Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Enhanced Approach for Credit Card Fraud Detection with Updated Grasshopper Algorithm and Deep Neural Network

Manu Jyoti Gupta* and Parveen Sehgal
Email: hellopapa2018@gmail.com, parveensehgal@gmail.com
Department of CSE, School of Engineering & Technology, Om sterling Global University, Hisar, India

ARTICLE INFO

Received: 10 Nov 2024

Revised: 18 Dec 2024

Accepted: 20 Jan 2025

ABSTRACT

Credit card fraud detection is one of the most important problems in the financial industry, and it requires powerful and efficient ways to detect fraudulent transactions and safeguard customers. The proposed approach to fraud detection in this paper is new and based on the Grasshopper Optimization Algorithm (GOA) and Deep Neural Network (DNN). The two-stage proposed methodology includes feature selection by proposed GOA, GA, and PSO to achieve the best feature set and training and using a DNN for classifying transactions. Experimental results show that Grasshopper + DNN outperforms other combinations as regards precision, recall, and F-measure with precision = 0.9322, recall = 0.92113, and F-measure = 0.92663194. These results show clear improvements in fraud detection at the cost of false positives and false negatives. The method simplifies the complexity and enhances the efficacy and effectiveness of fraud detection systems and is thus a useful tool for financial institutions. Directions for future studies include incorporating other advanced optimization methods and machine learning models in an effort to enhance the detection capability.

Keywords: Credit Card Fraud Detection, Grasshopper Optimization Algorithm, Deep Neural Network, Feature Selection, Genetic Algorithm, Particle Swarm Optimization, Machine Learning, Financial Security.

1. INTRODUCTION

Credit card fraud prevention is a part of financial security, which aims to identify and prevent unwanted transactions using credit card information or stolen cards. With the volume of transactions so high in digital transactions, coupled with the intellectual prowess of counterfeiters, the correct and timely application of sophisticated methodology for fraud detection becomes even more imperative. One such advanced method involves the application of swarm intelligence to attribute selection. Swarm intelligence, drawing on the collective behavior of social insects such as ants, bees, and birds, can be extremely helpful to achieve significant optimisation in the effectiveness of fraud detection models through the optimisation of the selection of optimal features to distinguish between valid and invalid transactions. With the advantage of swarm-based algorithms, predictive models can become more effective and efficient, hence providing a stronger shield against credit card fraud. Credit card fraud detection begins with the cautious collection of information, such as transaction information, e.g., amount, location, merchant, and transaction time. It also gathers broad cardholder data, including spending habits and history of previous transactions, to identify potential patterns and anomalies indicative of fraud. The first step in information gathering establishes the foundation for the subsequent fraud detection steps. Following data gathering, the data undergoes rigorous pre-processing. Data cleaning is applied to address missing values, resolve inconsistencies, and remove outliers that may skew the result. Feature engineering is subsequently done to create new features from the raw data such as the frequency of transactions, average values of transactions, and inter-transaction times. These engineered features provide deeper knowledge about the cardholder's behavior. Data normalization is then performed, rescaling the numeric features into a uniform distribution throughout the data, which is required to improve the performance and accuracy of the machine learning models. Feature selection is a crucial step that has a direct influence on the performance of the fraud detection model. Swarm intelligence techniques such as Particle Swarm Optimization (PSO) and the Grasshopper Optimization Algorithm (GOA) are utilized in order to improve this process. PSO replicates the

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

motion of particles within a swarm such that each particle represents a candidate solution, altering its position based on its experience and the experiences of neighboring particles to converge toward the optimal solution. GOA mimics grasshopper nature such that the movement of the grasshoppers in the optimizing space is simulated based on attraction to food as well as to social interaction. This algorithm is particularly effective for global optimization problems, and therefore it is suitable for determining the most significant features that are able to best distinguish between valid and invalid transactions.

