in certain studies.

The COA among the algorithms studied has a unique balance between exploration and exploitation, which leads to fast convergence and robust feature selection. In head-to-head comparisons, COA-optimized classifiers outperformed baseline models in terms of accuracy by up to 11% while reducing the feature set by more than 60% [4], [14]. COA provides a dual benefit of better accuracy and computational efficiency that makes it especially attractive for real-time fraud detection systems [20, 21].

The results also show that feature selection is the most important factor that affects the model performance. Optimization-driven feature selection not only prevents overfitting, but also helps in dealing with class imbalance by highlighting rare fraud indicators. The metaheuristic optimization, as explained in Section 7.2, enhances all the performance metrics such as precision, recall, F1-score and AUC-ROC.

These gains have certain limitations though. A large number of studies rely on a single benchmark dataset (e.g., European Card dataset) and might not be applicable to other transaction environments. The hybrid methods are too expensive to use in high throughput systems. Also, there is no standardized assessment procedure that could be used to compare studies. Explainable AI, federated learning to preserve privacy, and quantum-inspired incorporation of optimization should be a part of future work to enhance the detection ability.

5. Conclusion

Optimization is also a tool to be used for further enhancing credit card fraudulent detection models. This method can enhance the accuracy and efficiency. The application of bio-inspired algorithms, such as the Cuckoo Optimization Algorithm (COA), can enhance precision, recall, F1-score and AUC-ROC, which are key evaluation parameters for credit card fraud detection models. The application of COA in feature selection can discard less significant features and select more significant features, leading to enhancement in recall and precision as reviewed in section 3.2.. The use of COA can improve accuracy and reduce training time, as discussed in section 4.2, making it better than traditional algorithms.

The use of these optimization techniques can improve credit card fraud detection models, making them more suitable for a dynamic environment, as discussed in section 2.1. The use of different techniques for credit card fraud detection is discussed in section 5.2, which states that optimization can achieve a balance between accuracy and cost, making it suitable for credit card fraud detection models. More information can be found in [3], [5], and [18].

Summary of Findings from Systematic Review

However, conventional methods, such as rule-based systems and statistical methods, fail to adapt and become efficient in fighting evolving patterns of fraud, particularly for large datasets (sections 2.1 and 2.2). This is where machine learning algorithms, including SVM and LSTMs, come in, which effectively handle temporal patterns (section 3.1). Optimization algorithms also improve the models, including SVM and LSTMs, by fine-tuning them and enhancing feature selection (section 4.1). Among the optimization algorithms, the Cuckoo Optimization Algorithm (COA) is noteworthy for its effectiveness in enhancing accuracy and reducing data dimensionality for classifiers (sections 4.2 and 5.1). In particular, COA has shown superior performance compared to traditional optimization algorithms, such as the Particle Swarm Optimization, in terms of speed and efficiency, as demonstrated in case studies. Metrics such as precision, recall, and F1-score are used for evaluating the success of models (section 6.1), and optimization algorithms help handle class imbalance, which is common in fraud detection (section 6.2). In general, this ensemble of models enhances detection of fraud and eventually minimizes financial losses. See [3], [6], [7], [17], and [18].

Recommendations for Future Research in Credit Card Fraud Detection Systems Using COA

Credit card fraud detection through the use of Cuckoo Optimization Algorithm (COA) has a few areas in which the research area could be enhanced. One of them is enhancing COA with machine learning (and in particular with deep learning), which is discussed in [7]. The other is dealing with the traditional system problems, e.g. how COA can cope with new types of fraud. The other area is augmenting transparency particularly through explainable AI. One more is the growing data privacy, particularly federated learning or differential privacy. The other area is to expand the use of COA particularly to other areas as discussed in [4]. The other field is the expansion of the use of quantum computing, particularly to process complicated data. Each of these fields has the ability to enhance the force of COA in detecting credit card frauds.

REFERENCES

[1]. C. Li, N. Ding, Y. Zhai, and H. Dong, "Comparative study on credit card fraud detection based on different support vector machines," Intelligent Data Analysis, vol. 25, no. 1, pp. 105–119, Jan. 2021, doi: 10.3233/ida-195011.

[2]. J. Jurgovsky et al., "Sequence classification for credit-card fraud detection," Expert Systems With Applications, vol. 100, pp. 234–245, Jan. 2018, doi: 10.1016/j.eswa.2018.01.037.

[3]. A. Singh, A. Jain, and S. E. Biable, "Financial Fraud Detection Approach based on Firefly optimization algorithm and support Vector machine," Applied Computational Intelligence and Soft Computing, vol. 2022, pp. 1–10, Jun. 2022, doi: 10.1155/2022/1468015.

