SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V13I4P126

Volume 13 Issue 4, 307-316, April 2026

Original Article

Snow Leopard Green Anaconda Optimization-based Feature Selection with Credit Card Fraud Detection using Artificial Neural Network

Shuchita Sheokand[1], Sunita Beniwal[1*]

[1]*Department of Computer Science & Engineering, Guru Jambheshwar University of Science & Technology, Hisar, Haryana, India.*

[*]*Corresponding Author : sunitabeniwalcse@gmail.com*

Received: 22 January 2026 Revised: 22 February 2026 Accepted: 24 March 2026 Published: 30 April 2026

Abstract *- Credit card holders are easy targets for fraud. With digitalization, online payments are increasingly prevalent through e-commerce and other websites. This rapid growth in digital transactions has significantly increased the risk of online fraud. Several challenges are faced by fraud detection systems, including delays in verification, concept drift, and class imbalance. However, many of the learning algorithms developed for fraud detection make assumptions that are often impractical in practical fraud detection systems. To tackle these issues, a model named Artificial Neural Network with Snow Leopard Green Anaconda Optimization (ANN with SLGAO) was proposed for detecting fraud in credit cards. Initially, input data from the credit card fraud dataset was pre-processed using quantile normalization, followed by feature selection using hybrid SLGAO, and Borderline- Synthetic Minority Over-sampling Technique (SMOTE) was used for data augmentation. Finally, fraudulent transactions were detected using an Artificial Neural Network (ANN). The proposed ANN with SLGAO achieved an accuracy of 91.848%, specificity of 91.685%, and sensitivity of 91.644%.*

Keywords *- Artificial neural network, Credit card fraud, Green Anaconda Optimization, Snow Leopard Optimization Algorithm, Synthetic Minority Over-sampling Technique.*

1. Introduction

Most financial organizations have made business services accessible to the public through internet banking. In today's competitive financial environment, E-payment methods are essential for making services and purchases easier. These organizations offer customers debit cards to enhance convenience by allowing users to shop without cash. In addition to debit cards, credit cards offer additional benefits, such as protection against stolen cards. Customers must verify the purchase with the merchant before completing any transaction with a credit card [1]. In the global economy, credit card payments are increasingly becoming a key driver of modern digital commerce. Multiple stakeholders, such as payment processors, issuers, merchants, and banks, are exploring various approaches to leverage advancements in technologies to address their evolving needs. Emerging technologies are enabling the development of innovative payment solutions, driven by improved connectivity, increasing use of IoT devices, rising adoption of mobile devices, and in-app payment capabilities. These technologies have led to the evolution of payment using credit cards [2]. The impact of online financial loss is more significant if fraudsters obtain card details; they may use the cards themselves or share the information with others. In India, the details of credit cards of approximately 70 million individuals are available and sold on the dark web [3, 4].

Credit card fraud or identity theft occurs when someone other than the cardholder uses the card to make purchases without permission. A scam may occur when someone steals, fakes, or loses a credit card [5]. Fraudulent activities within the financial sector are on the rise, with a growing trend of card usage. The widespread use of credit cards has led to an increase in fraud. [6]. With a significant portion of global transactions relying on credit cards, fraudsters are finding ways to exploit credit card holders. Manipulation and deceptive tactics make it easier for people to fall victim to scams [1]. For detecting credit card fraud, various approaches, such as statistical methods, Machine Learning (ML), and Deep Learning (DL), are used. ML techniques help in detecting fraudulent transactions in real time by analyzing available data. However, statistical techniques such as clustering, hypothesis testing, and regression are employed to analyze and identify issues in credit card transactions [6]. Nowadays, Artificial Intelligence (AI) is a booming technology that paves the way for developing novel strategies. It can enhance next-

generation credit card fraud detection by enabling proactive monitoring of credit card limits, increasing approval rates, and minimizing declined transactions [2]. Deep Learning techniques automatically recognize complex patterns and features in datasets, enabling accurate detection of fraudulent activity [6].

Traditional fraud detection models suffer from lower scalability, increased computational complexity, and late detection, which often fail to capture nonlinear patterns and handle class imbalance effectively. Some approaches were able to achieve high accuracy at the cost of increased architectural and computational complexity, thereby limiting their application to large real-time datasets. Hence, a novel strategy is required for detecting fraud in credit cards that is computationally efficient, handles class imbalance, and is scalable. Motivated by these limitations, a hybrid optimization framework named Snow Leopard Green Anaconda Optimization (SLGAO) was developed to effectively identify the most relevant features for credit card fraud detection. Borderline-SMOTE was used to address class imbalance by generating synthetic minority-class samples and to improve the model's learning capability after pre-processing with quantile normalization. Finally, ANN was trained using selected optimal features to effectively learn complex transaction patterns and improve the detection of fraudulent activities.

The layout of the remaining sections in this paper is as follows: Section 2 provides an overview of methods for detecting credit card fraud; Section 3 describes the SLGAO methodology; Section 4 presents the ANN results with SLGAO; and Section 5 presents the conclusion and future directions.

2. Motivation

Credit card fraud is defined as unauthorized use of a card to make fraudulent transactions. It often results in financial losses for the cardholder or issuer. The growing threat of fraud and its significant financial consequences drive the development of new real-time fraud detection techniques, and these reviewed approaches focus specifically on detecting credit card fraud.

2.1. Literature Survey

N. S. Alfaiz et al. [4] proposed AllKNN-CatBoost for fraud detection. Even though this strategy managed the increasing transaction volumes without any decrease in performance, it struggled with potential threats and processing delays, hindering timely fraud detection. V. R. Ganji et al. [7] presented an SSPO-based DRN that uses Shuffled Shepherd Political Optimization and a Deep Residual network for detecting credit card fraud. This approach increased customer satisfaction by minimizing the number of false positives and optimizing the accuracy of legitimate communications. However, it required high computational resources, which limited its use on weaker systems. A. Alharbi et al. [8] devised a text2IMG technique for detecting fraud. This method helped to minimize potential losses and offered rapid fraud alerts. However, it faced challenges adapting to novel, sophisticated fraud techniques lacking historical patterns.

