International Journal of Computational and Experimental Science and ENgineering (IJCESEN)

Vol. 11-No.1 (2025) pp. 1128-1137
http://www.ijcesen.com

ISSN: 2149-9144

Research Article

A PSO-ACO based ANN Approach for Credit Card Fraud Detection

Shuchita Sheokand[1], Sunita Beniwal[2]*

[1]Department of Computer Science & Engineering, Guru Jambheshwar University of Science & Technology, Hisar, Haryana, India
Email: shuchita.sheokand@gmail.com - **ORCID:** 0000-0003-4708-951X

[2]Department of Computer Science & Engineering, Guru Jambheshwar University of Science & Technology, Hisar, Haryana, India
* **Corresponding Author Email:** sunitabeniwalcse@gmail.com - **ORCID:** 0000-0003-4708-9519

Article Info:

DOI: 10.22399/ijcesen.981
Received : 12 December 2024
Accepted : 08 February 2025

Keywords

ACO
PSO
ANN
Fraud Detection
Computational Efficiency

Abstract:

Credit card fraud is a major problem for both consumers and institutions in the ever-changing financial environment of today. Credit card fraud detection is a significant challenge in financial security, and a novel approach is proposed to enhance its accuracy. This work intends to detect fraudulent transactions on credit cards by use of PSO along with ACO in combination. The Hybrid PSO-ACO based ANN model uses PSO and ACO to refine the training process, resulting in improved classification performance. PSO optimizes the network's epoch settings and batch processing, while ACO fine-tunes batch selections. Experiments on two credit card transaction datasets show that the Hybrid PSO-ACO based ANN outperforms conventional ANN models and other optimization-based ANN approaches in terms of accuracy, sensitivity and specificity. The proposed model improves generalizing to fresh data, reduces overfitting, and balances minority class data. This work highlights the potential of combining multiple optimization techniques to advance fraud detection capabilities and provides a robust framework for future research.

1. Introduction

Credit card fraud has become a major threat in the digital era, resulting in substantial financial losses and eroding consumer trust in electronic payment systems [1]. Intricacy and complexity of dishonest behavior have made improved detection systems necessary. When trying to identify changing fraud trends, conventional approaches may miss fraudulent transactions or give false positives [2, 3]. In light of the shortcomings of traditional methods, current research is concentrated on the application of advanced mechanisms for credit card fraud detection [4-6]. It has been observed that deep learning and AI-based machine learning algorithms have been used to detect credit card fraud [7, 8]. In order to detect credit card fraud, some hybrid approaches have also been used [9, 10]. It has been observed that conventional research did use of AI based machine learning and deep learning systems for credit card fraud detection [11, 12]. Some of the research also considering hybrid approach where PSO and SVM are used for credit card fraud detection [13]. Moreover, several ensemble decision trees based credit card fraud detection mechanism are introduced by different researchers [14]. Deep learning-based model that used CNN and LSTM have been also used for credit card fraud detection [15, 16]. In this way, considering process flow, methodology, limitations of conventional research in area of credit card fraud detection [17] present research work offers an ANN [18, 19] based hybrid model integrating PSO [20, 21] along with ACO in order to solve these difficulties in case of more efficient credit card fraud detection. Combining PSO [22-24] along with ACO makes use of the advantages of both optimization approaches to raise detection accuracy along with efficiency, thereby reducing the CCF risks. Credit card theft poses a significant threat to financial organizations and consumers, leading to economic losses and weakening confidence in electronic payment systems [25]. The rapid growth of digital transactions and the complexity of dishonest plans necessitate strong and efficient fraud detection systems [26, 27]. Conventional techniques, often

based on rule-based systems, struggle to keep up with changing fraud strategies, resulting in significant false positive or missing detection rates [28]. ANNs have become a potential solution, but their effectiveness relies on training parameter optimization, a computationally demanding procedure [29]. Hybrid optimization methods combining the advantages of multiple algorithms are gaining attention for more accurate and efficient fraud detection systems. Two promising optimizers are PSO and ACO [30-32]. PSO uses swarm intelligence to investigate search spaces, while ACO mimics pheromone-based communication among agents to solve combinatorial problems. Combining these methods with ANNs can maximize the training process, improve model performance, and strengthen fraud detection powers. This study proposes a hybrid optimization framework combining PSO and ACO with ANNs to improve credit card fraud detection.

Rising and a main concern in case of banks and other financial organizations is CCF. Growing worry about credit card theft calls for further improvement in fraud detection systems Current fraud detection systems find great difficulty in always changing character of fraudulent activities, which often produces false positives along with significant financial losses. Apart from clear cash losses, credit card theft compromises consumer confidence along with soundness of financial system. Conventional models need sophisticated machine learning techniques as they have limited flexibility and significant false positive rates. An immediate need is enhancing systems' resilience and flexibility to rapidly identify fraudulent transactions with minimal false positives. In machine learning, optimization problems like determining ideal training parameter selections are also abound. Combining two hybrid optimizing methods, ACO along with PSO, could provide fresh approaches in case of fraud detection. Proposed research meets this need by offering a hybrid approach combining the best aspects of PSO [28] along with ACO [29-32] offering a more reliable means of credit card fraud detection. The paper is organized as follows: Section 1 provides an overview of problem along with the proposed solution. Section 2 discusses existing approaches of credit card fraud detection. In section 3 details the proposed hybrid model, including the application of PSO and ACO for optimization and experimental setup and datasets used are given. Section 4 presents results and analysis of the proposed model and gives a comparative analysis. And the findings are summarized and future research areas are outlined in last section.