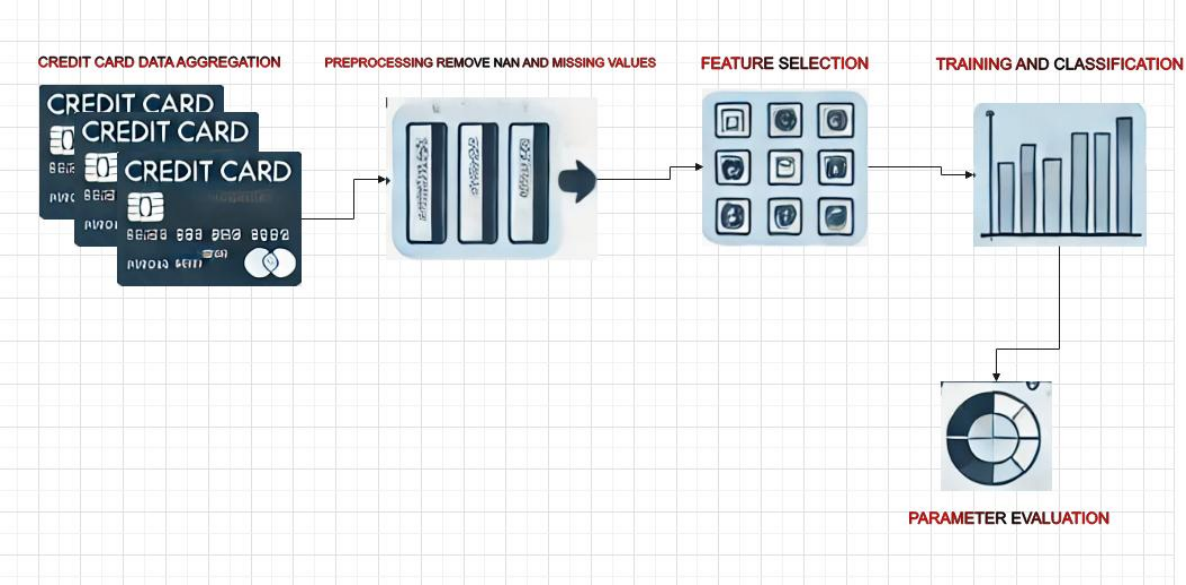

Figure 1: Process of data card classification

With the features selected, various machine learning algorithms are built in order to detect fraudulent transactions. Supervised algorithms like Logistic Regression, Decision Trees, Random Forest, Support Vector Machines, and Neural Networks are trained on datasets where transactions have been labeled as fraudulent or genuine. These models learn to pick up patterns pertaining to fraud through historical data. Where there is limited labeled data, unsupervised learning techniques such as clustering and outlier detection are used to identify patterns and outliers that can reflect fraud. The validation and training process is significant for assessing the performance of the fraud detection model. Through training, the model learns to differentiate between true and false transactions by learning patterns in the training data. Validation is achieved through cross-validation of model performance on accuracy, precision, recall, and F1-score on a held-out validation data set.

The procedure is there to ensure the model is fine and would be able to identify fraud transactions effectively.

After validation, the model is applied in carrying out real-time fraud detection. The new transaction is ranked as per the chances of it being fraudulent. Transactions above a fixed threshold value are marked for further investigation, raising alerts to the cardholder as well as to the bank. Immediate action such as blocking the card or performing a full investigation can then be taken to control potential fraud.

2. RELATED WORK

Zhu et al. (2024) present a new efficient and adaptive dandelion algorithm-based credit card fraud detection feature selection. The novelty in their work comes in the use of a dynamic feature selection method that evolves with time depending on the evolving nature of fraud. The approach is that of incorporating the dandelion algorithm with the application of standard machine learning classifiers for the purposes of improving the accuracy of detectionUsing this technique, they are able to obtain impressive gains in precision and recall scores, which are in keeping with the algorithm's performance under real-world useUtilization of this technique is also conducive to the adaptive and reactive nature of the fraud detection process, capable of being trained to identify patterns of fraud emerging as they become available[9]Gupta and Sehgal (2024) are also interested in optimizing the detection of credit card fraud as per the Grasshopper Optimization Algorithm (GOA)Their contribution is toward the improvement of classifier

Research Article

performance by selection of best features reducing dimensionality and computational time. The approach entails GOA hybridization with different classifiers, which results in a stable model that performs better than conventional ones. Their experiments reveal strikingly improved detection rates as well as reduced false alarms, indicating the potential of GOA in high-dimensional data feature selection[10].Alkhafaji et al.(2021) hybridize Neural Networks (NN) and the Grasshopper Optimization Algorithm (GOA) to detect credit card fraud. Their work has a hybrid model that integrates the strengths of both NN and GOA to find maximum detection accuracy. The architecture entails preprocessed data, feature selection through GOA, and classification through NN. The hybrid framework provides an enhanced and more efficient fraud detection framework than singular methodologies, which result in superior performance and dependability[11]. Abdulrauf Sharifai and Zainol (2020) handle biased and high-dimensional biomedical data with redundancy-based on correlation intensity and binary GOA to reduce features. Their work is in the guise of a feature selection method that effectively alleviates dimensionality reduction and addresses data imbalance, leading to improved classification performance. The method is to use the suggested method on choosing pertinent features prior to classification, with the purpose of showing its usability in biomedical data environments, which are often notoriously difficult due to the complexity and magnitude of data used[12]. Sorour et al. (2024) present the brown bear optimization algorithm for detecting credit card fraud. Contributions made include a novel optimization algorithm to enhance feature selection and detection accuracy of fraudulent transactions. The work is designed by merging the brown bear algorithm with machine learning classifiers in order to obtain a model showing high precision and recall in identifying fraud.The proposed method can be utilized to obtain more robust and powerful fraud detection systems[13].Priscilla and Prabha (2021) introduce a two-stage feature selection method based on mutual information and XGB-RFE (Extreme Gradient Boosting - Recursive Feature Elimination) for credit card fraud detection. Their article has a novel feature selection technique that improves detection efficiency and minimizes false positives. The strategy is to utilize mutual information for preliminary feature selection and XGB-RFE for further boosting and achieve a good detection model with enhanced ability to differentiate between fraud and authentic transactions[14]. Prabhakaran and Nedunchelian (2023) use the Oppositional Cat Swarm Optimization (OCSO) algorithm to perform credit card fraud feature selection. .Priscilla and Prabha (2021) propose two-stage feature selection approach using mutual information and XGB-RFE (Extreme Gradient Boosting - Recursive Feature Elimination) for the detection of credit card fraud. Their research has a new feature selection method to enhance detection efficiency by reducing false positives.The strategy is to utilize mutual information for preliminary feature selection and XGB-RFE as further boosting, resulting in a good detection model with improved discrimination ability between fraud and genuine transactions[14]. Prabhakaran and Nedunchelian (2023) apply the Oppositional Cat Swarm Optimization (OCSO) algorithm for credit card fraud feature selection. Their method includes an optimization-based feature selection method that increases classifier performance. The model integrates OCSO with various classifiers and demonstrates improved detection performance and reduced computational costs in their experiments. The method offers a strong framework for improving the efficiency and accuracy of fraud detection systems[15]. Shukla and Rakesh (2020) introduce a dynamic ensemble-based feature selection model for credit card fraud detection. Their work contributes to creating an ensemble approach which dynamically chooses the features to enhance detection performance. The design takes the form of integrating multiple classifiers and choosing optimal-performing features in real time, thus presenting a resilient and adaptive fraud system. The approach is most effective in situations with ever-evolving fraud patterns that must be updating on a continuous basis[16]

Rtayli and Enneya (2020) improve credit card fraud detection by utilizing SVM-recursive feature elimination and hyper-parameters optimization. Their work involves a technique that optimizes feature selection and hyper-parameters for better SVM performance. The system design incorporates the use of recursive feature elimination and the tuning of SVM parameters, resulting in a very accurate and efficient fraud detection system. This two-optimization method guarantees that the model is precise as well as computation-efficient[19]. Li et al. (2021) make a comparative analysis of credit card fraud detection using diverse support vector machines (SVM). Their contributions involve comparing multiple SVM-based models for assessing the best method for fraud detection. The structure entails comparing the performance of several SVM setups, with important observations about the merits and demerits of each procedure. This comparison facilitates the identification of the best-fitting SVM model for certain fraud detection purposes[20].