J. Karthika et al. [9] designed a model named DCNN, i.e., Dilated Convolutional Neural Network, for detecting fraud in credit cards. It allowed CNN to capture longer-range dependencies and multi-scale patterns in transactions. However, it reduced the number of majority-class samples, resulting in the loss of vital information.

Karthik et al. [10] combined boosting and bagging classifiers to design a hybrid ensemble model leveraging the key strengths of both techniques. By applying a hybrid strategy to handle data imbalance, their experiments on the Brazilian bank and UCSD-FICO datasets demonstrated strong robustness and reliability. Strelcenia and Prakoonwit [11] proposed the K-CGAN approach to evaluate and compare how well classifiers distinguish between fraudulent and legitimate transactions. Their method focused on analyzing classifier performance for both criminal and authorized transaction patterns.

Alshawi [12] presented a fraud detection approach designed to handle very small and highly imbalanced datasets. He trained several models, including LR, decision trees, random forest, Naïve Bayes, etc., using synthetic data generated through GANs. The results showed that all models, except Naïve Bayes, classified with an accuracy of 95% or higher. Mienye and Sun [13] demonstrated a robust deep-learning framework in which LSTM and GRU networks served as base learners, and a Multilayer Perceptron (MLP) served as the meta-learner. SMOTE-ENN was used to address class imbalance and improve the dataset's class distribution stability. Group Search Firefly Algorithm was designed by Jovanović et al. [14] to address credit card fraud detection, presenting a hybrid framework that combines machine learning techniques with swarm-based metaheuristic optimization. The study applied the enhanced Group Search Firefly approach to tune Extreme Learning Machines, Support Vector Machines, and Extreme Gradient Boosting classifiers.

Padhi et al. [15] applied the Rock Hyrax Swarm Optimization-based Feature Selection (RHSOFS) technique to enhance credit card fraud transaction detection by identifying a subset of relevant, optimal features from high-dimensional datasets. Prabhakaran and Nedunchelian [16] proposed the OCSODL-CCFD framework for detecting and classifying fraud. The method integrates several components, including pre-processing, feature selection using the OCSO algorithm, hyperparameter optimization using CKHA, and a BiGRU classifier. The OCSO-based design contributes to reduced computational complexity while enhancing overall classification performance.

2.2. Challenges

Despite significant advancements in ML and DL techniques, several limitations still exist. Traditional models may not capture nonlinear patterns in large-scale transaction data. The strategies developed lacked the ability to scale and adapt to data distribution across several dimensions within databases to detect fraud [4]. The occurrence of false alarms needs to be controlled, which was not done efficiently by existing techniques [7]. The time taken to detect fraud was longer, and computational complexity also increased [10].

The techniques were unable to address the class imbalance problem. The issue of overfitting and not being able to generalize to unseen fraud patterns was also there. [11, 12]. High accuracy at the cost of increased complexity in architecture and computation, hence limiting its application to large real-time datasets. (GAN-based). Also, large volumes of labelled data and hyperparameter tuning are required, making it impossible for practical situations. (LSTM, GRU, BiGRU).

Hence, there is a need to design a novel strategy for detecting fraud in credit cards that is computationally efficient, handles class imbalance, and is scalable. Motivated by these limitations, this study proposes a hybrid optimization-based feature selection method, Snow Leopard Green Anaconda Optimization (SLGAO), integrated with an Artificial Neural Network to enhance fraud detection performance.

3. Materials and Methods

3.1. System Model

Fraudulent transactions on credit cards cause financial losses for cardholders as well as financial institutions. It may also result in theft of identity, damage to reputation, and increased security costs. Moreover, evolving fraud techniques make it challenging for detection systems. To overcome these issues, an efficient ANN-based method with SLGAO was developed to detect credit card fraud. Initially, quantile normalization is employed for pre-processing. Then, feature selection is accomplished using SLGAO, and Borderline-SMOTE is employed to perform data augmentation. Finally, credit card fraud detection is accomplished by an ANN. The system model of ANN with SLGAO is portrayed in Figure 1.

3.2. Acquisition of Data

A dataset with a number of data points is considered. It is represented as follows.

$$G = \{G_1, G_2, \ldots\ldots, G_q, \ldots G_z\} \quad (1)$$

Here, G_q represents the qt^h data from a dataset G. This dataset [17] contains transactions from two days, with 492 fraud transactions out of a total of 284,807. The dataset is highly imbalanced, with fraudulent transactions accounting for only 0.172% of the dataset.

3.3. Pre-Processing using Quantile Normalization

Pre-processing is the process of resizing, normalizing, and reducing noise in the input data to improve quality for further analysis. Here, pre-processing is performed by utilizing quantile normalization with G_q as input data. It is an effective method for pre-processing, as it ensures the distribution of similar data across different datasets by making comparisons more reliable without any systematic biases.