2. Literature Review

Investigating credit card theft now takes front stage in order to guard consumers and financial institutions from significant losses. Many techniques have changed with time to provide more accurate and powerful fraud detection systems. Emphasizing the use of optimizing techniques, hybrid models, and machine learning, this survey of the literature synthesizes the most important works on the subject. El Hlouli et al. (2024) proposed a Weighted Binary ELM optimized by the Reptile Search Algorithm to enhance detection performance [1]. Comparative studies on oversampling techniques, such as the one by Amin et al. (2016), address class imbalance issues crucial for customer churn prediction, which is closely related to fraud detection scenarios [2]. Dal Pozzolo et al. (2017) introduced a realistic modeling framework and a novel learning strategy for fraud detection using NN, emphasizing the need for practical and effective solutions [3]. Similarly, Panigrahi et al. (2009) adopted a fusion approach that integrates Dempster–Shafer theory with Bayesian learning, highlighting the importance of combining probabilistic reasoning methods [4]. Firefly Algorithm enhancements have also been explored, as seen in the work of Rufai et al. (2021), who developed a credit card fraud detection system tailored for Nigerian financial institutions [5]. Feature selection techniques play a pivotal role in optimizing machine learning models, as demonstrated by Manokaran et al. (2023), who employed a novel set-theory-based hybrid method for anomaly detection in IoT edge systems [6]. Evolutionary algorithms, such as those reviewed by Jena et al. (2021), have become increasingly popular for designing fraud detection models due to their adaptability and robustness [7]. The application of PSO for global optimization, as discussed by Rauf et al. (2020), further showcases the potential of nature-inspired algorithms in addressing complex fraud detection challenges [8]. Transaction aggregation strategies, highlighted by Whitrow et al. (2009) [9], and data mining techniques reviewed by Ngai et al. (2011) [10], demonstrate the effectiveness of data-driven approaches for fraud detection. Phua et al. (2010) provide a comprehensive survey of data-mining-based fraud detection research, underlining the progression of classification frameworks over time [11]. More recently, genetic algorithms have been enhanced for feature selection in phishing URL detection, as presented by Kocyigit et al. (2024), reflecting a growing interest in applying advanced optimization techniques to related domains [12].

Saheed et al. (2024) proposed a modified BiLSTM model combined with hyperparameter tuning for cardiovascular disease prediction, demonstrating the potential of deep learning in mobile cloud environments [13]. Hybrid models such as the fusion of metaheuristic optimization techniques, as reviewed by Chalabi et al. (2022), and machine learning frameworks have been instrumental in addressing multi-objective challenges in fraud detection [14, 15]. Similarly, deep learning approaches, as reviewed by Nguyen et al. (2020) [16], and Mienye and Jere (2024) [18], have shown promise in credit card fraud detection, addressing challenges such as imbalanced datasets and computational complexity. Thennakoon et al. (2019) implemented real-time fraud detection using machine learning techniques, highlighting the importance of timely detection systems [17]. ANNs have also been extensively studied for fraud detection. Asha (2021) utilized ANNs for fraud detection [19], while Sahin (2011) compared ANN with logistic regression, highlighting the strengths of neural networks in capturing complex patterns [20]. Optimization algorithms have also been pivotal in improving fraud detection models [18]. Arora (2017) explored the hybridization of SOM and PSO for credit card fraud detection [21], while Prusti et al. (2023) combined genetic algorithms with PSO for enhanced detection accuracy [22]. The integration of neuro-fuzzy approaches with PSO and TLBO, as demonstrated by Ghodsi (2017), further showcases the adaptability of hybrid models in complex fraud scenarios [23]. Yılmaz (2023) extended this by developing a machine learning framework incorporating PSO for credit card fraud detection, emphasizing its efficiency and scalability [24]. Singh et al. (2022) proposed a financial fraud detection approach combining Firefly Optimization and SVM, demonstrating improved classification accuracy [25]. Similarly, Kamaruddin et al. (2023) evaluated various optimization and classifiers for electricity fraud prediction, emphasizing the utility of these methods in diverse fraud scenarios [26]. Comprehensive reviews, such as the one by Btoush et al. (2023), have highlighted the effectiveness of machine and deep learning models in addressing challenges in credit card cyber fraud detection [27]. Guo et al. (2019) developed a novel multi-objective PSO for comprehensible credit scoring [28], while Santana et al. (2019) explored variations of PSO to derive classification rules for credit risk in Ecuadorian financial institutions [29]. PSO has been instrumental in optimizing ANNs, as surveyed by Emambocus et al. (2023), showcasing their potential in enhancing model performance [30]. Kanan et al. proposed a novel ACO-based feature selection method, validated through comparative studies in face recognition systems.

3. Proposed Work

The key challenge in credit CFD is lowering computation costs and false positives while still efficiently spotting fraudulent activities. Often unable to fit dynamic nature of fraud, conventional techniques result in less-than-ideal performance. This work aims to create a hybrid model enhancing accuracy along with fraud detection system efficiency by means of PSO along with ACO. Figure 1 is overall process of proposed method and figure 2 shows PSO-ACO for batch and epoch optimization.