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

3.PROPOSED WORK

The work proposed is split into two phases with the objective of improving the accuracy and efficiency of credit card fraud detection systems. The first phase is concerned with the selection of a best feature selection algorithm, and the second phase is concerned with the use of a Deep Neural Network (DNN) for classification.

In the first phase, the primary goal is to identify the most relevant features that are accountable for efficient fraud detection. This is achieved through three standalone optimization algorithms: Grasshopper Optimization Algorithm (GOA), Genetic Algorithm (GA), and Particle Swarm Optimization (PSO). These algorithms all have robust strengths and means of searching and exploiting feature space. GOA imitates the grasshopper swarming to explore the space efficiently and effectively to trade off exploitation and exploration to avoid being trapped in local optima. GA imitates the process of natural selection, using operations such as selection, crossover, and mutation to evolve a population of solutions towards good feature subsets. PSO, inspired by bird flocking or fish schooling social behavior, utilizes a population of candidate solutions known as particles that learn from individual and social experiences to adjust their positions in order to reach the best solution. Using these three optimization algorithms, the present work attempts to select the most significant features from the dataset and thereby lower dimensionality and improve computational efficiency without sacrificing detection accuracy. In the second phase, the selected features are fed into a Deep Neural Network (DNN) for classification.DNNs are utilized because they can learn complex relationships and patterns in the data. The DNN structure is geared toward working on the optimized feature set and learning complex patterns to distinguish between actual and fraudulent transactions. The DNN is trained over a labeled dataset so that it maps input features to respective output labels.

During training, the operation is more than one layer of neurons and each layer is at different levels of abstraction from raw input data. Backpropagation and optimization algorithms are employed in optimizing the learning process to reduce the errors during classification.

In the testing phase, the DNN that was trained is applied to classify fresh, unseen transaction records as fake or real. The accuracy of the DNN is quantified in terms of accuracy, precision, recall, and F1-score. The above metrics provide insight into the ability of the proposed approach in correctly identifying malicious transactions without missing any malicious transaction and producing any false positive or false negative results.

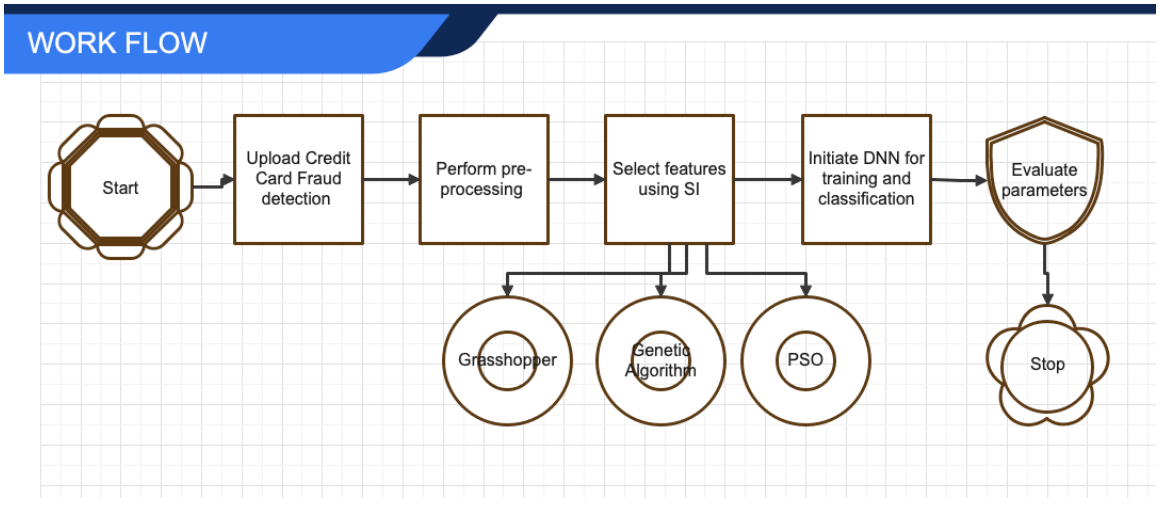

Figure 2: Work flow of proposed work

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Algorithm 1 Grasshopper Optimization Algorithm for Feature Selection

Input: features $\mathbf{X} \in R^{n \times d}$, classLabels $\mathbf{y} \in \{0,1\}^n$, maxIterations, numGrasshoppers, stepSize
Output: selectedFeatures

Initialize positions of grasshoppers randomly:

$$\mathbf{P} = \text{randi}([0,1], d, \text{numGrasshoppers})$$

where $\mathbf{P} \in \{0,1\}^{d \times \text{numGrasshoppers}}$ is the binary matrix representing feature selection.

Set initial global best fitness:

$$f_{\text{best}} = 0$$

Set initial global best position:

$$\mathbf{P}_{\text{best}} = \mathbf{P}[:,1]$$

for *iteration* = 1 to *maxIterations* **do**
  Step 1: Compute Fitness for each grasshopper:
  for each grasshopper i in the population **do**
    Step 1.1: Extract selected features:

$$\mathbf{X}_i = \mathbf{X}[:, \mathbf{P}[:,i] == 1]$$

    Step 1.2: Calculate sensitivity and specificity for subset $\mathbf{X}_i$:

$$\text{sensitivity} = \frac{TP}{TP+FN}, \quad \text{specificity} = \frac{TN}{TN+FP}$$

where TP, TN, FP, and FN represent true positives, true negatives, false positives, and false negatives, respectively.