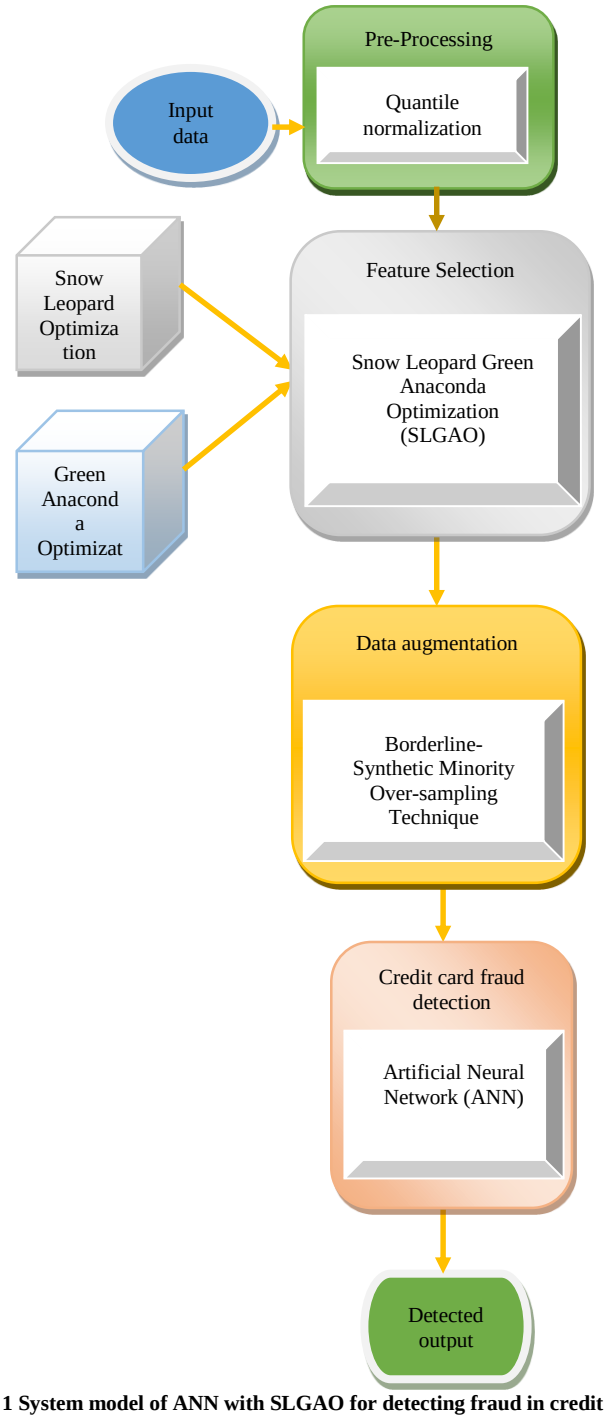

Fig. 1 System model of ANN with SLGAO for detecting fraud in credit cards

Quantile normalization [18] comprises several steps. Initially, the data from each sample is ranked, then restored to its original order. A class-specific method is applied to categorize the data into distinct classes, with each class being normalized separately. The discrete technique further improves this method by incorporating a batch factor, allowing separate grouping of both batches and classes. Finally, the quantile normalization approach is used to preserve distributional differences across various conditions. This is performed by assigning a weight based on the variability observed between groups. The data resulting from this quantile normalization is signified as G_q with [g×h] dimension

3.4. Feature Selection using SLGAO

Feature selection is the selection and identification of a subset of features from a large dataset. It helps improve the performance of the model by improving interpretability, reducing complexity, and reducing overfitting issues. Here, SLGAO performs feature selection. It is an efficient approach to perform selection of features as it can select the optimal feature subsets while avoiding overfitting.

SLGAO was used to improve feature weighting by combining the strengths of both algorithms. This hybrid approach effectively selects the most relevant features by enhancing model accuracy. Along with this, reducing the complexity of the feature set helps to prevent overfitting by ensuring the model generalizes better to unseen data. SLGAO adapts to changing patterns in the data by optimizing the feature weight distribution. Hence, it is a more stable and reliable model with improved performance and reduced overfitting risk. Here, $G_q$with [g×h] dimension is utilized as an input.

3.4.1. Solution Encoding

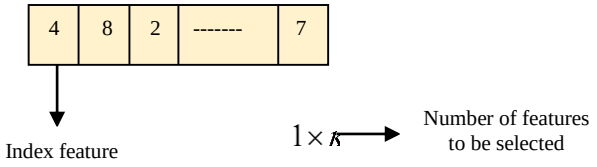

Fig. 2 Solution Encoding

This process entails generating a range of possible solutions within a defined search space, which helps identify optimal features by streamlining problem-solving through solution encoding. Solution encoding is illustrated in Figure 2.

3.4.2. Fitness Function

It is used to measure and identify the optimal solution to a given optimization problem, calculated using the weighted Euclidean distance to select the optimal features. It is expressed below.

$$Z(a_\sigma, b_\sigma) = \sqrt{\sum_{\sigma=1}^{j} J_\sigma (a_\sigma - b_\sigma)^2} \quad (2)$$

where,

$$\begin{cases} J_\sigma = a_\sigma, if\, a_\sigma \neq 0 \\ J_\sigma = 1 otherwise \end{cases} \quad (3)$$

Here, the features are represented as a_σ and the targeted feature is indicated as b_σ.

3.4.3. Algorithmic steps of SLGAO

SLGAO was used to select optimal features to enhance the classification accuracy and efficiency of models employed for credit card fraud detection. Here, SLOA and GAO are integrated to form SLGAO. SLOA [19] is an approach that was developed based on the hunting behavior of the snow leopard, and it could dynamically enhance detection accuracy by continuously learning from changing transaction behaviors.

The GAO [20] approach is based on the hunting and swimming behavior of the Green Anaconda, which could explore optimal solutions inspired by natural selection to enhance detection accuracy. By integrating these two algorithms, SLGAO is designed to select an optimal subset of unidentifiable features. The SLGAO flexibly modifies its search behavior, thus leading to faster convergence and more accurate solutions in complex credit card fraud detection scenarios. It follows the steps below.

Step 1: Initialization

In initialization, each member of a population is referred to as a snow leopard. Here, the position of each member in the search space is initiated using the expression below,

$$M = \{M_1, M_2, \ldots, M_p, \ldots, M_\Omega\} \quad (4)$$

Here, M_p denotes the p^{th} Snow leopard, the overall snow leopard count is denoted as Ω, and the snow leopard population is represented as M.

Step 2: Fitness Function

The fitness function is performed to select appropriate features. It is expressed in Eq. (2).