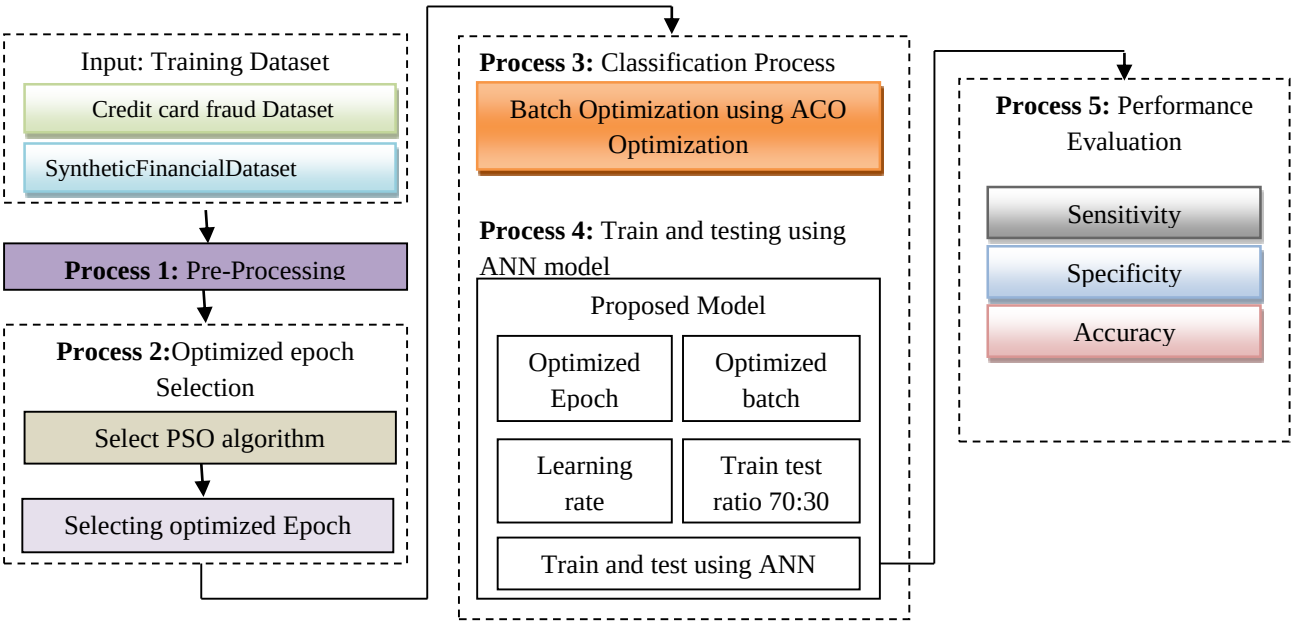


Figure 1. *Overall Process of Proposed Method*

Moreover, it has been observed that there is lack of accuracy in case of conventional ANN model. Thus proposed work is considering optimized batch and epoch for training ANN model with better accuracy, sensitivity and specificity. Focus of suggested work, which intends to generate a state of art CCF detection system, is integrating ACO together with PSO to boost detection accuracy along with efficiency. PSO is first used to optimize number of epochs in case of different batches of data. This process discovers best configurations in case of training model, designated P1, P2, P3, P4 and P5. Using ACO to choose optimal batch and epoch will help to further enhance training process of the model. Combining PSO and ACO seeks to solve the flaws in traditional FD methods. Thus proposed ANN is considering optimized hyper parameters such as batch size and epochs from optimizer. The hybrid ANN approach is expected to improve detection accuracy while concurrently lowering the processing load as a more efficient way in case of real-time FD in credit card transactions. The method is validated using measures like as accuracy, specificity, along with sensitivity by means of a real-world dataset.

3.1 Process Flow of Proposed Work

1. Data Collection: Buildan enormous credit card transaction database, classed as either genuine or fraudulent.Preprocessing: Clean the data along with do any required preparation, therefore giving the optimization algorithms best available input.
2. PSO Application: PSO can help you discover ideal number of epochs while training across many batches of data. Every batch results in a unique set of optimized epochs marked P1, P2, P3, P4, and P5.
3. ACO Application: Select the best batch along with epoch from PSO results by use of ACO.
4. Model Training and Validation: Train fraud detection model using ANN considering optimized batch and epoch, and validate its performance using a separate validation set.
5. Evaluation: Compare model performance to conventional approaches using accuracy, specificity, sensitivity.
6. Conclusion: Summarize findings, emphasizing the improved detection accuracy and reduced computational cost achieved by the proposed hybrid model.

3.2 Algorithm for Credit Card Fraud Detection Using PSO and ACO Optimization

Step 1 Data Collection is made where Dataset is D and Label is L

Step 2. Perform data Preprocessing that considers Data Cleaning: $D_{Clean,}$ Normalization: $D_{norm,}$ Feature Selection: $F_{selected}$Operations:

