ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec932

Meta-Heuristic Approach for Credit Card Fraud Detection Using Flower Pollination Algorithm with Spiking Neural Network (FPA+SNN)

Abubakar Umar[1,3]; Salisu Mamman Abdulrahman[2]; Sani Danjuma[3]; Mohammed Kabir Daud[1,3]; Musa Adamu Wakili[1]; Abdulmajid Babangida Umar[3]; Haris Abdullahi Shehu[4]

[2,4](Member Ieee)

[1]Abubakar Tafawa Balewa University, Bauchi, Bauchi State Nigeria
[2]Kano State University Science and Technology, Wudil, Kano State, Nigeria
[3]Yusuf Maitama Sule University, Kano State, Nigeria
[4]Victoria University of Wellington, 6011 Wellington, New Zealand

Publication Date: 2025/12/23

Abstract: The advancement of electronic banking has increased the acceptance and use of credit card rendering it as one of the most universally accepted method of payment globally. The incidence of transaction fraud required an effective detection technique to protect customers and financial companies from being trapped by fraudsters. The process of fraud detection, which pertains to the recognition of illicit activities within banking systems, is critical for ensuring financial stability, protecting customer interests, managing institutional reputation, and complying with regulatory requirements. The methodologies encompassing machine learning and deep learning have seen extensive application in addressing issues related to credit card fraud; however, a significant proportion of these methodologies encounter challenges, including erroneous classification and false positives, among other complications. Recent research shows that fraudsters persist in employing novel methodologies in their illicit activities by altering the characteristics or trends in their deceptive practices, thereby rendering fraudulent transactions indistinguishable from genuine ones in an effort to evade detection by current detection mechanisms. To optimize model precision and enhance fraud detection using deep learning feature selection (FS) is of paramount importance. This will alleviate the adverse impacts of noisy, irrelevant and redundant attributes present within the dataset. This research work proposed a new approach that uses Flower Pollination Algorithm (FPA) with Spike Neural Network (SNN) a deep learning technique called FPA-SNN for credit card fraud detection. Four datasets were used to implement the proposed approach, two of the datasets are highly unbalanced with a <1% positive class. To improve classification accuracy and precision we used Synthetic Minority Oversampling Technique (SMOTE) to solve the imbalance problem in the datasets. Realizing that the vast majority of studies in credit card fraud detection uses very few performance metrics for evaluating various machine learning and deep learning algorithms, we utilized multiple evaluation metrics; Accuracy, Precision, Recall, F1-score, the area under curve and the receiver operating characteristic curve (AUC_ROC), and Matthew's Correlation Coefficient (MCC) to test and evaluate the performance of our proposed model. Our Proposed model performed significantly well with highest MCC greater than 97 percent, as well as AUC-ROC greater than 99.9 percent which shows how robust the model is in feature selection and classification.

Keywords: *Credit Card Fraud Detection, Nature Inspired Algorithms, Deep Learning, Machine Learning, Flower Pollination Algorithm (PFA), Spike Neural Network (SNN), Feature Selection and Classification.*

How to Cite: Abubakar Umar; Salisu Mamman Abdulrahman; Sani Danjuma; Mohammed Kabir Daud; Musa Adamu Wakili; Abdulmajid Babangida Umar; Haris Abdullahi Shehu (2025) Meta-Heuristic Approach for Credit Card Fraud Detection Using Flower Pollination Algorithm with Spiking Neural Network (FPA+SNN). *International Journal of Innovative Science and ResearchTechnology*,10(12), 1357-1373. https://doi.org/10.38124/ijisrt/25dec932

I. INTRODUCTION

Companies and businesses have witnessed the digital revolution, allowing customers to browse and purchase things from the comfort of their homes [1]. There are several advantages which E- commerce platforms offer and this includes product and price comparison, cost reduction,

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec932

quicker purchase processing, customer flexibility, quicker market/buyer reaction, and many payment options. In pandemic situations, when governments enforce stay-at-home and lockdown policies to reduce human movement, e-commerce grew in popularity and importance. The period has led to rise in demand for online purchasing, including products and daily essentials like food and medication. Research revealed that worldwide e-commerce sales increased 27.6% in 2020 and also in 2021 increased by 14.3%, reaching almost $5 trillion. These statistics continue to grow slightly in 2022 and 2023 and now the e-commerce market is worth $6.9 trillion globally with expected sales to grow 9.8% by the end of 2024. The Nigerian e-Commerce market contributed to the worldwide growth rate of about 10.4% in this year 2024 (ECDB, 2024). This transformation from traditional methods of buying and selling to online continues to increase as people continue to adapt the use of online channels for almost all their daily transactions. [2] noted that due to the increase in an online transaction and a high volume of money it involves, draws the attention of fraudsters which can cause tremendous loss of money. E-commerce involves both online shopping and online payment of bills and taxes in which credit cards are very useful. It's not just convenient, but also time-saving. Many find payment using credit cards much more convenient in shops than cash [3]. Nowadays, online payment methods are widely used due to the rapid increase in non-cash electronic transactions. Credit cards are one of the electronic payments' methods and about 51% of transactions are reported using card-based payments [4]. It became clear that the increased reliance on e-commerce and the new methods of payment it offers has helped people in many different ways, especially now that the world is moving toward cashless society. In 2023, many countries begin to put more pressure on cashless transactions, and that attracts major risk of credit card fraud in budgetary exchanges. On the other hand, the online transaction is facing a lot of challenges from cybercriminals and fraudsters which are described as cyber fraud such as identity theft, phishing, credit card fraud etc.

Online payments represent a primary focal point for fraudulent activities, particularly in cases involving cards, where the absence of the physical card is inconsequential. There are typically two distinct categories of card payments: card present transactions, involving the physical card for purchase, and card not present transactions, where the card details suffice without the need for the physical card. The latter, known as card not present transactions, serves as the preferred mode for ecommerce, requiring solely the card details that can be securely stored in digital format. Nonetheless, this approach also presents an advantageous opportunity for fraudsters to exploit, given the challenges faced by sellers in authenticating the identity of purchasers. Additionally, alternative payment mechanisms like digital wallets and BNPL (Buy Now Pay Later) are susceptible to illicit activities, including Account Takeover (ATO) endeavours. It is also good to highlight the other technological terms such as 'dark web'; The dark web, a corner of the Internet where criminals can interact without being traced, is often where fraudsters buy and sell card and account details, and share information on how to go about committing fraud. Some of this information can include what tools to use to commit fraud and the best ways of going undetected. [5] noted that, recent development in information and communication technologies have created a highly connected world. Different types of communication platforms are available which offer a large volume of information that is easily accessible. This development opened another opportunity for fraudsters and attackers to hide their malicious activities within the mountains of data. With the persistent growth of such communication platforms, opportunities for fraudsters to manipulate them for their benefits have also increased.