Step 3: Travel Routes and Movement phase

Through marking scent, snow leopards choose their positions and travel routes. It follows a zig-zag pattern along with indirect paths. Usually, it scrapes the ground with its hind paws to mark the scent. Moreover, it moves towards one another or traces the movement of other Snow leopards based on these natural behaviors. It is expressed below.

$$H_p(w+1) = H_p(w)\left[1 - c\left[U \times sign\left(Z_p - Z_d\right)\right]\right] + c.H_{d,v} \times sign\left(Z_p - Z_d\right) \quad (5)$$

Here, $H_p(w)$ represents the newly found value, $d$denotes row number for the leading Snow leopard, and the row number of the selected Snow leopard p is located at v^{th} axis, within [0,1] interval the generated arbitrary number is denoted as c, and the row number of the elected snow leopard is signified as Z.

Expression of GAO is,

$$H_p(w+1) = H_p(w) + \left(1 - 2c_p\right)\frac{S_\beta - T_\beta}{B} \quad (6)$$

The iteration count of the algorithm is represented as B, respectively, and the lower and upper bounds are indicated as S and T.

The updated solution of SLGAO is

$$H_p(w+1) = \frac{\left((2c_p - 1)\frac{S_\beta - T_\beta}{B}\right)[1 - cU \times sign(Z_p - Z_d)] + c.H_{d,v} \times sign(Z_p - Z_d)}{cU \times sign(Z_p - Z_d)} \quad (7)$$

Where,

$$U = round(1 + c) \quad (8)$$

Here, $H_p(w+1)$ represents the output, $d$denotes row number for leading Snow leopard, problem variable is signified as v, row number of selected snow leopard p is located at v^{th}axis, within $[0, 1]$ Interval, the generated arbitrary number is denoted as c, and the row number of the elected snow leopard is signified as z. Iteration count of the algorithm is signified as B, lower and upper bounds are indicated as $S$and T.

Here $c$is made adaptive, then SLGAO is expressed as,

$$c = k - \left(\frac{\chi}{M}\right) \times x \quad (9)$$

Here, the parameter constant k is considered as 2, χ is the iteration. Then, the overall Snow leopard number is denoted as M and the problem variable number as x.

Step 4: Hunting

During the hunting phase, snow leopards exhibit stalking and attacking behaviors, along with the updating of group members' positions. The expression for the hunting behavior of the snow leopard p is,

$$\delta_{p,v} = H_{p,v}, v = 1,2,3,\ldots,m \quad (10)$$

where, $H_{p,v}$ denotes the new value of the problem variable v.

Step 5: Reproduction

The natural reproductive behaviors of the snow leopard are detailed in this reproduction step. Assuming that each mating pair of snow leopards produces one cub, this can be formulated as:

$$V_n = \frac{H_n + A_{\Omega - n + 1}}{2}, n = 1,2,3,\ldots,\frac{\Omega}{2} \quad (11)$$

Here, by mating two snow leopards, a cub is born and is represented as n.

Step 6: Mortality

In SLGAO, the snow leopard population remains constant during each iteration due to mortality, despite reproduction potentially increasing the population. During each reproduction cycle, the snow leopard count is equivalent to the number of cubs born.

Step 7: Reevaluation of fitness

The fitness function is assessed repeatedly until the best solution is reached.

Step 8: Termination

It terminates when the best solution is attained by continuously repeating iterations, and the obtained output is indicated as R_q with the dimension of $[g \times h]$, such that $o > h$.

3.4.4. Data augmentation utilizing Borderline-SMOTE oversampling

Data Augmentation is a method for expanding the database by using existing data points. This aims to increase the performance and robustness of the trained samples. Here, the Borderline-SMOTE oversampling method is used to perform data augmentation. As it can enhance model performance in imbalanced datasets, and generate synthetic samples for the minority class by targeting borderline instances. Here, $R_q$with $[g \times h]$ the dimension is given as an input.

The Borderline-SMOTE [21] algorithm helps to balance classes in a database, mainly near the class boundary, by oversampling the minority class. It mainly identifies the nearest neighbors and then selects the neighbors that are closer to the majority class, and this chosen group is referred to as DANGER.

$$Syn_\tau = \gamma_\tau + \rho_\tau \times \Re_\tau, \tau = 1,2,\ldots,\lambda \quad (12)$$

Here, an arbitrary number is indicated as ρ_τ, and instance in DANGER set is denoted asγ_τ. The generated result is indicated as $P_q$with $[e \times h]$ dimension, where $g < h$.

3.5. Fraud Detection using an ANN model

Detecting fraud in credit cards is significant for preserving financial transactions and preventing unauthorized access to users' accounts. These systems examine user behavior, historical data, and transaction patterns to identify abnormalities that could signal fraudulent activity. Here, the ANN model is used to perform fraud detection in credit cards.

The input utilized in this network is P_q with $[e \times h]$ dimension, which is the augmented data.

3.5.1. ANN Architecture

The architecture of an ANN is derived from the structure and function of the human brain, with nodes interconnected in a manner that resembles the way neurons are linked in the brain. It includes 15 hidden layers, and the RELU is used as the activation function in credit card fraud detection [22]. ANN's architecture is portrayed in Figure 3.

Here, the augmented data P_q is utilized as an input; this input is provided to various nodes such as Node 1, Node 2,…, Node z. Then the weight associated with the input is represented as i_1, i_2,..i_z. These input, along with weights, is provided to the neuron, and the generated output is represented as L_q. This L_q is the credit card fraud detection output.