$D_{clean} = Clean\_data(D)$

$D_{norm} = normalize\_data(D_{clean})$

$F_{Selceted} = feature\_selection(D_{norm})$

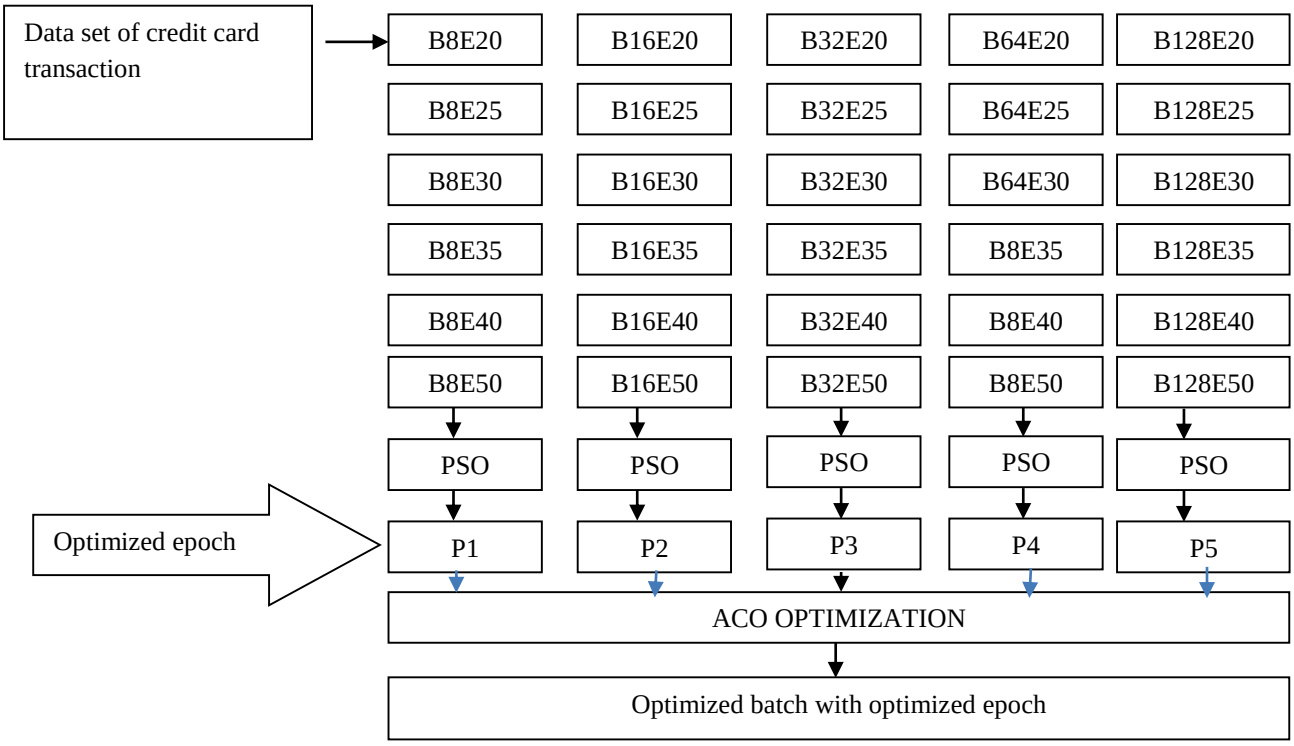


Figure 2. *PSO-ACO for batch and epoch optimization*

Step 3 Apply PSO algorithm to get optimized epochs for each batch
PSO Initialization: Parameters P_{PSO}
Optimized Epochs: Eopt= {P1, P2, P3, P4, P5}
Initialize PSO with P_{PSO}
for each batch Bi in batches $\{B_1, B_2,\ldots,B_n\}$:
E_{opti}=PSO_optimize_epochs (B_i)
Store optimized epochs as P1, P2, P3, P4, P5

4. Apply ACO based optimization in order to get best batch and epoch configuration
ACO Initialization: Parameters P_{ACO}
Best Batch and Epochs: B_{best},E_{best}
Initialize ACO with P_{ACO}
for each combination of Bi and Eopti:
Model Mi=initialize_ANN
Train Mi with Bi and Eopti
Evaluate Mi to get performance metrics
Select best batch B_{best} and epochs E_{best} using ACO

5. Perform Model Training and Validation for credit card detection
Model Initialization: M_{final}
Training and Validation Results: $V_{results}$
M_{final}=initialize_ANN
Train M_{final} with B_{best} and E_{best}
$V_{results}$=validate_model (M_{final}, validation data)

6. Evaluate Accuracy A, Sensitivity (Recall) *S*,Specificity Sp
A = (TP + TN) (TP + TN + FP + FN}
S = TP/ (TP + FN)
Sp = TN/ (TN + FP)

7.Compare A,S,Sp of proposed with conventional models where training has been made considering 3 cases
ANN based non optimized model,
ANN based PSO model
ANN based ACO model

3.3 Description Of Proposed Work

Description of dataset is given below in table 1. There is a fraud or genuine designation attached to every single transaction.

Table 1. *Dataset used*

Attribute	Credit Card Fraud Detection
Source	Purchases in Europe (September 2013)
Instances	284,807
Classes	2
Classes (Good/Bad)	284,315/ 492

Preprocessing: The data has to be cleaned and preprocessed before optimization can begin. Both feature selection and normalization are done to pre-process the data.

PSO Application: Finds the optimal amount of training epochs for many batches of data using PSO. Optimal epochs P1, P2, P3, P4, along with P5 are the result of PSO's exploration of the solution space, which determines the optimal batch size.

$$\mathbf{Pi=argminP\ \{Loss\ (\theta, P)\ |\ P \in \{Pmin,, Pmax\}\}}$$

where Pi is the optimal epoch for the ith batch, θ represents model parameters, along with Loss(θ,P) is the loss function dependent on the number of epochs P.
ACO Application: ACO based optimization is used in order to get best batch and epoch configuration. To choose the optimal batch and epoch, ACO mimics the ant's behavior by calculating the shortest route.

$$\mathbf{B^*=argminB\ \{Cost\ (PB)+\alpha \cdot Efficiency\ (PB)\}}$$

where B* is the selected batch, PB is the corresponding epoch from PSO, Cost (PB) represents the computational cost, and Efficiency (PB) represents the model efficiency, with α as a weighting factor.
Model Training and Validation:With the batch and epoch chosen in the ACO stage, ANN model is trained to identify fraud. The generalizability of the model is verified by means of another validation set.

$$\mathbf{\theta^*=argmin\theta\ \{Loss(\theta;X^*,y^*)\}}$$

where θ* are the optimized model parameters, X* is the training set, and y* are the corresponding labels.
Evaluation: Use accuracy, specificity, and sensitivity as performance indicators to assess the trained model. The efficiency of the suggested hybrid model may be shown by comparing these findings with those of standard approaches.