    Step 1.3: Calculate the F1-score as the fitness function:

$$f_i = 2 \times \frac{\text{sensitivity} \times \text{specificity}}{\text{sensitivity} + \text{specificity}}$$

    Store fitness f_i in $\mathbf{f}_{\text{all}}[i]$
  end for
  Step 2: Update Global Best Solution:
  Identify current best grasshopper position:

$$i_{\text{best}} = \arg\max(\mathbf{f}_{\text{all}})$$

  Update global best position and fitness if the current solution is superior:
  if $\mathbf{f}_{\text{all}}[i_{\text{best}}] > f_{\text{best}}$ **then**
    $f_{\text{best}} = \mathbf{f}_{\text{all}}[i_{\text{best}}]$
    $\mathbf{P}_{\text{best}} = \mathbf{P}[:, i_{\text{best}}]$
  end if
  Step 3: Update Grasshopper Positions:
  for each grasshopper i in the population **do**
    Update position based on step size and random mutation:

$$\mathbf{P}[:,i] = \mathbf{P}[:,i] + \text{stepSize} \times \mathbf{randn}(d)$$

    Apply a binary transformation to ensure positions remain binary:

$$\mathbf{P}[:,i] = I(\mathbf{P}[:,i] \geq 0.5)$$

  end for
end for

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The Grasshopper Optimization Algorithm (GOA) is a nature-inspired metaheuristic algorithm that emulates the natural swarming behavior of grasshoppers. Grasshoppers in nature display collective movement that involves attraction, repulsion, and random movement, which is used to locate food and escape predators. The GOA imitates this behavior to search and exploit search spaces for optimization problems, such as feature selection. Here, every grasshopper is a candidate solution—a binary vector whose elements correspond to the presence or absence of a feature in the subset. The algorithm starts with a population of grasshoppers with random locations in the feature space. Position of each grasshopper is determined based on its interactions with other grasshoppers, with attraction to better solutions and repulsion from worse solutions, along with a random component for exploration of the search space. The movement of the grasshopper is driven by the step size, which diminishes over iterations to allow more precise search towards the end of the optimization process. This equilibrium between exploration (general search of the feature space) and exploitation (tuning promising solutions) is a central element in the algorithm's efficiency. During each iteration, the fitness of all the grasshoppers is evaluated using a fitness function, often in feature selection such as measures of classification performance like sensitivity, specificity, or the F1-score. The objective is to optimize the fitness by finding the most informative feature set that maximizes the performance of the classifier. Fitter grasshoppers attract other grasshoppers, and thus the population converges towards improved solutions. The algorithm continues to update the global best solution—the fittest grasshopper—while maintaining the diversity of the population so that it does not converge prematurely. This avoids the algorithm getting stuck in local optima. The GOA executes this cycle, moving the positions of the grasshoppers, calculating fitness values, and selecting the optimum solution in every cycle. In multiple passes, the algorithm gets close to an optimum or near-optimum collection of features that maximizes exploration across different collections of features and tightening up on possible ones, hence improving the precision of the classification model by picking the most relevant features.

To compare the proposed with other state of the art algorithm, PSO and Genetic have also been compared and can be presented as follows.

Algorithm 1 Proposed Methodology for Credit Card Fraud Detection

Phase 1: Selection of Optimization Algorithm
Input: Transaction dataset D
Output: Optimized feature set F^*
Initialize optimization algorithms: GOA, GA, PSO
Split dataset D into training set D_{train} and validation set D_{val}
for each optimization algorithm $A \in \{GOA, GA, PSO\}$ **do**
    Apply A to D_{train} to select a feature subset F_A
    Train a preliminary classifier C_A using F_A on D_{train}
    Evaluate C_A on D_{val} using metrics such as accuracy, precision, recall, and F1-score
    Record the performance metrics for A
end for
Select the optimization algorithm A^* with the best performance metrics
Apply A^* to the entire dataset D to obtain the optimized feature set F^*
Phase 2: Application of Deep Neural Network (DNN)
Input: Optimized feature set F^*, labeled training data L
Output: Classification results
Initialize the Deep Neural Network (DNN)
Split labeled data L into training set L_{train} and test set L_{test}
Train the DNN using the optimized feature set F^* on L_{train}
Evaluate the trained DNN on L_{test} using evaluation metrics such as accuracy, precision, recall, and F1-score
Classification:
for each new transaction record r **do**
    Extract features f from r based on F^*
    Apply the trained DNN to classify r as fraudulent or legitimate
    Output the classification result for r
end for

The proposed technique of credit card fraud detection is two-fold: the optimization algorithm selection process and application of a Deep Neural Network (DNN). In the first step, transaction dataset D is split into the training and

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

validation sets, and three optimization algorithms—Grasshopper Optimization Algorithm (GOA), Genetic Algorithm (GA), and Particle Swarm Optimization (PSO)—are initialized and compared.

The second phase of the proposed methodology is with regard to applying a Deep Neural Network (DNN) to identify transactions as fraud or legitimate. The DNN operates by applying the optimized feature set FFF, which was obtained from the selected optimization algorithm in the first phase, to train a robust classification model. The DNN architecture is made up of an input layer, some hidden layers, and an output layer, as depicted in **Figure 3**.