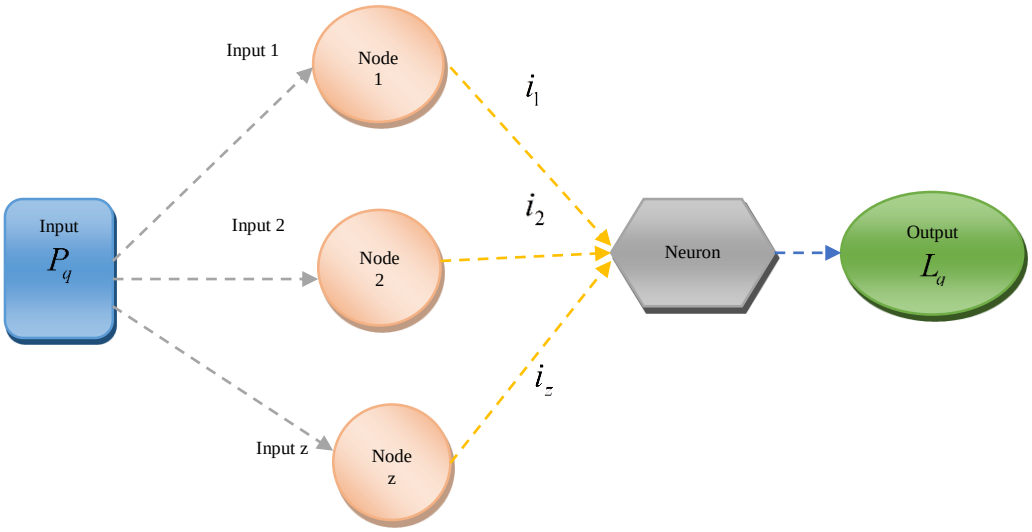

Fig. 3 Architecture of ANN

4. Results and Discussion

The results of the ANN with SLGAO are discussed in this part.

4.1. Experimental Setup

The implementation of ANN with SLGAO for detecting fraud in credit cards was conducted using the Python programming environment. These experiments were carried out on a system with an Intel Core i7 processor, 16 GB RAM, and Windows 10 operating system. All simulations and model training were executed using Python-based machine learning libraries. The proposed ANN model consists of an input layer, multiple hidden layers, and an output layer. The architecture includes 15 hidden layers with ReLU (Rectified Linear Unit) as the activation function to capture nonlinear patterns in credit card transaction data. The dataset was divided into training and testing, with 90% of the data used as training data and the remaining 10 % as testing data to check the performance of the proposed model. K-fold cross-validation with K = 9 was also used to check the model's generalization ability. The evaluation of the proposed ANN-SLGAO model was done using accuracy, sensitivity, and specificity measures. These configurations allow for reproducing the results and enable comparison with other models used in this study.

4.2. Dataset Description

The dataset [17] contains details of transactions made using credit cards over two days by cardholders from Europe in September 2013. The dataset contains 284,807 transactions, of which 492 are fraudulent, making the dataset highly imbalanced with only 0.172% fraud transactions in the complete dataset. All variables in the input are numerical and were obtained through Principal Component Analysis (PCA) to protect confidentiality. In addition to the PCA components, the dataset includes two additional features: Amount and Time. Amount reflects transaction value and may be useful for cost-sensitive learning tasks. Time measures the seconds elapsed since the first transaction, and

4.3. Evaluation Metrics

Accuracy, specificity, and sensitivity metrics were utilized for measuring the efficiency of the ANN with SLGAO.

4.3.1. Accuracy

It measures the model's ability to determine whether a transaction is fraudulent or legitimate [16].

$$Accuracy = \frac{C_r + D_r}{C_r + C_s + D_s + D_r} \quad (13)$$

Here, a true negative is indicated as C_s, C_r denotes true positive, $D_s$represents false negatives and $D_r$specifies false positives.

4.3.2. Sensitivity

It refers to the proportion of credit card fraud cases that are correctly identified [23], and it is expressed as

$$Sensitivity = \frac{C_r}{C_r + D_s} \quad (14)$$

4.3.3. Specificity

It refers to the proportion of legitimate credit card transactions that are correctly identified as non-fraudulent. It is expressed as:

$$Specificity = \frac{C_s}{C_s + D_r} \quad (15)$$

4.4. Ablation Analysis

Some approaches, such as ANN without feature selection, ANN with GAO (Feature selection), and ANN with SLO (Feature selection), are compared with the Proposed ANN with SLGAO to assess its efficiency using varying training data and K-fold evaluation.

4.4.1. Evaluation based on Training Data

A comparative evaluation of the proposed ANN with SLGAO is illustrated in Figure 4. The evaluation of the proposed method with respect to accuracy is depicted in Figure 4(a). For training data of 90%, the accuracy of the proposed ANN with SLGAO is 91.301%, while other methods have an accuracy of 88.810%, 89.965%, and 90.652%. Figure 4 (b) illustrates the assessment of the ANN with SLGAO with respect to sensitivity. For training data at 90%, conventional methods have sensitivities of 88.678%, 89.691%, and 90.442%. Moreover, the proposed method has a sensitivity of 91.228%. Figure 4 (c) illustrates the assessment of the ANN with SLGAO with respect to specificity. For training data at 90%, conventional methods have specificities of 88.564%, 89.537%, and 91.175%. Moreover, the proposed method has a specificity of 91.265%.