3.4 Evaluation metrics

Accuracy: Considers both positive and negative predictions to measure the model's overall accuracy.

$$Accuracy = (TP + TN)\ /\ (TP + TN + FP + FN)$$

Sensitivity / Recall: Measures model's ability to correctly identify fraudulent transactions.

$$Sensitivity = TP/(TP + FN)$$

Specificity: This statistic reveals the model's accuracy in detecting legitimate transactions and its capability to avoid false positives.

$$Specificity = TN/(TN + FP)$$

4. Results and Discussion:

This section presents results of proposed approach and comparison with other techniques. The dataset used in the present work is very large and imbalanced consisting of more than 2lakh instances. The dataset used in the present work has 284315 genuine transactions and fraudulent transactions are only 492. Random sampling is done to select a subset representative of the complete dataset. In random sampling every instance has an equal opportunity of getting selected. As the dataset used is imbalanced, i.e. number of genuine transactions is large as compared to fraudulent transactions the subset generated after random sampling is also imbalanced. Some technique needs to be used for overcoming this imbalance. Present research work has used SMOTE technique to handle class imbalance issue. SMOTE is an advanced technique for oversampling the minority class in an imbalanced dataset. SMOTE addresses class imbalance, improves learning for the minority class and prevents overfitting, hence enhancing model performance on minority class and improving model generalization.

Hybrid Approach (ANN + PSO + ACO):

ANN: The base model used for classification.

PSO: PSO is used to optimize certain parameters of ANN, like weights and biases, by simulating the behavior of a swarm of particles that search for optimal configuration.

ACO: ACO is used to fine-tune parameters, like batch size and learning rate, to enhance the training performance and reduce the loss.

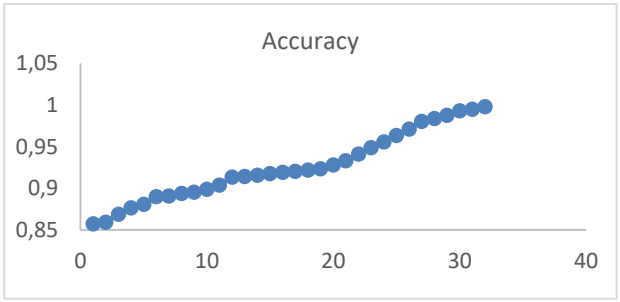
Optimized Hyperparameters: The model was trained for 35 epochs, and this was determined to be the optimal number. The batch size of 16 was optimized using a hybrid approach involving PSO and ACO. Each epoch represents a full pass through the dataset. The model uses an optimized batch size of 16, which is consistent throughout the training process. This batch size helped achieve the best performance during training and validation.

The confusion matrix given below in table 2 shows the model's predictions. Positive class denotes genuine transactions and negative class denotes fraud transactions. The confusion matrix indicates that the model is making accurate predictions with only two wrong predictions. The combination of the optimization techniques ACO and PSO leads to improved performance, achieving high accuracy, sensitivity, specificity, and F1-score. The model performs well both in training and validation, with a strong ability to correctly classify both positive and negative cases, and it generalizes well to unseen data. Combining PSO and ACO allows for more efficient hyperparameter tuning, resulting in a model that achieves higher accuracy, faster convergence, and better generalization.

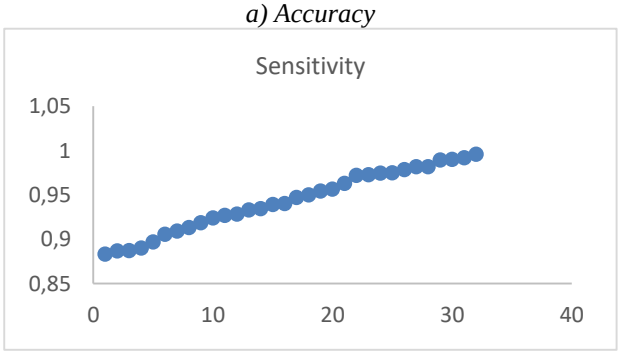
Table 2. *Confusion Matrix for Hybrid Approach*

	Class 1	**Class 2**
Class 1	510	0
Class 2	2	488

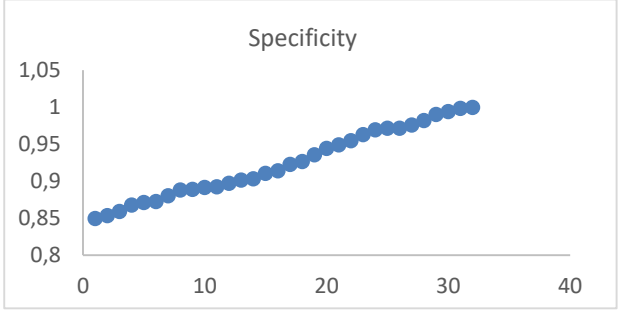
As the training progresses, the accuracy increases indicating that the model is learning effectively. The training accuracy is 100% in final epochs, which shows that the model is performing very well on the training data. The validation accuracy stabilizes at 99.80% in the final epochs, showing that the model generalizes well to unseen data and 99.8% of the predictions are correct. Sensitivity is 99.59% indicating that the model has a high rate of detecting positive cases. The specificity is 100% meaning there are no false positives, and the model correctly identified all negative cases. All cases of fraud transactions are correctly identified by proposed model. Figure 3 shows the epoch wise performance of proposed approach.



a) Accuracy



b) Sensitivity



c) Specificity

Figure 3. *Epoch wise comparison*

Figure 3.a shows the accuracy comparison. It can be seen from the graph that as the number of epoch increases, there is an increase in the accuracy. When epochs are less, accuracy is low. After 30 epochs, accuracy stabilizes and we get an accuracy of 99.8% for 32 epochs. Figure 3.b shows the comparison of recall or sensitivity. For 32nd epoch sensitivity of 99.59% is achieved. Figure 3.c shows the specificity of the proposed model in each epoch. It depends on how effectively the fraud transactions are detected by the proposed approach. Proposed approach had a specificity of 100%, i.e., the model is able to detect all fraud transactions effectively. In initial epochs, specificity is quite low and keeps on increasing with number of epochs. Proposed model is able to perform efficiently with good performance in terms of accuracy, specificity and sensitivity.