A study from Juniper Research reported that estimated fraud will rise from $17.5 billion in 2020 to $20 billion by 2021 and these statistics continue to increase as it is expected to rise to $7.95 trillion by 2027 [6]. Furthermore, research revealed that in 2021 there was a combined loss of $32.43 billion resulting from credit card fraud transactions, credit card companies, retailers, and consumers [7]. More recently, [8] also quoted from the report published by Nelson that in 2022 in estimated credit card fraud was $33 billion and predicted to $400 billion by the next decade. These statistics demonstrate the importance of e-commerce and the need for the financial institution to implement fraud detection and prevention systems to avoid financial losses. Currently, there are many research studies investigating different strategies to mitigate the fraud issues in e-commerce. Detecting fraudulent activities related to credit cards is increasingly impacting the quality of service, expenses, and reputation of financial institutions[9]. Consequently, the development of a robust model aimed at identifying credit card fraud is imperative for regulatory bodies, banking institutions, and clientele. The validation of transactions in advance and the identification of credit card fraud plays a pivotal role in mitigating risks for customers and curbing fraudulent activities associated with credit cards from a risk management standpoint. The process of fraud detection involves the examination of historical data to ascertain the legitimacy of a transaction [10]. In a broad context, credit card transactions may be executed through physical or digital means. Physical transactions are conducted via the presentation of the credit card during the transaction, whereas digital transactions are performed through telecommunication medium or internet platforms. Historically, enterprises or businesses have depended on rules alone to mitigate fraudulent activities. Nevertheless, this approach has caused certain complications, such as the unwarranted obstruction of numerous legitimate customers and the resultant deceleration of the banking system, among other issues. Given that individuals are employing various devices for diverse transactions, anomaly detection systems also referred to as outlier detection systems continue to encounter increasingly many challenges due to the exponential growth in online transactions and the multifaceted nature of anomaly patterns. Additionally, the occurrence of unauthorized credit card utilizations can manifest in various forms, thereby complicating the identification process [11].

Researchers have proposed a lot of techniques and models for converting fraud as there are many anti-fraud

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec932

measures that have evolved over time. However, fraudsters are always trying to find alternative ways out as there are constant developments within fraud rendering those proposed methods void. Cybercriminals always tend to be one step in advance preparing how to commit their crime by taking advantage of the account owner. They employ a combination of social engineering and technological expertise that enables them to bypass existing safeguards. The primary objective for fraudsters revolves around monetary gain, so the prime target for exploitation is a payment system. In the realm of digital transactions, obstacles such as fraud demand our attention, particularly with the emergence of innovative fraudulent schemes like 'silent fraud.' combined with weaknesses of cyber security, are contributing significantly to a mix of attack courses. Having a clear understanding of fraud is crucial to strengthening the protection whilst credit cards safe from unwanted exploitation.

Nowadays, the occurrence of credit card fraud has emerged as one of the most intricate and significant concerns worldwide, surpassing even the preceding decades. [12] describes Credit Card Fraud (CCF) as a type of fraud in which the card owner's identity is stolen and performs an unlawful transaction using his/her credit card details. Credit card frauds are of different types such as counterfeit fraud, theft fraud, application fraud and behavioural fraud. Owing to the widespread adoption of credit cards, the proliferation of security challenges has escalated, consequently exacerbating fraudulent activities aimed at acquiring unauthorized monetary gains [13]. Unfortunately, credit card fraud is a multifaceted problem in financial services and as such it results in significant financial losses each year. Detecting credit card fraud is an ethical issue faced by credit card issuance, banks, financial institutions, companies, and mortgage companies. Developing effective fraud detection techniques is critical in order to minimize these losses. Credit card fraud detection is a vital application in the financial sector, and deep learning has appeared as a powerful tool to improve the accuracy and efficiency of fraud detection systems. Although many techniques, such as statistical methods, machine learning, big data analytics, some nature inspired algorithms etc are applied. There is a need to study and investigate the literature in order to know the state of art techniques used to combat crime on credit cards as well as their capabilities and the limitations. The target is to find out the gap from the literature so as to propose suitable techniques that will improve those existing techniques in order to reduce or stop financial loss.

- *Motivation and Challenges*

With a continued increase in the number of individuals using credit cards for online purchases, alongside the increase in adoption of cashless payment systems in many developing countries led to the increase in incidence of credit card fraud resulting in huge financial losses. Hence, to minimize the losses, it is very necessary for researchers to formulate new technique or approach that can assist financial institutions in detecting instances of credit card fraud. Many credits card fraud detection systems have been presented in the past; however, achieving consistent reliability poses considerable challenges due to the rapidly changing behaviour of both fraudsters and legitimate users. This scenario motivates us to investigate various existing credit card fraud detection techniques and strategies, which encouraged the formulation of our proposed approach based on Flower Pollination Algorithm (FPA) and Spiking Neural Networks (SNN) to provide a better way of detecting fraudulent transaction using credit card.

II. LITERATURE REVIEW

This section highlights the relevant literature on credit card fraud detection. It covers the state of art machine learning and deep learning as well as other hybrid approaches applied in credit card fraud detection. It begins with the background of the study which discussed briefly the type of credit card fraud detection. The remaining parts of this section contained a review of related works that utilized different approaches mentioned above with an addition of metaheuristics and optimization techniques applied to credit card fraud detection. Finally, the section ends with a summary of literature review table that highlighted the gaps identified in the literature which guide us in proposing new approach.

In the field of machine learning, deep learning, and artificial intelligence, credit card fraud detection continues to attract many researchers. Due to its significance to society, it has been widely studied by both researchers and practitioners through offline and field studies. Existing fraud detection models utilizing certain metrics perform well in detection rate in some cases, while in other cases, they experience certain drawbacks. Various techniques are applied to predict fraud in available transaction datasets (including imbalanced datasets). Accuracy, precision, recall, F-score, and other metric parameters, as well as the training methodologies, are investigated in this review. We briefly report the studies from these aspects in this section.

Many research works have been done to detect credit card fraud employing a wide range of innovative techniques and technologies to enhance security and protect consumers from financial losses. These techniques include traditional methods, machine learning, deep learning, evolutionary algorithms and some other hybrid techniques that combines different techniques to have better solutions [14], [15]. Previously, machine learning classification algorithms were proposed to solve credit card fraud and related problems. For example, K-Nearest Neighbors, Decision Tree (DT), Support Vector Machine (SVM), AdaBoost, (KNN), Naïve Bayes (NB), Random Forest (RF), Gradient Boosting Machines (GBM), Light Gradient Boosting Machine (LightGBM), Extreme Gradient Boosting (XGBoost), and Category Boosting (CatBoost) among others [16], [17], [18], [19]. To further improve the machine learning based model, an ensemble learning techniques were presented. The idea of an ensemble is to merge different classification models to improve the overall performance of the model. An ensemble of machine learning models of Random Forests, logistic regression and Neural Networks in-cooperated with two data resembling algorithms namely random oversampling and random under-sampling was proposed by [20]. The result revealed that Random Forest can classify normal transactions

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec932

correctly but misclassifies the fraudulent transactions, while Neural Networks can classify fraud transactions correctly but misclassify some of the transactions are normal. This implies that, the model will inherit the problem of individual classification algorithms. Hence, this might not provide the best possible solution. Other techniques that utilized neural network was proposed for tackling the issues of credit card fraud detection for example, the work of [21]. In the same vein, [22] proposed a model for credit card fraud detection which utilized Convolutional Neural Networks (CNN). In their work, they tried to provide an additional layer to the model where twenty (layers) were used for extracting features and perform classification of credit card transactions as fraudulent or non-fraudulent. The model achieved significant results compared with traditional machine earning model such as SVM, KNN, XGBoost among others especially in the case of imbalance dataset. [23] proposed a hybrid deep learning technique that combines an auto encoder and convolutional neural network (CNN) for credit card fraud detection using artificial intelligent (AI).