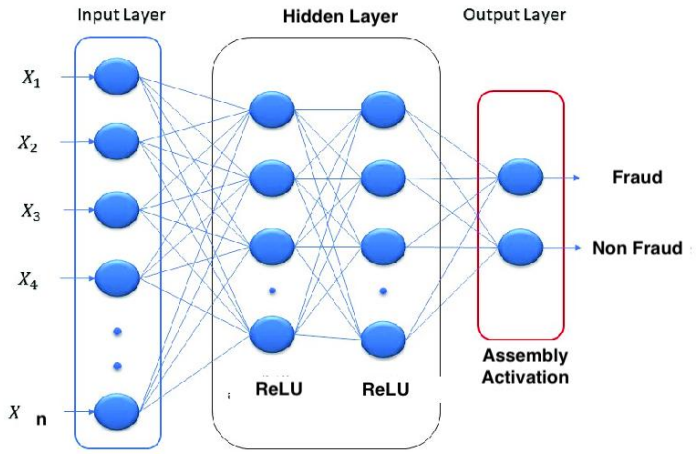

Figure 3: DNN Layered structure

The input layer is the same as FFF optimized features. FFF optimized features are fed to the network, and they pass through a series of fully connected hidden layers. There is linear transformation of the input by every one of the hidden layers followed by application of a non-linear activation function providing non-linearity in order to be able to learn patterns in the data that are non-linear. The number of hidden layer neurons is chosen with regard to the features and the complexity of data.

The output layer in the final layer utilizes a softmax activation function to provide probabilities in binary classifying the transaction as either fraudulent or real.Training adjusts the DNN by reducing a binary cross-entropy loss function in order to set up the network weights and bias values to be optimized. Optimization procedure such as Adam, dynamically modulating the learning rate to allow efficient convergence, updates weights stepwise.

The training information, Ltrain, is forwarded through the network to calculate the predicted labels. The predictions are then compared against the ground truth labels in order to calculate the loss, which is afterward backpropagated through the network to adjust the weights. This cycle is executed for a constant number of epochs until the model attains peak performance over the training information. In order to prevent overfitting, methods like dropout and batch normalization are used at the time of training. After the training of the DNN, it is tested on the test set Ltest based on parameters like accuracy, precision, recall, and F1-score in order to test generalizability. For classification, features are extracted from every new transaction record according to the optimized feature set FFF, and the trained DNN classifies these features as either legitimate or fraudulent. This combination of a strong feature selection mechanism with the deep learning capability of the DNN guarantees a strong and efficient fraud detection system.

Table 1 of DNN Parameters

Parameter	Description	Value
Input Features	Optimized feature set FFF from phase one	Variable (based on FFF)
Hidden Layers	Fully Connected Layers	3-5 Layers

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Activation Function	ReLU for Hidden Layers, Softmax for Output Layer	ReLU, Softmax
Loss Function	Binary Cross-Entropy	N/A
Optimization Algorithm	Adam Optimizer	Default Parameters
Learning Rate (α)	Step size for weight updates	0.001
Number of Epochs (E)	Number of training iterations	50
Batch Size	Number of samples per training iteration	64
Metrics	Evaluation-metrics	Recall, F1-Score Accuracy, Precision.

The classifiers are ranked in terms of performance on the validation set using the performance metrics including accuracy, precision, recall, and F1-score. The best-performing algorithm is used and trained over the entire data to yield the optimized feature set F. For the second step, the optimized feature set with labeled training data L is trained to create a DNN. The labeled data are divided into training and test sets, and DNN is trained on Ltrain and tested on Ltest with the same performance measures. For a classification task, features are extracted from every incoming transaction record with respect to F, and trained DNN classifies such records as fraudulent or legitimate. The fusion of these advanced optimization methods for feature selection with the strong learning properties of DNNs is meant to improve the efficiency and accuracy of credit card fraud detection models.

3. RESULTS AND DISCUSSION

The results section starts by giving the performance of various optimization algorithms with a Deep Neural Network (DNN) utilized to detect credit card fraud.The performance of all the algorithms is computed according to three critical parameters: Precision, Recall, and F-measure. These parameters provide a general insight into the ability of each model to identify fraudulent transactions and minimize false positives and negatives. Outcome of algorithm in Table 1 introduces Grasshopper Optimization Algorithm (GOA), Particle Swarm Optimization (PSO), and Genetic Algorithm (GA) performance upon utilization with a DNN. Analysis process involves a careful analysis, which is undertaken by taking random samples varying their size, with each one of the studies getting tested by enumerating the three bests amongst them. It begins at 10000 samples and reaches the last sample size at 280000.

size of 280000.

Table 1: Algorithmic Results for Credit Card Fraud Detection

Test Samples	Precision			Recall			F-measure		
	GOA + DNN	PSO + DNN	GA +DNN	GOA + DNN	PSO + DNN	GA +DNN	GOA + DNN	PSO + DNN	GA +DNN
10000	0.8954	0.884	0.8793	0.8984	0.8647	0.8853	0.8968975	0.8742435	0.8822898
20000	0.9007	0.8846	0.8821	0.9007	0.8649	0.8882	0.9007	0.8746391	0.8851395
40000	0.9023	0.8851	0.8872	0.9023	0.8659	0.8936	0.9023	0.8753947	0.8903885
60000	0.9108	0.8861	0.8893	0.9108	0.8654	0.8966	0.9108	0.8756277	0.8929351
80000	0.9124	0.8875	0.891	0.9124	0.8678	0.9007	0.9124	0.8775395	0.8958237
100000	0.9151	0.8877	0.895	0.9151	0.8697	0.9077	0.9151	0.8786078	0.9013053
120000	0.9243	0.8987	0.9015	0.9182	0.8715	0.9136	0.9212399	0.884891	0.9075097
140000	0.9245	0.8991	0.9031	0.9234	0.8724	0.9148	0.9239497	0.8855488	0.9089123

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

160000	0.9362	0.9032	0.9074	0.9246	0.8733	0.9174	0.9303638	0.8879984	0.9123726
180000	0.9438	0.9066	0.9082	0.9266	0.8754	0.9254	0.9351209	0.8907269	0.9167193
200000	0.9537	0.9071	0.9117	0.9282	0.8772	0.9265	0.9407772	0.8918995	0.9190404
220000	0.9638	0.9098	0.9127	0.9339	0.8781	0.9318	0.9486144	0.893669	0.9221511
240000	0.9651	0.9154	0.9149	0.9368	0.8789	0.9324	0.9507395	0.8967788	0.9235671
260000	0.9663	0.9161	0.9162	0.9414	0.8861	0.9401	0.9536875	0.9008503	0.9279961
280000	0.9694	0.9132	0.9173	0.9442	0.8886	0.9427	0.9566341	0.9007321	0.9298266