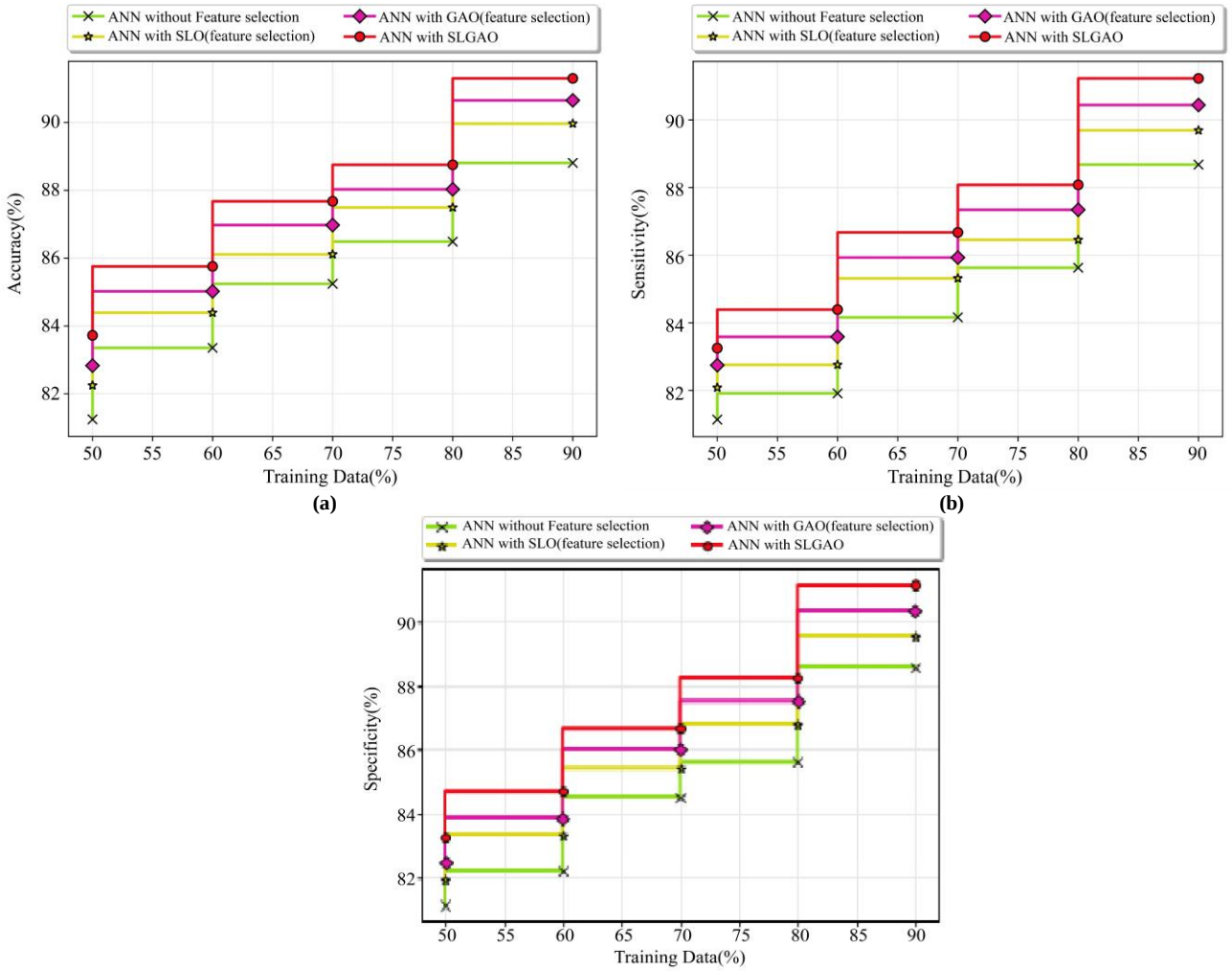

Fig. 4 Assessment of the proposed ANN with SLGAO based on training data using a) Accuracy, b) Sensitivity, and c) Specificity

4.4.2. Evaluation based on K-Fold Evaluation

Figure 5 illustrates the evaluation of the ANN with SLGAO with K-fold evaluation. In Figure 5(a) the evaluation of the ANN with SLGAO in terms of accuracy is displayed. For K value 9, the ANN with SLGAO achieves an accuracy of 91.848%, while the other traditional methods achieve accuracies of 89.969%, 90.776%, and 91.321%. The ANN with SLGAO sensitivity assessment is shown in Figure 5 (b). Proposed ANN with SLGAO has a sensitivity of 91.644%, while the other methods have 89.194%, 90.300%, and 91.140% for K = 9. The assessment of ANN with SLGAO for specificity is shown in Figure 5 (b). Proposed ANN with SLGAO has a specificity of 91.685%, and the other methods have 89.336%, 90.248%, 91.078%, and 91.685% for K value 9.