In 2022 [24] conducted an intensive review and pointed out some limitation of machine leaning such as unable to yield high accuracy due to data imbalance and heterogeneity. In order to enhance the capability of machine learning to detect fraudulent transactions, they proposed hybrid approach based on real-time that uses ANN for effective detection alongside with federated learning framework to provide data privacy. But one of the limitations of their proposed model is that, since that model will be training at individual server before combine at the central server, which means data is not shared centrally then there is every possibility that the trained model will learn patterns decoded by hackers. Another challenge is that real-life deployment is not feasible because banks and financial institutions have different rules and regulations that govern their operations. Similar approach was presented by [25] in which federated detection system was employed on European credit card transaction dataset. In the experiment, Accuracy, precision and recall were used as parameters for accessing the performance of the model. The result revealed that proposed method achieved 97% accuracy, with 87.5% as precision and 88.9% as recall. However, some of the model's the problem is; privacy is an issue where sensitive data are likely to leak through global parameters access and as such federated transfer learning was recommended. There is room for improvement on the model performance. Federate learning was also presented by [26] using CNN based on resembling method to improve efficiency and address imbalanced class issues. Moreover, deep learning techniques such as long-short term memory (LSTM) and it is variants were proposed by many researchers; amongst which include [27], [28],in[29] amongst others.

More recently, some optimization approaches were used to deal with issues of imbalance datasets so as to produce a reliable model for credit cards fraud detection. Some of the proposed approaches include Hybrid Grey Wolf Optimizer (GWO) with Isolation Forest (IF) algorithms was presented by [11] while Boosted Grey Wolf Optimizer (BGWO) algorithm was proposed by[31] and Brown Bear Optimization Algorithm (BBOA) by [32]. Despite all these efforts, the problem of credit cards continues and it continued to cause great loss of money[8]; as such there is a need to further investigate and provide suitable technique that can be able to protect both individuals and financial industries.

III. PROPOSED MODEL

In this research, we proposed Flower Pollination Algorithm (FPA) with Spiking Neural Network (SNN) as a new technique due its advantages of not being trap at the local optima. FPA is meant to conduct feature selection and then SNN to perform classification based on the given dataset (s). Figure 1 shows the proposed model. The flower pollination algorithm (FPA) was developed by Xin-She Yang in 2012. This algorithm is mimicking the nature and the of flower pollination. It is demonstrated a promising result in feature selection problems especially when dealing with high dimensional data. Some of the researches that utilized FPA include[33] [34], [35] among others.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec932

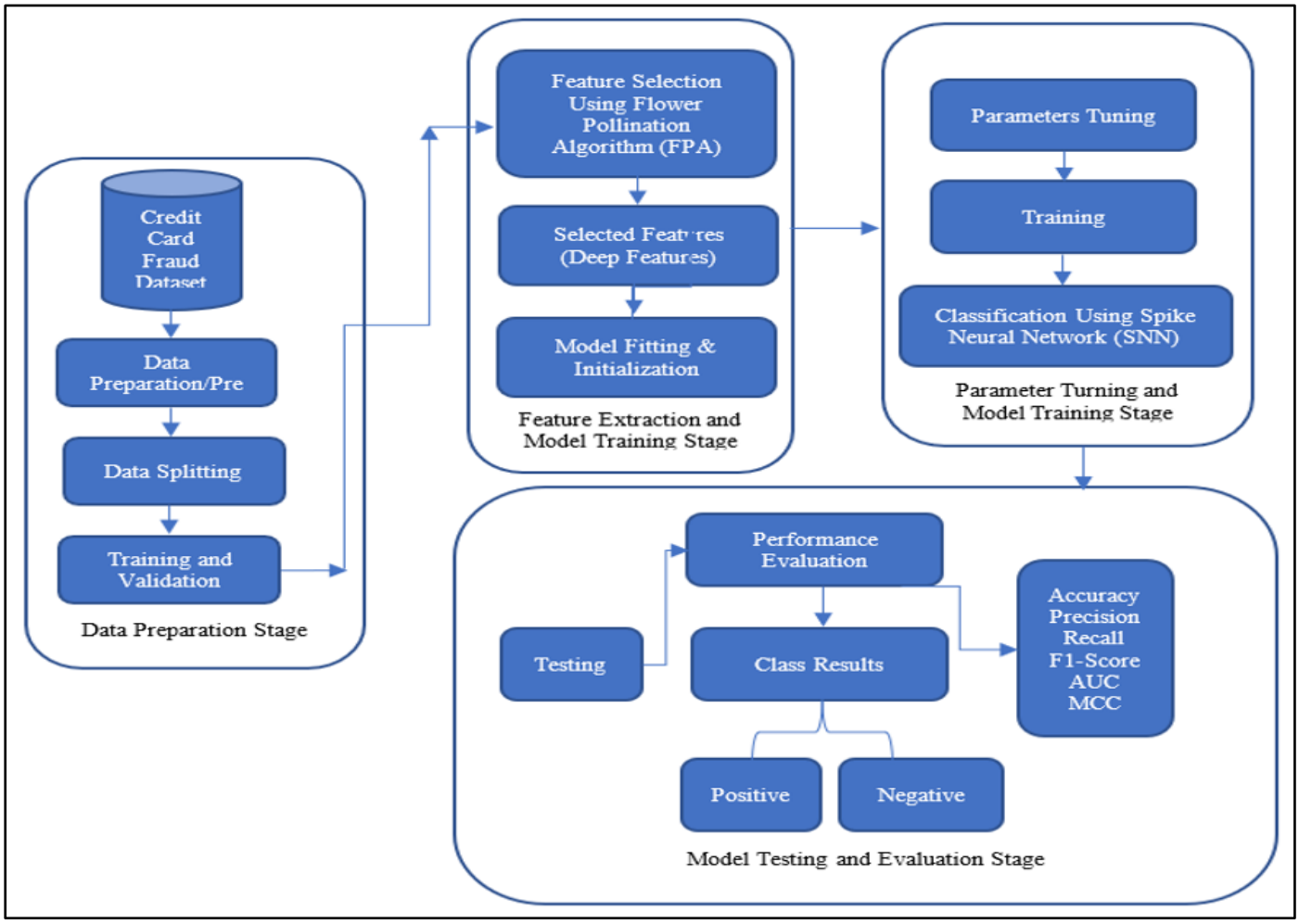

Fig 1 Proposed FPA+ SNN Model

```
Algorithm1: Flower Pollination Algorithm (FPA)
Input:
f(x)          // Objective (fitness) function
N             // Population size (number of flowers)
MaxIter       // Maximum number of iterations
p             // Switch probability (0 ≤ p ≤ 1)
γ             // Scaling factor
λ             // Lévy distribution parameter
Output:
g_best        // Best solution found
Begin
Initialize population Xi (i = 1, 2, ..., N) randomly
Evaluate fitness f(Xi) for all Xi
Identify the current best solution g_best
For iter = 1 to MaxIter do
For i = 1 to N do
Generate random number r ∈ [0, 1]
If r < p then
// Global Pollination (Lévy Flight)
L ← Lévy(λ)
Xi_new ← Xi + γ × L × (g_best − Xi)
Else
// Local Pollination
Select two random solutions Xj and Xk, j ≠ k ≠ i
ε ← random number ∈ [0, 1]
Xi_new ← Xi + ε × (Xj − Xk)
End If
```

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec932

```
Evaluate fitness f(Xi_new)
// evaluate new solution
If f(Xi_new) < f(Xi) then // if new solution is better then update them in the
population
Xi ← Xi_new
End If
// Update global best
If f(Xi) < f(g_best) then
g_best ← Xi
End If
End For
End For
Return g_best// return global best
End
```

Fig 2 Pseudo Code of the Proposed Flower Pollination Algorithm (Source: [36])

➢ *Algorithm 2: Spike Neural Network*

Spiking Neural Networks (SNNs) are regarded as the third generation of neural networks with an ability to get beyond ANN bottlenecks. It is dynamic and excels in activities such as speech, computer vision, robotics applications, and dynamic picture identification. One possible remedy for the problem of energy consumption is SNN. Similar to neurons in actual neural networks, neurons in SNNs exchange discrete electrical impulses called spikes while operating constantly. Three types of training methods exist for SNNs: supervised learning with gradient descent and spike backpropagation, unsupervised learning with local learning rules at the synapse (such as spike-time-dependent plasticity), and reinforcement learning with reward/error signal using reward modulated plasticity [37].