4.1 Comparative Analysis:

For analysing the performance of the proposed hybrid approach on given dataset, a comparative analysis is done. The techniques used for comparison are:

1. ANN on randomly sampled dataset
2. ANN on class balanced dataset
3. ANN+PSO on class balanced dataset.
4. ANN+ACO on class balanced dataset.

Table 3 depicts the performance of all the techniques. Value of true positives, true negatives, false positives and false negatives is given. In first technique class balancing is not done and random sampling is done which selects a small subset from the complete dataset. Number of fraud transactions selected is very less and hence can lead to overfitting. To overcome the issue of overfitting, SMOTE has been used to handle class imbalance issue. Second row of the table shows the results after class balancing. SMOTE uses oversampling for the minority class in an imbalanced dataset. As can be seen more records for fraud transactions are added to balance the dataset. It addresses class imbalance, improves learning for the minority class and prevents overfitting. In third technique, PSO is used with ANN. The use of PSO helped improve the ANN by optimizing its hyperparameters (weights) for better performance. Last technique used for comparison is ANN with ACO. ACO was used to fine-tune hyperparameters to enhance the performance of the ANN, leading to optimal results in terms of predictive accuracy. The batch size of 16 was determined to be the most effective using ACO, which helps optimize the learning rate to enhance model performance.

Table 3. *Predictions made by various techniques*

	TP	FP	FN	TN
ANN on randomly sampled dataset(1)	508	0	33	92
ANN on class balanced dataset(2)	504	3	37	456
ANN+PSO on class balanced dataset(3)	506	4	29	461
ANN+ACO on class balanced dataset(4)	510	0	11	479
ANN+ACO+PSO (Proposed model)	510	0	2	488

Comparison of Various Parameters

The Hybrid Approach (ANN + PSO + ACO) outperforms other methods across all parameters. It achieves the highest accuracy, sensitivity and specificity showing that combining ANN with both PSO and ACO optimizations leads to significant improvements in both model performance and generalization. Figure 4 presents comparison of various techniques Specificity measures the ability of the model to correctly identify negative instances. ANN had a specificity of 100%, meaning the model was able to correctly classify all negative cases. Class Balancing led to decrease in specificity. ANN and PSO classified 99.22%, negative instances correctly. ANN and ACO, had a specificity of 100%, demonstrating that ACO optimization successfully preserved the model's ability to identify all negative instances. The Hybrid Approach achieved perfect specificity at 100%, highlighting the effectiveness of combining these three methods in maintaining high performance in correctly identifying negative cases. Sensitivity measures the ability of the model to correctly identify positive instances. In dataset used, the transactions without fraud are labeled as ‘positive’ and fraudulent transactions are labeled as

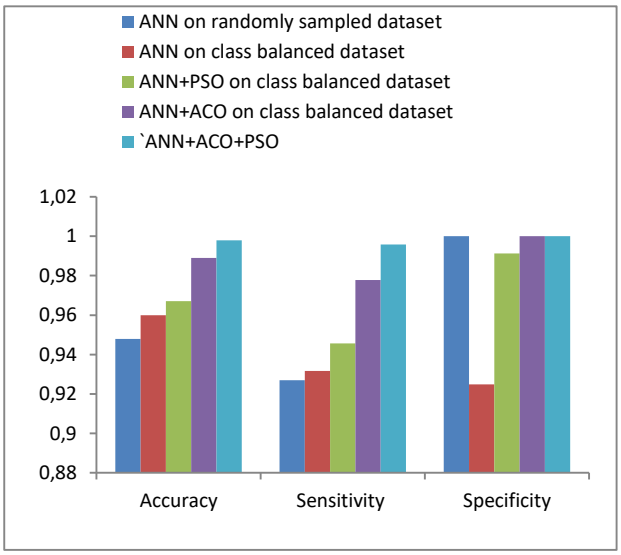


Figure 4. *Comparison of accuracy, sensitivity and specificity*

'negative'. ANN without class balancing reported a sensitivity of 92.70% but when Class Balancing was applied sensitivity improved. With ANN and PSO, sensitivity improved to 94.57%, reflecting that the PSO optimization helped the model in identifying true positives more effectively. ANN and ACO further boosted sensitivity to 97.78%, showcasing the effectiveness of ACO in enhancing the model's performance. Finally, the Hybrid Approach (ANN + PSO + ACO) achieved an impressive sensitivity of 99.59%, indicating that the combination of all three techniques led to optimal detection of positive cases.

Accuracy of the model is one of the key indicators of its overall performance. ANN used without class balancing gave an accuracy of 94.79% which increased after class balancing to 96%, indicating that balancing the dataset helped improve model performance. Further optimization ANN using PSO resulted in slight improvement in accuracy, showing that PSO helped in tuning the model for better performance. Using ACO with ANN accuracy improved reaching 98.90%, emphasizing the positive effects of ACO. Finally, the hybrid proposed approach (ANN + PSO + ACO) achieved an accuracy of 99.80%, demonstrating that ACO and PSO helped in optimizing the model for better performance.