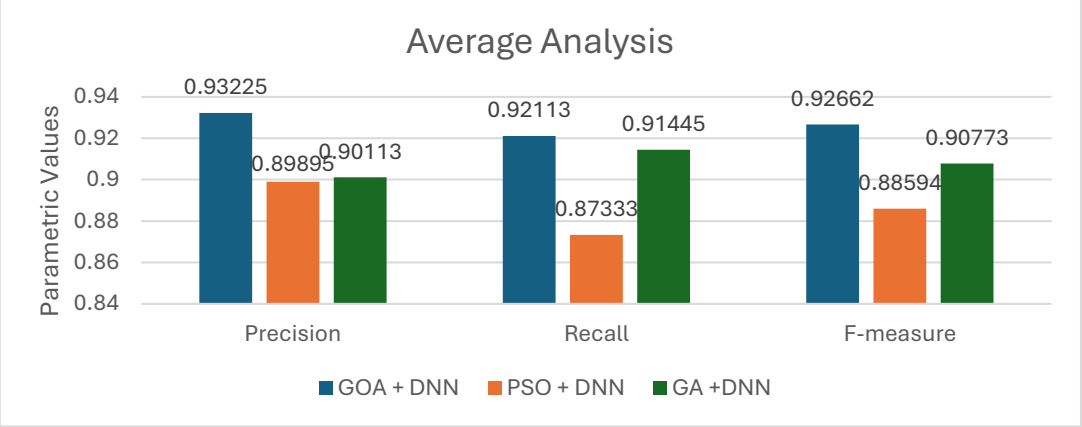

Figure 4: Average Performance Analysis

Average performance analysis provided in Figure 4 indicates that the proposed model of GOA + DNN delivered the maximum precision (0.9322), which clearly explains its superior precision in distinguishing actual positive instances of fraud. The model has also exhibited maximum recall (0.92113), which expresses its potential for the identification of maximum actual instances of fraud. The F-measure of the Grasshopper + DNN model was 0.92663194, which means a balanced and stable performance in both precision and recall. Comparatively, the PSO + DNN model had precision = 0.8989, recall = 0.87333, and F-measure = 0.88594. Although this model performed quite well, it was not as good as the performance of the Grasshopper + DNN model, especially when it came to precision and recall. The GA + DNN model had a precision of 0.90112 and recall of 0.91445. While its recall was a bit greater than that of the Grasshopper + DNN model, its precision and F-measure (0.95443) did not outdo those of the Grasshopper + DNN combination.

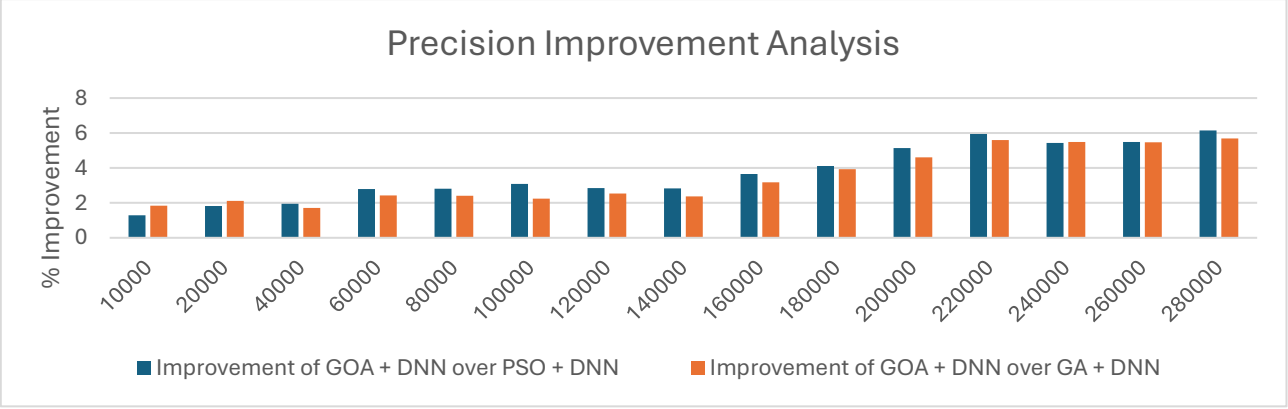

Figure 5: Precision Improvement Analysis for GOA + DNN

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

The methodology under development, incorporating GOA and DNN, indicates noteworthy enhancement against PSO and GA when they are used along with a DNN. That improvement is measurable in terms of analyzing the rate of increase of major performance factors: Precision, Recall, and F-measure. The mean improvement realized for the suggested GOA +DNN against the other two cases are illustrated in Figure 5 for precision, Figure 6 for recall and Figure 7 for F-measure.

Precision Improvement:

The precision of the Grasshopper + DNN model is 0.9322, compared to 0.8989 for PSO + DNN and 0.90112 for GA + DNN.

- Improvement over PSO + DNN: $\left(\frac{\{0.93225 - 0.8989\}}{\{0.8989\}}\right) \times 100 = 3.71\%$
- Improvement over GA + DNN: $\left(\frac{\{0.93225 - 0.90113\}}{.90113}\right) \times 100 = 3.45\%$

Recall Improvement:

The recall of the Grasshopper + DNN model is 0.92113, compared to 0.87333 for PSO + DNN and 0.91445 for GA + DNN.