A spiking neural network (SNN) consists of neurons connected by synapses that transmit information through discrete spikes rather than continuous values, distinguishing it from traditional artificial neural networks. Inputs are processed over a fixed time window, requiring multiple forward passes during which presynaptic neuron activity generates synaptic currents that influence the membrane potential (Vmem) of postsynaptic neurons. When the membrane potential reaches a defined threshold (Vthresh), the neuron fires a spike and resets to its resting state (Vrest). The behavior of SNNs depends on the chosen neuron models, membrane potential dynamics, and learning rules, which vary according to network architecture and application requirements [38], [39]. Below is the pseudocode for SNN.

Algorithm2: Pseudocode for Spiking Neural Network (SNN)

```
Input:
D = {(x1, y1), (x2, y2), ..., (xN, yN}// Input spike-encoded dataset
T = simulation time window
η = learning rate
θ = neuron firing threshold
τ = membrane decay constant
W = initial synaptic weights
Output:
Trained synaptic weights W*
Begin
Initialize synaptic weights W randomly
Initialize membrane potentials V of all neurons to 0
Initialize spike trains S to 0

For each epoch = 1 to MaxEpoch do
For each training sample (x, y) in D do
Encode input x into spike trains S_in
Reset membrane potentials V
Reset neuron spikes S_out

            For time t = 1 to T do
For each neuron i do
// Integrate incoming spikes
V_i(t) ← V_i(t-1)*exp(-Δt / τ)
+ Σ_j (W_ij × S_j(t))
```

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec932

```
// Fire spike if threshold is exceeded
If V_i(t) ≥ θ then
S_i(t) ← 1
V_i(t) ← 0          // Reset after spike
Else
S_i(t) ← 0
End If
End For
End For
// Learning phase (example: supervised / STDP-based update)
For each synapse W_i,j do
ΔW_ij ← η × LearningRule(S_j, S_i, y)
W_ij ← W_ij + ΔW_ij
End For
End For
End For
Return trained weights W*

End
```

Fig 3 Pseudo Code of Spike Neural Network ([39])

In an SNN architecture, reconfigurable scalar weights represent spiking neurons and connecting synapses. As the first step in creating an SNN, the analogue input data is encoded into the spike trains using either a rate-based approach, a type of temporal coding, or population coding. Robotics, computer vision, dynamic picture recognition, and several more domains have all used SNN encoding in both supervised and unsupervised learning techniques.

IV. DATASETS

Datasets are the basic building blocks for testing the performance of any proposed model. Since models are trained based on the existing data so as to learn the patterns and make predictions on the new data that will be injected into them. In this research we utilized three (3) different datasets Namely; European cardholder's transaction dataset (2013), Anonymized credit card transactions (2023) and Simulated Credit Card Transactions generated using Sparkov (2019-2020). All the datasets are publicly available for use at Kaggle repository.

➢ *European Credit Card Transaction Dataset (ECCD) 2023*

This dataset contains the credit card transactions made by European cardholders in 2023. It contains more than 550,000 records in total, and the data has been anonymised to protect the cardholders' identities. The main objective of this dataset is to facilitate the development of fraud detection models and algorithms that can identify potentially fraudulent transactions. The characteristics of the features in this dataset are as follows:

- ID: This represents a unique identifier used to identify each transaction
- V1-V28: Represents features that are anonymous and reflect different transaction attributes (e.g., time, location, etc.)
- Amount: This represents the amount transact
- Class: Binary label that indicates (1) if the transaction is fraudulent or (0) if the transaction is non-fraudulent

➢ *European Credit Card Transaction Dataset (ECCD) 2013*

The initial dataset includes credit card transactions done by cardholders throughout Europe in September 2013. Out of the 284,807 transactions that were recorded in a two-day period, 492 transactions were fraudulently registered, according to this information. Because of the extreme imbalance in the dataset, 0.172% of all transactions belong to the positive class (frauds). Its sole input variables are numbers that come from a Principle Component Analysis (PCA) transformation. Unfortunately, the original characteristics and other background information regarding the data cannot be disclosed owing to confidentiality concerns. Features are denoted by V1, V2…V28, which are the results of principal component analysis (PCA) transformations. "Time" and "Amount" are the only two characteristics that PCA has not changed. The seconds that pass between each transaction and the initial transaction are contained in the feature "Time.". The response variable feature is called "Class," has a value of 1 in the event of fraud and 0 in all other cases. Evidence from the research proved that many researches utilized this dataset, amongst which including [40],[41], [42] and [32].

➢ *Australian Credit Card Transaction Dataset*

The UCI Machine Learning Repository will be the source of the Australian credit dataset. There are 690 credit applications in this dataset, and each one is distinguished by 15 characteristics. Of these, one binary class label reflects the outcome of the credit application (1 for approval and 0 for

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec932

refusal), and six are numerical attributes and eight are categorical. With 307 cases of granted applications and 383 instances of refused applications, the dataset shows an imbalance in the distribution of classes. This dataset was recently utilized by[32].

➢ *Simulated Credit Card Transaction Dataset (SCCD) 2019-2020*

This dataset contains both legitimate and fraud transactions recorded within two years (that is from the duration 1st Jan 2019 - 31st Dec 2020) and it is generated using Sparkov. It covers credit cards of 1000 customers doing transactions with a pool of 800 merchants. The formation of the dataset was done using simulator which has certain pre-defined list of merchants, customers and transaction categories. A python library called "faker" was utilized, and with the number of customers, merchants were used to generated the dataset. This dataset contained 109,434 transactions, labeled as either normal or fraudulent with each transaction includes 20 features. Amon all the 109,434 transactions, only a small fraction (0.57%) were fraud transactions, while the majority class (99%) represents legitimate transactions. This problem of imbalanced is a serious issue in model development.

The realistic features of simulated credit card dataset and it is structure offers a significant insight into transaction behaviors, which make a vital resource for research in credit card fraud detection. For proper classifying the context of transactions as either legitimate or fraudulent, the following variables were used to represents the target labels for each transaction:

- Class = 1: Indicates a fraudulent transaction.
- Class = 0: Indicates a legitimate transaction.
- This dataset was utilized by many researchers among which is[31].

Table 1 Datasets Summary

S/N	Dataset Name	Number of Instances	Number of Features
1	European Credit Card, 2013	284,807	28
2	European Credit Card, 2023	550,000	30
3.	Simulated Credit Card Transaction, 2019-2020	1,852,394	20
4.	Australian Credit Card Transaction	690	15

These datasets were used for model testing our proposed model. Previous discussion under literature review testifies that the chosen datasets were utilized previously by many researchers. This motivated us to use the same dataset as a benchmark for testing our model. These datasets need to undergo some pre-processing before injecting them into model for experimental execution.

It is noted that two of the datasets namely; European Credit Card Transaction Dataset (ECCD) 2013 and Simulated Credit Card Transaction Dataset (SCCD) 2019-2020 suffers from severe class imbalance with a 99% negative class (non-fraud) and 1% positive (fraud). This posed a challenge that need to be tackle to get a consistent and reliable results.