5. Conclusion

In conclusion, the Hybrid Approach consistently outperforms other models across all accuracy parameters. It achieves the highest accuracy, sensitivity, and specificity demonstrating that the combined use of ANN, PSO, and ACO results in an optimized model. The sequential improvements in each metric reflect how the introduction of each optimization technique, PSO and ACO, improves the model's overall ability to detect both positive and negative instances, leading to optimal performance. The model has a high accuracy rate and specificity. However, the sensitivity could be improved depending on the application. The model has shown improved generalization to the validation set after class balancing. It has achieved high accuracy (96%) and sensitivity (92.49%). This is likely due to class balancing, which helps the model handle imbalanced datasets by adjusting its focus on the minority class. The confusion matrix shows fewer false positives and false negatives, indicating the model's reliability in distinguishing between positive and negative classes. The use of PSO, a nature-inspired optimization technique, likely improved the ANN by optimizing its hyperparameters for better performance. Overall, the model is well-suited for applications where both positive and negative detection is critical. An ANN optimized with ACO has been trained to classify a dataset with optimized batch size of 16. The model performs excellently, with high accuracy, recall and specificity. ACO fine-tunes hyperparameters, to enhance model performance. The training process shows a 100% accuracy and a validation accuracy of 99.80%. The hybrid approach combines ANN, PSO, and ACO to achieve high accuracy, sensitivity, specificity, and F1-score. The model's overall accuracy is 99.80%, with a sensitivity of 99.59%, specificity of 100%, and a F1-score of 99.80%. This hybrid approach allows for more efficient hyperparameter tuning, resulting in higher accuracy, faster convergence, and better generalization. This study has future scope in several possible ways that might increase usefulness along with efficacy of the suggested hybrid PSO ACO model in case of CCF detection. Model can be used in more general financial system to manage more complicated and varied datasets including many kinds of fraud patterns across multiple sectors. Furthermore other optimization methods may be applied to improve performance and adaptability of the model. Integration of real-time data processing capabilities is another exciting direction for future research as it enables the model to identify fraud as transactions take place, which is very vital in a financial world.

Author Statements:

- **Ethical approval:** The conducted research is not related to either human or animal use.
- **Conflict of interest:** The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper
- **Acknowledgement:** The authors declare that they have nobody or no-company to acknowledge.
- **Author contributions:** The authors declare that they have equal right on this paper.
- **Funding information:** The authors declare that there is no funding to be acknowledged.
- **Data availability statement:** The data that support the findings of this study are available on request from the corresponding author. The data are not publicly available due to privacy or ethical restrictions.

References

[1] El Hlouli, F. Z., Riffi, J., Mahraz, M. A., Yahyaouy, A., El Fazazy, K., & Tairi, H. (2024). Weighted

binary ELM optimized by the reptile search algorithm, application to credit card fraud detection. *Multimedia Tools and Applications*. 83(39);86383–86404. https://doi.org/10.1007/s11042-024-19508-x

[2] Amin, A., Anwar, S., Adnan, A., Nawaz, M., Howard, N., Qadir, J., Hawalah, A., & Hussain, A. (2016). Comparing oversampling techniques to handle the class imbalance problem: A customer churn prediction case study. *IEEE Access.* 4, 7940–7957. https://doi.org/10.1109/access.2016.2619719

[3] Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C., & Bontempi, G. (2017). Credit card fraud detection: A realistic modeling and a novel learning strategy. *IEEE Transactions on Neural Networks and Learning Systems.* 29(8);3784–3797. https://doi.org/10.1109/tnnls.2017.2736643

[4] Panigrahi, S., Kundu, A., Sural, S., & Majumdar, A. K. (2009). Credit card fraud detection: A fusion approach using Dempster–Shafer theory and Bayesian learning. *Information Fusion.* 10(4);354–363. https://doi.org/10.1016/j.inffus.2008.04.001

[5] Rufai, K. I., Usman, O. L., Muniyandi, R. C., & Oyinkanola, L. O. (2021). Modelling Credit Card Payment Fraud Detection System For Financial Institutions In Nigeria Using An Improved Firefly Algorithm. *International Journal of Information Processing and Communication* 11(1);9–25.

[6] Manokaran, J., Vairavel, G., & Vijaya, J. (2023, September 15). A novel set theory rule-based hybrid feature selection technique for efficient anomaly detection system in IoT edge. *In 2023 International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security (iQ-CCHESS).* 1–6. https://doi.org/10.1109/iq-cchess56596.2023.10391717

[7] Jena, J. J., Pandey, M., Rautaray, S. S., & Jena, S. (2021). Evolutionary algorithms-based machine learning models. *In Trends of Data Science and Applications: Theory and Practices.* 954;91–111. https://doi.org/10.1007/978-981-33-6815-6_5

[8] Rauf, H. T., Shoaib, U., Lali, M. I., Alhaisoni, M., Irfan, M. N., & Khan, M. A. (2020). Particle swarm optimization with probability sequence for global optimization. *IEEE Access.* 8;110535–110549. https://doi.org/10.1109/access.2020.3002725

[9] Whitrow, C., Hand, D. J., Juszczak, P., Weston, D., & Adams, N. M. (2009). Transaction aggregation as a strategy for credit card fraud detection. *Data Mining and Knowledge Discovery*, 18;30–55.

[10] Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. *Decision Support Systems.* 50(3);559–569. https://doi.org/10.1007/s10618-008-0116-z

[11] Phua, C., Lee, V., Smith, K., & Gayler, R. (2010). A comprehensive survey of data mining-based fraud detection research. *Artificial Intelligence Review*. 34(4), 321–344. https://doi.org/10.48550/arXiv.1009.6119

[12] Kocyigit, E., Korkmaz, M., Sahingoz, O. K., & Diri, B. (2024, July 12). Enhanced feature selection using genetic algorithm for machine-learning-based phishing URL detection. *Applied Sciences.* 14(14), 6081. https://doi.org/10.3390/app14146081

[13] Saheed, Y. K., Salau-Ibrahim, T. T., Abdulsalam, M., Adeniji, I. A., & Balogun, B. F. (2024, August 1). Modified bi-directional long short-term memory and hyperparameter tuning of supervised machine learning models for cardiovascular heart disease prediction in mobile cloud environment. *Biomedical Signal Processing and Control.* 94, 106319. https://doi.org/10.1016/j.bspc.2024.106319