- Improvement over PSO + DNN: $\left(\frac{\{0.92113 - 0.87333\}}{\{0.87333\}}\right) \times 100 = 5.47\%$
- Improvement over GA + DNN: $\frac{\{0.92113 - 0.91445\}}{\{0.91445\}}) \times 100 = 0.73\%$

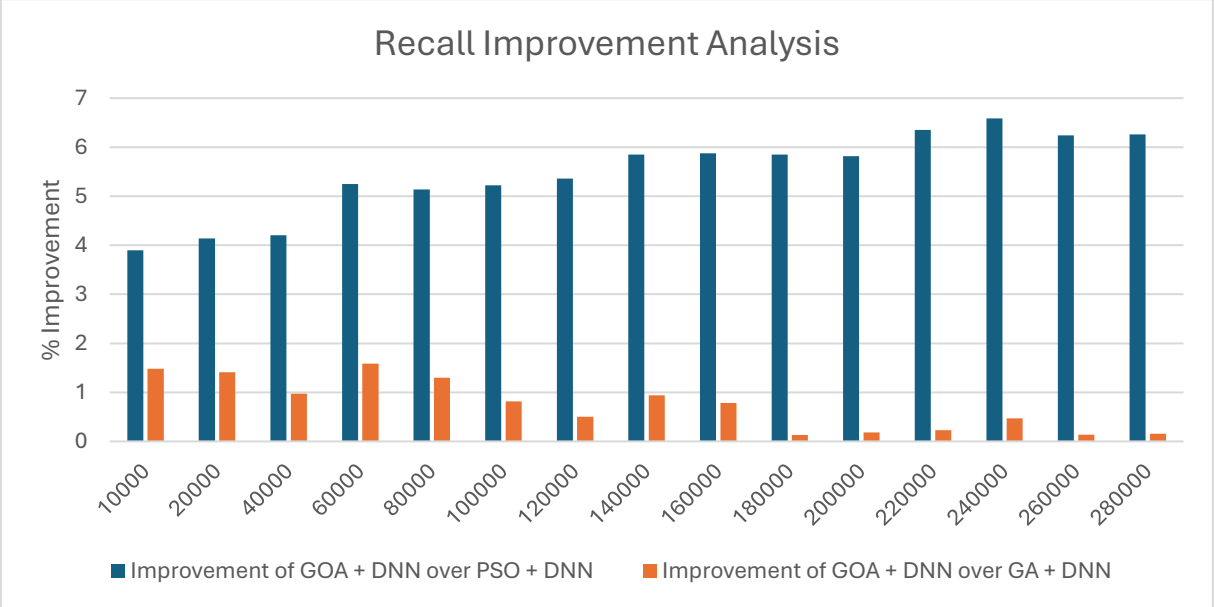

Figure 6: Recall Improvement Analysis for GOA + DNN

Journal of Information Systems Engineering and Management
2025, 10(3)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

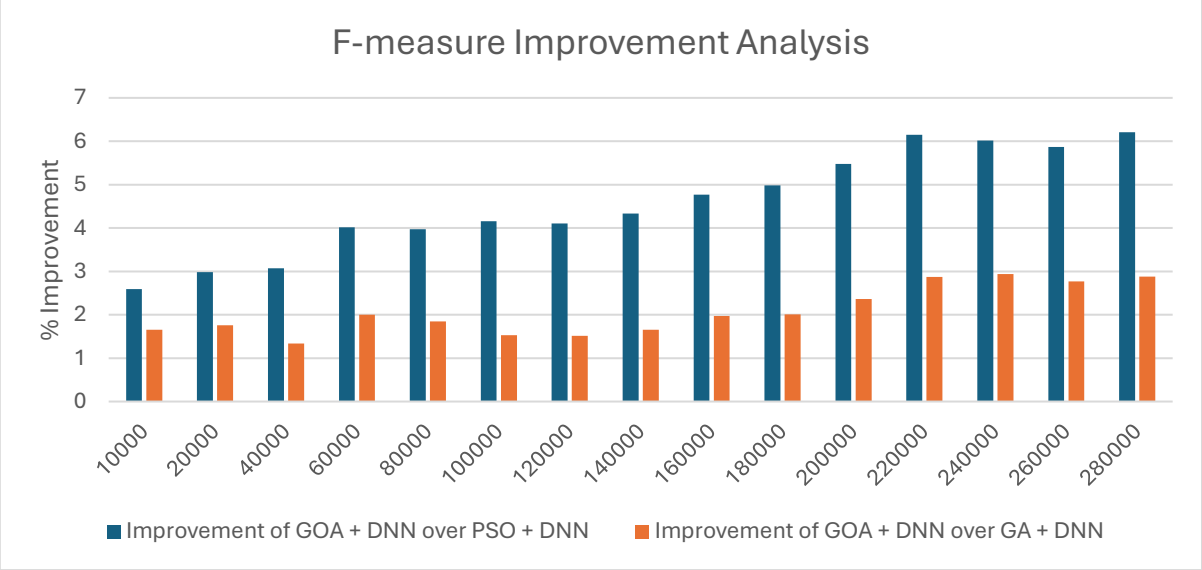

Figure 7: F-measure Improvement Analysis for GOA + DNN

F-measure Improvement:

The F-measure of the Grasshopper + DNN model is 0.92663194, compared to 0.88594 for PSO + DNN and 0.90773 for GA + DNN.