V. DATA PREPARATION AND PRE-PROCESSING

At this phase, the dataset needs to be imported and then reshuffle to ensure random distribution of classes. In the next stage, unnecessary tables were dropped, then feature set (x) and target variables (y) for both training and testing datasets were defined. For SCCD 2019-2020 we dynamically identified categorical and numerical columns, then converted transaction date and time to a date time object in order to extract features (like hour, day and month). Categorical variables were then encoded using label encoder and numerical features were scaled using standard scalar. The European datasets (2013 and 2023) contains only numerical inputs variables which were obtained from PCA transformation.

All the datasets were scaled into a NumPy array for feature selection and classification. The high dimensional array representing the features to be selected when the learning algorithms are employed in order to get relevant features that form the subsets representing features with high relevance to return high classification accuracy with lower error rate.

➢ *Handling Class Imbalance with SMOTE*

The Synthetic Minority Over-Sampling Technique (SMOTE) constitutes a proficient methodological framework for mitigating the challenges posed by imbalanced class distributions, wherein it engages in the over-sampling of the minority class alongside the under-sampling of the majority class. This technique exploits the concept of k-nearest neighbors to randomly select proximate data points for the purpose of interpolation, employing a parameterization that exists within a continuum from 0 to 1. In contrast to conventional sampling techniques, SMOTE operates within the feature space as opposed to the data space, thereby yielding outcomes that exhibit enhanced precision[43]. To solve the problem of dataset imbalance on ECCD 2013 and SCCD 2019-2020 we used Synthetic Minority Oversampling Technique (SMOTE) to synthetically generate minority class instances (fraud) because undersampling leads to information loss. The resulting datasets are in a balanced of 50:5 distribution. The figures 4 and 5 shows the graphical distribution before and after SMOTE was applied.

Furthermore, the dataset was scaled using the standard and minmax technique to ensure data consistency in pre-processing. The scaled data was used to in training and testing the models.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec932

VI. PERFORMANCE EVALUATION METRICS

Every prediction or detection model must undergo performance analysis and evaluation in order to determine its advantages and disadvantages. Studies on credit card fraud detection indicate that accuracy, precision, recall (sensitivity), F1-score, area under the curve, and Matthews Correlation Coefficient (MCC) are the most often utilized metrics for model assessments [44], [45] and [46], but majority of researches used few of the aforementioned performance criteria for measuring the effectiveness of the detection models.

The particular needs and objectives of the fraud detection system determine which of the metrics should be used. To evaluate our proposed model, six (6) performance metrics i.e accuracy, precision, recall, f1-score, area under curve, and MCC are adopted as utilized by [32], [47] and several other researchers. The following equations hold true:

- Accuracy: The percentage of all transactions (fraudulent and non-fraudulent) that are accurately detected. The prediction model's error rate is also used to calculate it.

$$Accuracy\ (Acc) = \frac{TP + TN}{TP + TN + FN + PN} \quad (1)$$

- Precision (Positive Predictive Value): The percentage of fraudulent transactions that are successfully recognized among all those that are flagged as fraudulent. It is computed as follows:

$$Precision = \frac{True\ Positives}{True\ Positives\ +\ False\ Positives} \quad (2)$$

- Recall: The percentage of real fraudulent transactions that are accurately discovered is often referred to as Sensitivity or True Positive Rate. It is computed as follows:

$$Recall = \frac{True\ Positives}{True\ Positives\ +\ False\ Negatives} \quad (3)$$

- F1-Score: A balance between recall and accuracy calculated as the harmonic mean of the two measures. It is computed as follows:

$$F1 - Score = 2\ x\ \frac{Precision\ x\ Recall}{Precision\ +\ Recall} \quad (4)$$

- Operating characteristic curve of the receiver and area under the ROC curve (AUC_ROC): This measure is employed to assess how well a binary classification model performs. It offers an extensive assessment of the model's capacity to discriminate between legitimate and fraudulent transactions at different threshold values.

- Matthews Correlation Coefficient (MCC): This serves as a quantifiable metric for assessing the correlation between predicted and actual samples (it is used to assess how well binary classifications are made). False Positives (FP), False Negatives (FN), True Positives (TP), and True Negatives (TN) are all considered. It has a range of -1 to +1, where +1 denotes an exact prediction, a value of 0 denotes performance inferior to random predictions, and -1 denotes a complete discrepancy between the prediction and the observation. The MCC is regarded as a robust and all-encompassing metric, widely acknowledged as the most effective for addressing binary classification challenges. True Positive Rate (TPR) also constitutes a critical metric, particularly in the context of fraud detection, as an elevated TPR correlates with an enhanced capacity to identify fraudulent data (Zhu 2020).. It is computed as follows:

$$MCC = \frac{TP\ x\ TN - FP\ x\ FN}{\sqrt{(TP + FP)(TP + FN)(TN + FP)(TN + FN)}} \quad (5)$$

Table 2 Parameters Configurations

S/N	Algorithm	Parameters
1	Flower Pollination Algorithm	n_Flowerers = 20, Max-iteration= 30 and population (p) = 0.8,
2	Spike Neural Network	Learning rate = 0.001, Epoch = 30, Batch size =32 Hidden dimension = 128

Where:

- ✓ *n_flowers:* number of candidate solutions
- ✓ *max_iter:* maximum number of iterations
- ✓ *p:* switch probability between global and local pollination

VII. RESULTS

The proposed model is targeted towards detecting which transaction is fraudulent and/or legitimate in the given datasets using various parameters. The experiments were carried out using four (4) different datasets as described above. It is executed using five-folds cross-validation for each of the datasets. This was employed to test the model's performance in each subset of the four datasets so as to ensure model's performance is robust and generalizable across different subsets of the data. The datasets were splits into 70-30 percent ratio for training and testing sets. The training was conducted on 70% and testing was done on 30% to assess the model's ability to correctly classify previously unseen data. This is to ensure that the model's performance on completely new data and it is ability to generalize beyond the trained data. Synthetic Minority Oversampling Technique (SMOTE) was used to handle the issue of the imbalanced classes for European dataset 2013 and simulated credit card dataset 2019-2020 which are highly imbalanced. The experiment was carried out for 30 epochs cycles and all other parameters were set exactly the same for the all four (4) datasets. The experiment was executed using FPA with SNN. The FPA performed Feature selection and then SNN classified the transactions as legitimate or fraudulent. The same settings were exactly used in all the four (4) datasets (European credit card transaction dataset 2013, European credit card transaction dataset 2023, Simulated credit card transactions

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec932

2019-2020 and Australian credit card transaction datasets). The results obtained were presented in table 3 accompanied with the comparative analysis to justify the need for our proposed model.

Table 3 Results (FPA+ SNN)

Dataset	Accuracy	Precision	Recall	F1-Score	AUC-ROC	MCC
European Credit Card Dataset 2023	0.9869	0.9869	0.9869	0.9868	0.9991	0.9738
European Credit Card Dataset 2013	0.9781	0.9788	0.9781	0.9781	0.9985	0.9568
Simulated Credit Card Dataset 2019-2020	0.8605	0.8749	0.8605	0.8591	0.9199	0.7352
Australian Credit Card Dataset	0.9245	0.9259	0.9245	0.9242	0.9749	0.8484

Table 3 presented the results obtained after successful execution of all the experiments. The experiments were carried out in phases, at each phase a particular dataset was applied to test the model.

At first phase of the experiment, European credit card dataset 2023 was used for testing the model and the result indicated that the model attained an accuracy of 0.9869. Same value was obtained for precision, f1-score and recall while AUC-ROC is 0.9991 and MCC is 0.9738. The experiment further revealed that the model was able to select 5 features out the original 29 features. Training loss function is less is slightly above 0.11 using 30 epochs and became stable at 0.039 while the ROC attained stable stage at 1.0 which gives it final value of 0.9991. Figure 4 shows the training loss curve and ROC curve as well as the corresponding confusion matrix showing the actual and predicted fraud transactions.