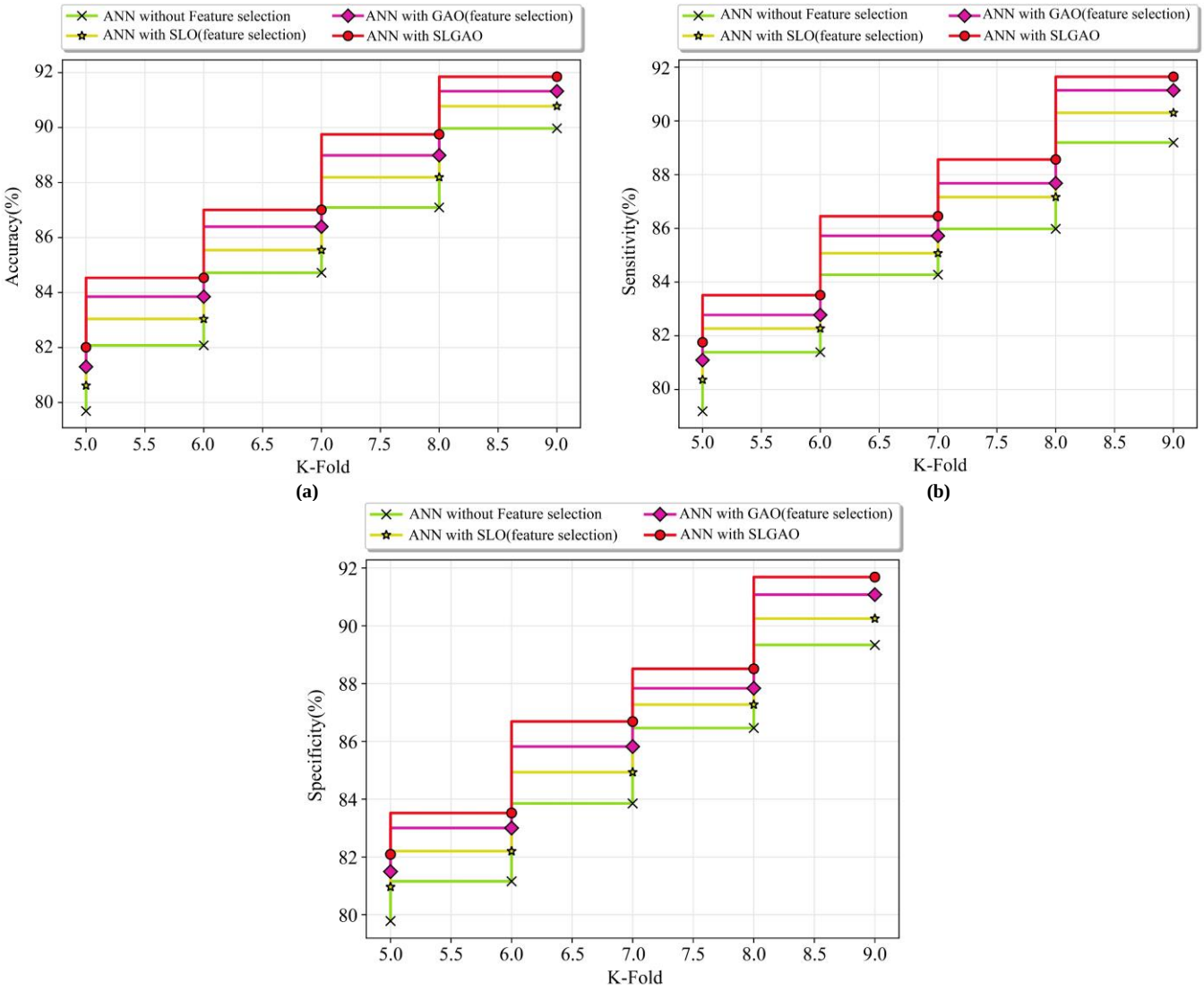

Fig. 5 Evaluation of ANN with SLGAO based on K-fold evaluation using a) Accuracy, b) Sensitivity, and c) Specificity

4.5. Comparative Discussion

A comparison of ANN with SLGAO across various setups is shown in Table 1. Here, the performance of the ANN with SLGAO is evaluated using accuracy, sensitivity, and specificity. In 90% of the training data, the proposed ANN with SLGAO has an accuracy of 91.301%. However, the other methods have accuracies of 88.810%, 89.965%, and 90.652%. This demonstrates that ANN with SLGAO has the ability to learn patterns and accurately detect fraudulent transactions. For 90% training data, the traditional methods have sensitivities of 88.678%, 89.691%, and 90.442%, while the ANN with SLGAO has a sensitivity of 91.228%. It shows that ANN with SLGAO has the ability to identify the positive cases effectively. The optimal outcomes are attained by ANN with SLGAO, such as 91.848% of accuracy, and 91.644% of sensitivity, and 91.685% of specificity. Thus, the proposed ANN with the SLGAO method can effectively identify fraudulent transactions while minimizing false positives.

Table 1. Comparative discussion of ANN with SLGAO

Evaluation	Metrics	ANN without feature selection	ANN with Feature Selection using GAO	ANN with Feature selection SLO	Proposed ANN with SLGAO
Training data=90%	Accuracy (%)	88.810	89.965	90.652	91.301
	Sensitivity (%)	88.678	89.691	90.442	91.228
	Specificity (%)	88.564	89.537	90.373	91.175
K fold=9	Accuracy (%)	89.969	90.776	91.321	91.848
	Sensitivity (%)	89.194	90.300	91.140	91.644
	Specificity (%)	89.336	90.248	91.078	91.685

The performance of the proposed feature selection method is evaluated against existing techniques such as AllKNN-CatBoost [4], SSPO-based DRN [7], text2IMG conversion technique [8], and DCNN [9]. All the techniques are analysed under four setups and compared with the ANN to identify its efficiency. Setup-1 is the feature selection by SLOA. Setup-2 is the feature selection by GAO. Setup-3 is without feature selection. Setup-4 is the feature selection using SLGAO. The comparative analysis across these setups for different classifiers is shown in Table 2.

Table 2. The comparative analysis across setups for different classifiers

Training data = 90%	Metrics	AllKNN-CatBoost	SSPO-based DRN	text2IMG conversion technique	DCNN	ANN with Adaptive SLGAO
Setup-1	Accuracy (%)	80.999	81.900	83.038	85.760	90.258
	Sensitivity (%)	80.117	82.682	84.578	86.373	90.052
	Specificity (%)	79.960	81.232	83.342	85.790	90.265
Setup-2	Accuracy (%)	82.917	83.320	85.292	86.181	90.692
	Sensitivity (%)	81.551	82.826	84.955	86.327	90.567
	Specificity (%)	81.851	83.510	84.964	86.539	90.561
Setup-3	Accuracy (%)	84.066	85.293	87.619	88.217	91.137
	Sensitivity (%)	83.504	84.228	85.271	87.286	91.169
	Specificity (%)	81.378	83.064	85.714	87.916	91.101
Setup-4	Accuracy (%)	84.491	85.198	87.835	89.300	91.301
	Sensitivity (%)	84.724	86.593	87.352	88.561	91.228
	Specificity (%)	83.356	84.575	86.227	88.925	91.175

5. Conclusion

The main goal of detecting fraud in credit cards is to identify and prevent fraudulent transactions, thereby reducing financial losses for cardholders and financial organizations. However, it faces challenges while distinguishing fraudulent transactions from legitimate ones. To tackle these issues, developing effective detection models is significant to improve security. Hence, a model named ANN with SLGAO is proposed for feature selection and detecting fraud in credit cards. Input data from the credit card fraud detection dataset is passed to the pre-processing phase. Pre-processing of the input data is achieved using quantile normalization. Then, feature selection is accomplished using hybrid SLGAO, which is the combination of the SLOA and GAO. Moreover, Borderline-SMOTE is used to conduct data augmentation. Finally, fraud in credit cards is detected by an ANN. The experimental results of the proposed SLGAO have achieved 91.848% of accuracy, and 91.644% of sensitivity, and 91.685% of specificity.