[4]. S. E. Sorour, K. M. AlBarrak, A. A. Abohany, and A. a. A. El-Mageed, "Credit card fraud detection using the brown bear optimization algorithm," Alexandria Engineering Journal, vol. 104, pp. 171–192, Jun. 2024, doi: 10.1016/j.aej.2024.06.040.

[5]. A. A. Compagnino et al., "An introduction to machine learning methods for fraud Detection," Applied Sciences, vol. 15, no. 21, p. 11787, Nov. 2025, doi: 10.3390/app152111787.

[6]. 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, doi: 10.1007/s42452-025-06999-y.

[7]. X. Qiu, W. Qin, C. Guo, and W. Mao, "Credit Card Fraud Detection Algorithm Based on Improved Particle Swarm Optimization," IEEE Xplore, pp. 380–385, Apr. 2024, doi: 10.1109/icsp62122.2024.10743499.

[8]. N. S. A. Mohammed, M. S. Saraya, A. M. Thabet, and L. M. Labib, "Credit card fraud detection using metaheuristic techniques," MEJ Mansoura Engineering Journal, vol. 51, no. 1, Jan. 2026, doi: 10.58491/2735-4202.3354.

[9]. S. Kumar, V. K. Gunjan, M. D. Ansari, and R. Pathak, "Credit card fraud detection using support vector machine," in Lecture notes in networks and systems, 2022, pp. 27–37. doi: 10.1007/978-981-16-6407-6_3.

[10]. M. Dashora, P. Sharma, and A. Bhargava, "Credit Card Fraud Detection using PSO Optimized Neural Network," International Journal of Engineering and Advanced Technology, vol. 9, no. 4, pp. 360–363, Apr. 2020, doi: 10.35940/ijeat.d6484.049420.

[11]. S. K. M. Hossain, S. A. Ema, and H. Sohn, "Rule-Based Classification Based on Ant Colony Optimization: A Comprehensive Review," Applied Computational Intelligence and Soft Computing, vol. 2022, pp. 1–17, Apr. 2022, doi: 10.1155/2022/2232000.

[12]. W. Puspita and M. F. A. Hakim, "Optimization of logistic regression algorithm using Grey Wolf Optimizer for credit card fraud detection," Scientific Journal of Informatics, vol. 12, no. 4, pp. 673–684, Dec. 2025, doi: 10.15294/sji.v12i4.26807.

[13]. M. Tayebi and S. E. Kafhali, "Credit card fraud detection based on hyperparameters optimization using the differential evolution," International Journal of Information Security and Privacy, vol. 16, no. 1, pp. 1–21, Nov. 2022, doi: 10.4018/ijisp.314156.

[14]. M. S. A. Yajid et al., "Hybrid Big Bang-Big crunch with cuckoo search for feature selection in credit card fraud detection," Scientific Reports, vol. 15, no. 1, p. 23925, Jul. 2025, doi: 10.1038/s41598-025-97149-2.

[15]. M. Twaij and A. Lakizadeh, "An enhanced intrusion detection system for wireless sensor networks using Cuckoo-Optimized neural networks," Iraqi Journal of Data Science., vol. 2, no. 2, pp. 32–43, Jun. 2025, doi: 10.51173/ijds.v2i2.30.

[16]. P. Mohapatra, S. Chakravarty, and P. K. Dash, "An improved cuckoo search based extreme learning machine for medical data classification," Swarm and Evolutionary Computation, vol. 24, pp. 25–49, Jun. 2015, doi: 10.1016/j.swevo.2015.05.003.

[17]. S. Saad, I. Nadher, and S. M. Hameed, "Credit Card Fraud Detection Challenges and Solutions: A review," Iraqi Journal of Science, pp. 2287–2303, Apr. 2024, doi: 10.24996/ijs.2024.65.4.42.

[18]. Sadgali, N. Sael, and F. Benabbou, "Fraud detection in credit card transaction using neural networks," Proceedings of the 4th International Conference on Smart City Applications, pp. 1–4, Oct. 2019, doi: 10.1145/3368756.3369082.

[19]. Kolaski, L. R. Logan, and J. P. A. Ioannidis, "Guidance to best tools and practices for systematic reviews," Systematic

Reviews, vol. 12, no. 1, p. 96, Jun. 2023, doi: 10.1186/s13643-023-02255-9.

[20]. X.-S. Yang and S. Deb, "Cuckoo Search via Lévy flights," IEEE Xplore, pp. 210–214, Jan. 2009, doi: 10.1109/nabic.2009.5393690.

[21]. A. Mniai, M. Tarik, and K. Jebari, "A novel framework for credit card fraud detection," IEEE Access, vol. 11, pp. 112776–112786, Jan. 2023, doi: 10.1109/access.2023.3323842.