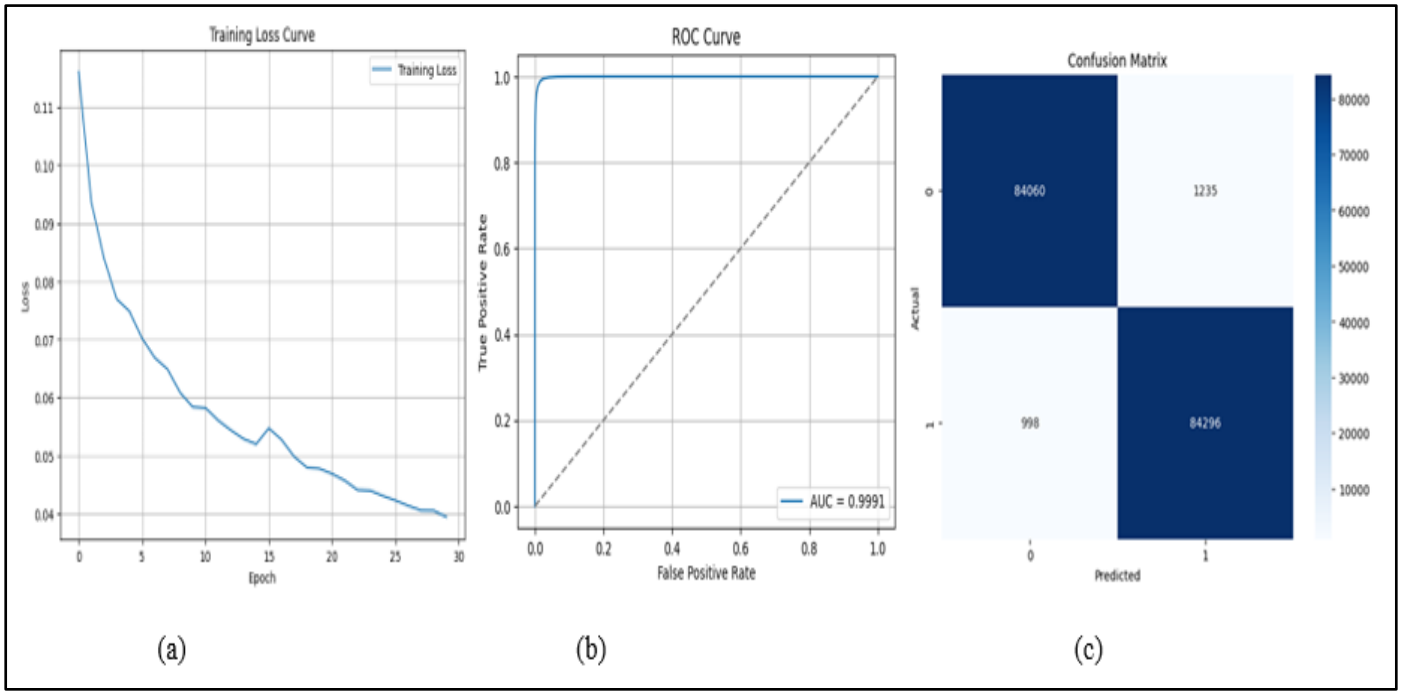

Fig 4 Training Loss (a), ROC Curves (b) and Confusion Matrix (c) for European Credit Card Dataset 2023

Figure 4(a) shows the training loss obtained after successful execution of Flower Pollination Algorithm (FPA) integrated with a Spiking Neural Network (SNN) which demonstrated strong performance in credit card fraud detection using the 2023 European Credit Card Dataset, as shown by a consistent declined in training loss over 30 epochs. The rapid decrease in loss from 0.115 to below 0.08 within the first five (5) epochs which indicated its effectiveness in early learning of transaction behavior, while the gradual stabilization after the 10th epoch reflects refined parameter optimization within the SNN. There was a minor noticeable fluctuation near epoch 15 indicating the role of FPA's global pollination exploration in avoiding local minima. Eventually, the model achieved a final loss of approximately 0.039, confirming improved convergence, enhanced predictive accuracy, and increased reliability. These findings highlight the FPA+SNN approach as a promising and efficient solution for real-time, intelligent credit card fraud detection.

The ROC curve shown in Figure 4(b) presented a classification efficiency of FPA+SNN model for detecting credit card fraud, revealing its strong ability to differentiate between classes. The curve's alignment toward the upper-left corner which shows that the sensitivity and specificity are near-optimal across multiple decision thresholds. With an AUC value of 0.9991, the model demonstrated an exceptional predictive performance, successfully identifying fraudulent and non-fraudulent transactions with very few false-positive cases. While The confusion matrix figure 4(c) indicated that the proposed FPA+SNN model performs extremely well in distinguishing fraudulent from legitimate transactions. It is

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec932

shows that from the actual non-fraud cases, 84,060 were correctly classified, while 1,235 were classified as false positives. Similarly, the model accurately identified 84,296 as fraudulent transactions and misclassified 998 as non-fraud. These results are an indication of highly balanced and reliable classifier with strong sensitivity and specificity, demonstrating the model's robustness and suitability for high dimensional dataset, and real-time credit card fraud detection.

At second phase, our proposed model was tested using 2013 European credit card transaction dataset. The results presented in table 3 shows that, our proposed model (FPA+SNN) attained an accuracy of 0.9781, with a precision of 0.9788 precision and a recall of 0.9781. Furthermore, the model was able to achieved an F1-score of 0.9781 which is an indication of balanced classification performance. The model also recorded an AUC-ROC of 0.9985 showing its discriminative capability and an MCC 0f 0.9568 reflecting model's strong reliability even under class imbalance. Figure 5 shows the graphical representation of training loss, AUC-ROC and confusion matrix.