The proposed model was able to effectively identify fraudulent transactions, but some limitations need to be acknowledged. As the model was evaluated on a dataset that contains transactions of a limited time period, the model may not be able to generalize to evolving fraud patterns in real-world financial systems. Also, the data is highly imbalanced. The Borderline-SMOTE technique may not generate artificial data that fully represents real fraud activity. This can reduce the performance of the model if applied to large-scale systems. In the future, the proposed model can be implemented on larger and more diverse real-world datasets collected from different financial institutions and time periods.

Conflicts of Interest

The authors declare no conflict of interest.

Funding Statement

The authors declare that no external funding was received for this research.

References

[1] Rejwan Bin Sulaiman, Vitaly Schetinin, and Paul Sant, "Review of Machine Learning Approach on Credit Card Fraud Detection," *Human-Centric Intelligent Systems*, vol. 2, pp. 55-68, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Asma Cherif et al., "Credit Card Fraud Detection in the Era of Disruptive Technologies: A Systematic Review," *Journal of King Saud University – Computer and Information Sciences*, vol. 35, no. 1, pp. 145-174, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[3] Saurabh C. Dubey, Ketan S. Mundhe, and Aditya A. Kadam, "Credit Card Fraud Detection Using Artificial Neural Network and Backpropagation," *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, pp. 268-273, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Noor Saleh Alfaiz, and Suliman Mohamed Fati, "Enhanced Credit Card Fraud Detection Model using Machine Learning," *Electronics*, vol. 11, no. 4, pp. 1-16, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Pampana Gnana Venkata Sai, P. Srinivasulu, Tulasi Raju Nethala, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," *International Journal of Novel Research and Development*, vol. 9, no. 10, pp. 310-318, 2024. [Publisher Link]

[6] Abdul Rehman Khalid et al., "Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach," *Big Data and Cognitive Computing*, vol. 8, no. 1, pp. 1-27, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[7] Venkata Ratnam Ganji, Aparna Chaparala, and Radhika Sajja, "Shuffled Shepherd Political Optimization-Based Deep Learning Method for Credit Card Fraud Detection," *Concurrency and Computation: Practice and Experience*, vol. 35, no. 10, pp. 1-19, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[8] Abdullah Alharbi et al., "A Novel Text2IMG Mechanism of Credit Card Fraud Detection: A Deep Learning Approach," *Electronics*, vol. 11, no. 5, pp. 1-18, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] J. Karthika, and A. Senthilselvi, "Smart Credit Card Fraud Detection System based on Dilated Convolutional Neural Network with Sampling Technique," *Multimedia Tools and Applications*, vol. 82, no. 20, pp. 31691-31708, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[10] V. S. S. Karthik, Abinash Mishra, and U. Srinivasulu Reddy, "Credit Card Fraud Detection by Modeling Behavioral Patterns using a Hybrid Ensemble Model," *Arabian Journal for Science and Engineering*, vol. 47, pp. 1987-1997, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Emilija Strelcenia, and Simant Prakoonwit, "Improving Classification Performance in Credit Card Fraud Detection by using New Data Augmentation," *AI*, vol. 4, no. 1, pp. 172-198, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[12] Bandar Alshawi, "Utilizing GANs for Credit Card Fraud Detection: A Comparison of Supervised Learning Algorithms," *Engineering, Technology & Applied Science Research*, vol. 13, no. 6, pp. 12264-12270, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[13] Ibomoiye Domor Mienye, and Yanxia Sun, "A Deep Learning Ensemble with Data Resampling for Credit Card Fraud Detection," *IEEE Access*, vol. 11, pp. 30628-30638, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[14] Dijana Jovanovic et al., "Tuning Machine Learning Models Using a Group Search Firefly Algorithm for Credit Card Fraud Detection," *Mathematics*, vol. 10, no. 13, pp. 1-30, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[15] Bharat Kumar Padhi et al., "RHSOFS: Feature Selection Using the Rock Hyrax Swarm Optimization Algorithm for Credit Card Fraud Detection System," *Sensors*, vol. 22, no. 23, pp. 1-18, 9321, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[16] N. Prabhakaran, and R. Nedunchelian, "Oppositional Cat Swarm Optimization-Based Feature Selection Approach for Credit Card Fraud Detection," *Computational Intelligence and Neuroscience*, vol. 2023, no. 1, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[17] Credit Card Fraud Detection, Kaggle Dataset, 2025. [Online]. Available: https://www.kaggle.com/mlg-ulb/creditcardfraud

[18] Yaxing Zhao, Limsoon Wong, and Wilson Wen Bin Goh, "How to do Quantile Normalization Correctly for Gene Expression Data Analyses," *Scientific Reports*, vol. 10, pp. 1-11, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Petr Coufal et al., "Snow Leopard Optimization Algorithm: A New Nature-Based Optimization Algorithm for Solving Optimization Problems," *Mathematics*, vol. 9, no. 21, pp. 1-26, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Mohammad Dehghani, Pavel Trojovský, and Om Parkash Malik, "Green Anaconda Optimization: A New Bio-Inspired Metaheuristic Algorithm for Solving Optimization Problems," *Biomimetics*, vol. 8, no. 1, pp. 1-60, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[21] Taejun Lee, Minju Kim, and Sung-Phil Kim, "Data Augmentation Effects using Borderline-SMOTE on Classification of a P300-based BCI," *2020 8th International Winter Conference on Brain-Computer Interface (BCI)*, Gangwon, Korea (South), pp. 1-4, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[22] R.B. Asha, and Suresh Kumar, "Credit Card Fraud Detection using Artificial Neural Network," *Global Transitions Proceedings*, vol. 2, no. 1, pp. 35-41, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[23] J. Pradeep Kandhasamy, and S. Balamurali, "Performance Analysis of Classifier Models to Predict Diabetes Mellitus," *Procedia Computer Science*, vol. 47, pp. 45-51, 2015. [CrossRef] [Google Scholar] [Publisher Link]