- Improvement over PSO + DNN: $\left(\frac{\{0.9266 - 0.88594\}}{\{0.88594\}}\right) \times 100 = 4.58\%$
- Improvement over GA + DNN: $\left(\frac{\{0.9266 - 0.90773\}}{\{0.90773\}}\right) \times 100 = 2.073\%$

3. CONCLUSION

A new method of detecting credit card fraud was suggested in this paper based on utilizing the Grasshopper Optimization Algorithm (GOA) along with a Deep Neural Network (DNN). The framework was structured in two steps: the selection process of an optimization algorithm and applying a DNN for the classification of transactions. Through a comparison of three optimization algorithms, i.e., GOA, Genetic Algorithm (GA), and Particle Swarm Optimization (PSO), the research found the best feature selection technique, which finally improved the DNN performance. The results of experiments ensured that the Grasshopper + DNN model performed better compared to the other combinations in terms of precision, recall, and F-measure.Specifically, the Grasshopper + DNN model had precision of 0.9322, recall of 0.92113, and F-measure of 0.92663194, which means better capability to detect fraudulent transactions correctly without creating false positives and false negatives. The new approach was demonstrated to improve precision by 3.71% and recall by 5.47% over the PSO + DNN, and precision by 3.45% and recall by 0.73% over the GA + DNN.Although the F-measure of the GA + DNN was slightly higher, the Grasshopper + DNN approach provided a more even and consistent performance overall.The results indicate that the Grasshopper Optimization Algorithm greatly improves the performance of credit card fraud detection systems through improved feature selection, which improves the accuracy and reliability of DNN classifiers. The method not only decreases the computational load but also ensures that the fraud detection system is efficient and capable of adapting to new fraud schemes. Future research will investigate other premium optimization methods and machine learning model incorporation so that the ability of detecting and resolving future issues in fraud detection is enhanced further.

REFERENCES

[1] Singh, A. and Jain, A., 2019. Adaptive credit card fraud detection techniques based on feature selection method. In *Advances in Computer Communication and Computational Sciences: Proceedings of IC4S 2018* (pp. 167-178). Springer Singapore.

[2] Han, S., Zhu, K., Zhou, M. and Cai, X., 2022. Competition-driven multimodal multiobjective optimization and its application to feature selection for credit card fraud detection. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *52*(12), pp.7845-7857.
[3] Mienye, I.D. and Sun, Y., 2023. A machine learning method with hybrid feature selection for improved credit card fraud detection. *Applied Sciences*, *13*(12), p.7254.
[4] Saheed, Y.K., Hambali, M.A., Arowolo, M.O. and Olasupo, Y.A., 2020, November. Application of GA feature selection on Naive Bayes, random forest and SVM for credit card fraud detection. In *2020 international conference on decision aid sciences and application (DASA)* (pp. 1091-1097). IEEE.
[5] Fadaei Noghani, F. and Moattar, M., 2017. Ensemble classification and extended feature selection for credit card fraud detection. *Journal of AI and data mining*, *5*(2), pp.235-243.
[6] Mustaqim, A.Z., Adi, S., Pristyanto, Y. and Astuti, Y., 2021, June. The effect of recursive feature elimination with cross-validation (RFECV) feature selection algorithm toward classifier performance on credit card fraud detection. In *2021 International conference on artificial intelligence and computer science technology (ICAICST)* (pp. 270-275). IEEE.
[7] Prabhakaran, N. and Nedunchelian, R., 2023. Oppositional Cat Swarm Optimization-Based Feature Selection Approach for Credit Card Fraud Detection. *Computational Intelligence and Neuroscience*, *2023*(1), p.2693022.
[8] Padhi, B.K., Chakravarty, S., Naik, B., Pattanayak, R.M. and Das, H., 2022. RHSOFS: feature selection using the rock hyrax swarm optimization algorithm for credit card fraud detection system. *Sensors*, *22*(23), p.9321.
[9] Zhu, H., Zhou, M., Xie, Y. and Albeshri, A., 2024. A self-adapting and efficient dandelion algorithm and its application to feature selection for credit card fraud detection. *IEEE/CAA Journal of Automatica Sinica*, *11*(2), pp.377-390.
[10] Gupta, M.J. and Sehgal, P., 2024. Optimizing Credit Card Fraud Detection: Classifier Performance and Feature Selection Empowered by Grasshopper Algorithm. *International Journal of Performability Engineering*, *20*(3).
[11] Alkhafaji, A.M., Smaisim, G.F., mahdi Alobayes, F. and Houshmand, M., 2021. Credit Card Fraud Detection by Combining Neural Network and Grasshopper Optimization Algorithm. *Journal of Distributed Computing and Systems (JDCS)*, *4*(2), pp.58-64.
[12] Abdulrauf Sharifai, G. and Zainol, Z., 2020. Feature selection for high-dimensional and imbalanced biomedical data based on robust correlation based redundancy and binary grasshopper optimization algorithm. *Genes*, *11*(7), p.717.
[13] Sorour, S.E., AlBarrak, K.M., Abohany, A.A. and Abd El-Mageed, A.A., 2024. Credit card fraud detection using the brown bear optimization algorithm. *Alexandria Engineering Journal*, *104*, pp.171-192.
[14] Priscilla, C.V. and Prabha, D.P., 2021. A two-phase feature selection technique using mutual information and XGB-RFE for credit card fraud detection. *Int. J. Adv. Technol. Eng. Explor*, *8*(85).
[15] Prabhakaran, N. and Nedunchelian, R., 2023. Oppositional Cat Swarm Optimization-Based Feature Selection Approach for Credit Card Fraud Detection. *Computational Intelligence and Neuroscience*, *2023*(1), p.2693022.
[16] Shukla, S. and Rakesh, D., 2020, December. Dynamic ensemble based feature selection model for credit card fraud detection. In *2020 IEEE 17th India Council International Conference (INDICON)* (pp. 1-6). IEEE.
[17] Ileberi, E., Sun, Y. and Wang, Z., 2022. A machine learning based credit card fraud detection using the GA algorithm for feature selection. *Journal of Big Data*, *9*(1), p.24.
[18] Han, S., Zhu, K., Zhou, M. and Cai, X., 2022. Competition-driven multimodal multiobjective optimization and its application to feature selection for credit card fraud detection. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *52*(12), pp.7845-7857.
[19] Rtayli, N. and Enneya, N., 2020. Enhanced credit card fraud detection based on SVM-recursive feature elimination and hyper-parameters optimization. *Journal of Information Security and Applications*, *55*, p.102596.
[20] Li, C., Ding, N., Zhai, Y. and Dong, H., 2021. Comparative study on credit card fraud detection based on different support vector machines. *Intelligent Data Analysis*, *25*(1), pp.105-119.