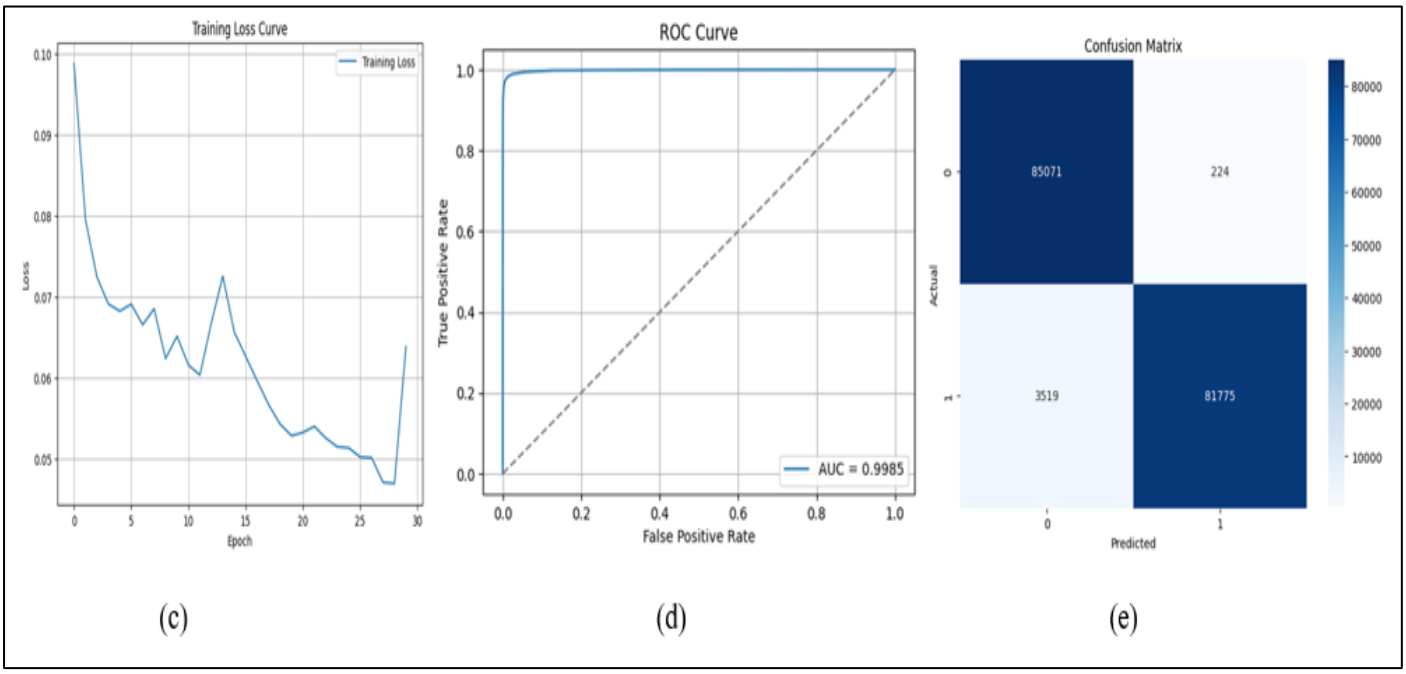

Fig 5 Training Loss (c), ROC Curves (d) and Confusion Matrix(e) for European Credit Card Dataset 2013

The figure 5(c) shows the training loss drops steeply from around 0.10 to about 0.07, indicating that the model was able to learned the patterns from the dataset quickly at the early training stage. There was a graduate improvement as the model Loss continues to decrease but at a slower rate. A minor fluctuation was observed, which may be caused by relatively high learning rate. The curve stabilizes between 0.05 and 0.065**,** showing that the model reaches a stable learning stage and at around Epoch 27, the model achieved its lowest loss value**,** which indicated that the model reaches its peak training performance. There was sudden rise (spike) at the final epoch but does not significantly affect the overall performance of the model. While the for figure 5(d) shows the ROC-curve indicated a very high true positive rate (TPR) at almost every threshold with corresponding a very low false positive rate (FPR)**.** This clearly showed as the model achieved an AUC of 0.9985 which indicated that the model performed well in predicting the classes. The confusion matrix figure 5(e) was obtained after successful execution of the model using 2013 European Credit Card Dataset which revealed the model's strong ability to distinguish between legitimate and fraudulent transactions. The model was able to correctly classified 85,071 as genuine transactions, while 224 were incorrectly identified as fraud, demonstrating high specificity. The model also identified 81,775 fraud cases accurately, though 3,519 were misclassified as non-fraud, showing a moderate false-negative rate due to highly imbalanced nature of datasets used. These results indicate that the model returned high accuracy and reliable classification performance.

The third phase of the experiment was executed based on Simulated Credit Card Dataset 2019-2020. The same goal was setup for FPA to handle Feature selection while SNN to classify the transactions as legitimate or fraudulent. The result show that FPA+SNN attained 0.8605 accuracy with a precision of 0.8749 and 0.8605 recall. Also, the model was able to obtained 0.8591 as f1-score with AUC-ROC of 0.9199 and 0.7352 as MCC. Figure 5 shows the pictorial representations of training loss curve, AUC_ROC and the confusion matrix.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec932

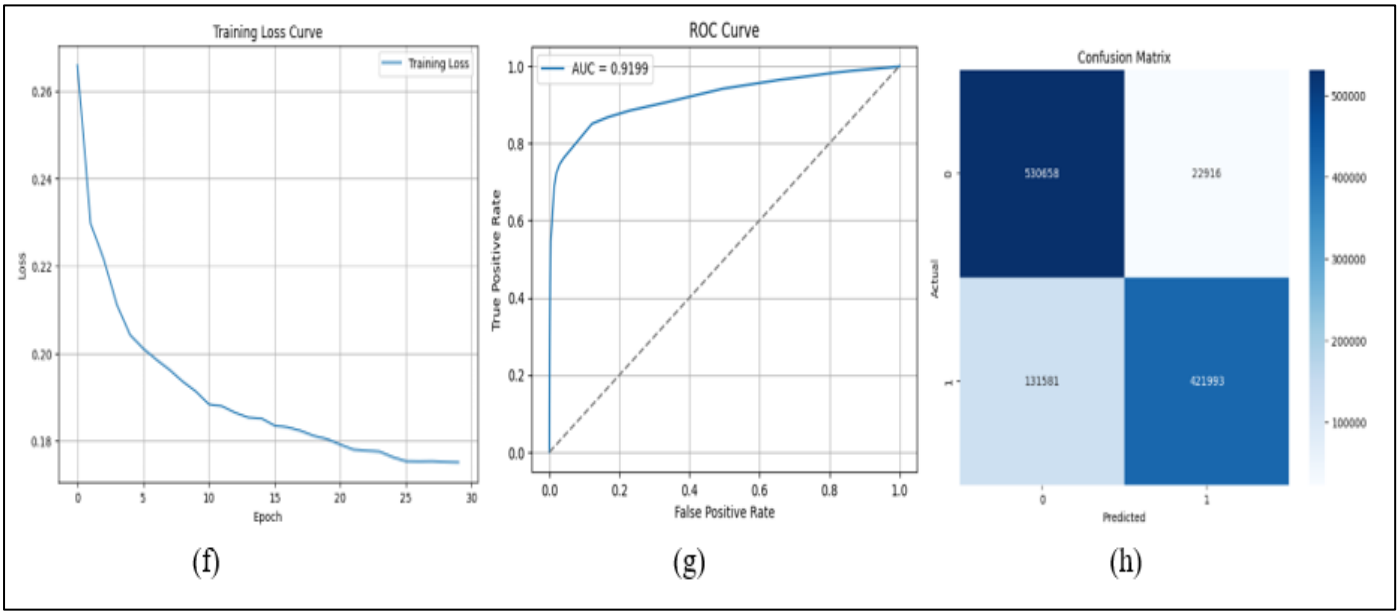

Fig 6 Training Loss (f), ROC Curves (g) and Confusion Matrix (h) for Simulated Credit Card Dataset 2019-2020

The training loss curve figure 6(f) demonstrated effective and stable learning behavior of our proposed model (FPA-SNN). A sharp reduction in loss is observed during the early stage (epochs), indicating rapid convergence and efficient capture of discriminative patterns in the dataset. This is followed by a gradual and consistent decline in loss across subsequent epochs, reflecting fine-grained optimization of synaptic weights facilitated by the Flower Pollination Algorithm's balanced exploration to exploitation mechanism. The smooth convergence to a low final loss value highlighted the stability of the training process and confirms the suitability of our proposed model for complex pattern recognition tasks such as fraud detection. The ROC curve figure 6(g) obtained demonstrated good classification performance, with the curve consistently approaching the upper-left region of the plot, which indicated high sensitivity and specificity across different thresholds. The Area Under the Curve (AUC) attained a value of 0.9199 shows how capability of the model's effectiveness in differentiate between positive and negative classes with a low false-positive rate. From the confusion matrix figure 6(h), it clearly seen that the model accurately classified 530,658 as non-fraudulent transactions and 421,993 as fraudulent transactions, demonstrating high true negative and true positive rates, respectively. While some misclassifications remain with 22,916 false positives and 131,581 as false negatives. The results reflect a reasonable trade-off typical of large, imbalanced datasets. Overall, the matrix confirms the model's effectiveness in capturing dominant transaction patterns and highlights its robustness for large-scale fraud detection.