[14] Chalabi, N. E., Attia, A., Bouziane, A., Hassaballah, M., & Akhtar, Z. (2022, September 4). Recent trends in face recognition using metaheuristic optimization. *In Handbook of Nature-Inspired Optimization Algorithms: The State of the Art.* 85–112. https://doi.org/10.1007/978-3-031-07516-2_5

[15] Rao, S., Verma, A. K., & Bhatia, T. (2021, December 30). A review on social spam detection: Challenges, open issues, and future directions. *Expert Systems with Applications.* 186, 115742. https://doi.org/10.1016/j.eswa.2021.115742

[16] Nguyen, T. T., Tahir, H., Abdelrazek, M., & Babar, A. (2020). Deep learning methods for credit card fraud detection. *arXiv preprint.* https://doi.org/10.48550/arXiv.2012.03754

[17] Thennakoon, A., Bhagyani, C., Premadasa, S., Mihiranga, S., & Kuruwitaarachchi, N. (2019, January 10). Real-time credit card fraud detection using machine learning. *In 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence).* 488–493.

[18] Mienye, I. D., & Jere, N. (2024, July 11). Deep learning for credit card fraud detection: A review of algorithms, challenges, and solutions. *IEEE Access.*

[19] Asha, R. B., & KR, S. K. (2021). Credit card fraud detection using artificial neural networks. *Global Transitions Proceedings.* 2(1);35–41. https://doi.org/10.1109/access.2024.3426955

[20] Sahin, Y., & Duman, E. (2011). Detecting credit card fraud by ANN and logistic regression. *In Proceedings of the 2011 International Symposium on Innovations in Intelligent Systems and Applications.* 315–319. https://doi.org/10.1109/inista.2011.5946108

[21] Arora, S., & Kumar, D. (2017). Hybridization of SOM and PSO for detecting fraud in credit card. *International Journal of Information Systems in the Service Sector.* 9(3);17–36. https://doi.org/10.4018/ijisss.2017070102

[22] Prusti, D., Rout, J. K., & Rath, S. K. (2023). Detection of credit card fraud by applying genetic algorithm and particle swarm optimization. *In Machine Learning, Image Processing, Network Security and Data Sciences: Select Proceedings of 3rd International Conference on MIND 2021. Springer Nature Singapore.* 357–369. https://doi.org/10.1007/978-981-19-5868-7_27

[23] Ghodsi, M., & Saniee Abadeh, M. (2017). Fraud detection of credit cards using neuro-fuzzy approach based on TLBO and PSO algorithms. *Journal of Computer & Robotics.* 10(2);57–68.

[24] Yılmaz, A. A. (2023). A machine learning-based framework using the particle swarm optimization algorithm for credit card fraud detection. *Communications Faculty of Sciences University of Ankara Series A2-A3 Physical Sciences and Engineering*. 66(1);82–94. https://doi.org/10.33769/aupse.1361266

[25] Singh, A., Jain, A., & Biable, S. E. (2022). Financial fraud detection approach based on firefly optimization algorithm and support vector machine. *Applied Computational Intelligence and Soft Computing.* 2022(1), 1468015. https://doi.org/10.1155/2022/1468015

[26] Kamaruddin, A. S., Hadrawi, M. F., Wah, Y. B., & Aliman, S. (2023). An evaluation of nature-inspired optimization algorithms and machine learning classifiers for electricity fraud prediction. *Indonesian Journal of Electrical Engineering and Computer Science.* 32(1);458–467. https://doi.org/10.11591/ijeecs.v32.i1.pp468-477

[27] Btoush, E. A. L. M., Zhou, X., Gururajan, R., Chan, K. C., Genrich, R., & Sankaran, P. (2023). A systematic review of literature on credit card cyber fraud detection using machine and deep learning. *PeerJ Computer Science*. 9, e1278. https://doi.org/10.7717/peerj-cs.1278

[28] Guo, Y., He, J., Xu, L., & Liu, W. (2019). A novel multi-objective particle swarm optimization for comprehensible credit scoring. *Soft Computing*. 23;9009–9023. https://doi.org/10.1007/s00500-018-3509-y

[29] Jimbo Santana, P., Lanzarini, L., & Bariviera, A. F. (2019). Variations of particle swarm optimization for obtaining classification rules applied to credit risk in financial institutions of Ecuador. *Risks*. 8(1);2. https://doi.org/10.3390/risks8010002

[30] Emambocus, B. A. S., Jasser, M. B., & Amphawan, A. (2023). A survey on the optimization of artificial neural networks using swarm intelligence algorithms. *IEEE Access*. 11, 1280–1294. https://doi.org/10.1109/access.2022.3233596

[31] Waffa Abdul-Abbas Shehab, Haiffa Muhsan B. Alrikabi, Abeer A. Abdul–Razaq, Huda Karem Nasser, & Asaad Shakir Hameed. (2024). Comparative Analysis of New Solutions for the Capacitated Vehicle Routing Problem Against CVRPLIB Benchmark. *International Journal of Computational and Experimental Science and Engineering*, 10(4). https://doi.org/10.22399/ijcesen.626

[32] I. Bhuvaneshwarri, M. Maheswari, C. Kalaivanan, P. Deepthi, Tatiraju V. Rajani Kanth, & V. Saravanan. (2025). Hybrid Swarm Intelligence-Based Neural Framework for Optimizing Real-Time Computational Models in Engineering Systems. *International Journal of Computational and Experimental Science and Engineering*, 11(1). https://doi.org/10.22399/ijcesen.1001