Finally, phase four, employed FPA+SNN was tested on Australian Credit Card Transaction Dataset (ACCD) and the model revealed an accuracy of 0.9245 with corresponding precision of 0.9259 and recall of 0.9245. The model achieved F1-score of 0.9242. we further evaluated the model using AUC-ROC and MCC and it was able to achieved 0.9749 and 0.8484 respectively. Figure 7 Below shows the training loss curve, ROC-curve as well as the confusion matrix.

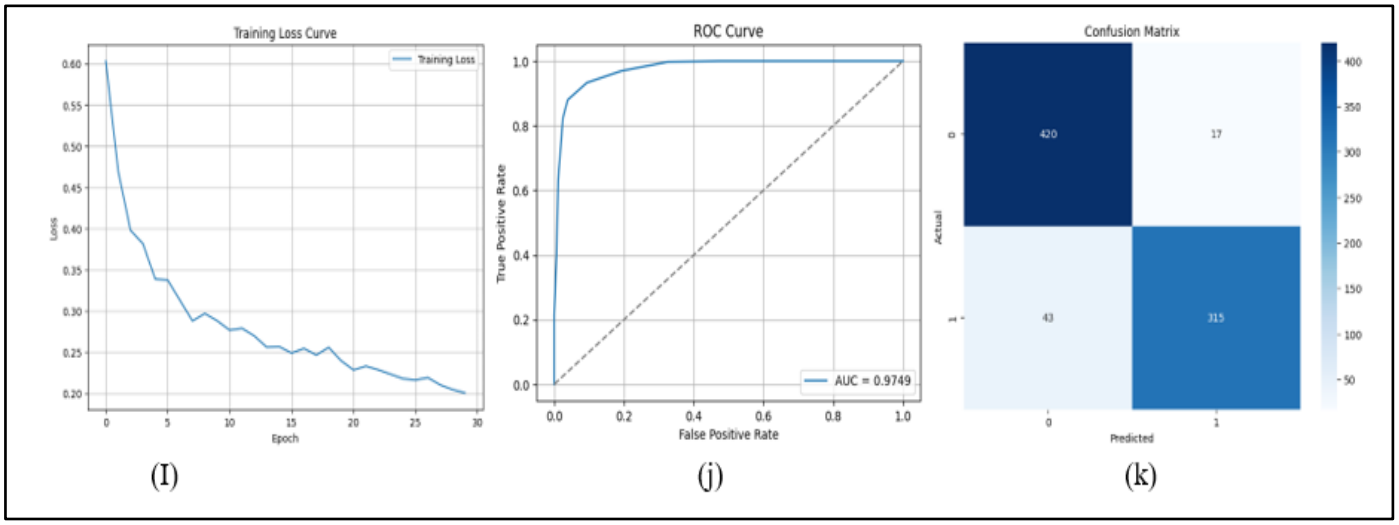

Fig 7 Training Loss(I), ROC Curves (j) and Confusion Matrix (k) for Australian Dataset

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec932

The training loss curve figure 7(i) obtained from the Australian credit card transaction dataset demonstrated effective learning and stable convergence of the proposed Flower Pollination Algorithm with Spiking Neural Network (FPA+SNN). The model exhibits a rapid reduction in loss during the initial epochs, steadily decreased from approximately 0.60 to below 0.35 within the first five epochs, indicating efficient early extraction of discriminative transaction features. Subsequent epochs show more gradual and consistent decline in loss, reflecting refined optimization of synaptic weights and firing thresholds inherent to the SNN architecture. By the final epoch, the loss converges to approximately 0.20, confirming training stability and improved predictive capability. This clearly indicated an effectiveness of FPA in guiding the SNN toward reliable convergence and strong detection of fraud cases on Australian dataset.

The ROC curve figure 7(j) shows steeply rise toward the upper-left region, indicating a high true positive rate at relatively low false positive rates across varying thresholds. The model achieved an AUC value of 0.9749, reflecting the model classification capability to distinguish fraudulent transactions from legitimate ones. This high AUC score confirms the effectiveness and reliability of the proposed FPA+SNN approach for credit card fraud detection within the Australian dataset. The confusion matrix for the FPA+SNN model figure 7(k) was able to correctly classified 420 legitimate transactions with only 17 false positives, which demonstrated high specificity. It also accurately detected 315 fraudulent transactions, while 43 cases were misclassified as non-fraud.

In this study, we employed graphical representation to illustrate the effectiveness of our proposed approach in identifying fraudulent transactions within credit card datasets. The ROC-AUC plot is a widely used visualization means for assessing the performance of machine learning and deep learning models, especially in the context of imbalanced datasets. The ROC-AUC curve delineates the false positive rate along the x-axis and the true positive rate along the y-axis, as illustrated in the aforementioned figures 4, 5, 6, and 7. The AUC curves revealed the superior performance of our proposed methodology across all datasets, which aligns with the findings detailed in Table 3. The results indicated that our proposed model is capable of distinguishing between fraudulent and legitimate transactions, confirming the model reliability and practical applicability for fraud detection as tested across all the four datasets.

The comprehensive findings suggest that our predictive model attained high levels of accuracy and precision within the European credit card datasets, concurrently preserving substantial metrics for recall, AUC-ROC, and MCC, thereby underscoring our model's effectiveness in detecting fraudulent transactions. However, the performance appears to be suboptimal in the other two datasets (Simulated credit card and Australian datasets), which is attributed to the low dimensionality in the case of Australian dataset while for Simulated credit card transaction dataset, the imbalance nature of the dataset as well as noisy, redundant and irrelevant features which led to time consuming while executing the model are some of the factors that caused low performance from these datasets as evidence from the literature (Ayoub et al., 2025).

VIII. PERFORMANCE COMPARISON

In order to ascertain the performance of our proposed method we compared with the recent models such as Boosted Grey Wolf Optimization presented by[31] and Brown Bear Optimization Algorithm (BBOA) presented by [32]. It is worth mentioning that, in our proposed model, the FPA is employed for feature selection to deal with redundant, noisy and irrelevant features in the datasets while spiking Neural Networks (SNN) was used for classification. This comparison aimed to validate the model efficiency on credit card fraud detection. Our comparison focuses on the metrics used for testing the performance of credit card fraud detection models such as accuracy, precision, recall, F1-score AUC-curve and MCC. The comparisons were made across three datasets, methods and metrics to ensure superiority and justification of our proposed model.

Considering the inherent class imbalance in the two datasets used (the European Credit Card Transaction Dataset (2013) and the Simulated Credit Card Dataset (2019-2020), each exhibiting an approximate 99:1 ratio between the majority class 0 and minority class 1. All models were evaluated across all the performance metrics that go beyond accuracy, as accuracy alone can be misleading in highly imbalanced datasets. Therefore, our comparisons focused on the Area Under the Receiver Operating Characteristic Curve (AUC-ROC) and the Matthews Correlation Coefficient (MCC), which are particularly well suited for assessing classification performance under class imbalance.

Table 4 Performance Comparison of our Proposed Model with (BBOA + SVM, BBOA +KNN, and BBOA +Xgb-tree) and (BBOA + KNN and BBOA + Xgb-tree)

Article	Models	Datasets	Metrics					
			Accuracy	Precision	Recall	F1-score	AUC-ROC	MCC
[32]	BBOA + SVM	Australian Dataset	0.8879	0.8151	0.9013	0.8560	0.9160	0.7673
	BBOA + KNN		0.8986	0.8915	0.8261	0.8575	0.9023	0.7803
	BBOA + Xgb-tree		0.9106	0.8865	0.8706	0.8780	0.9124	0.8081
	Our Proposed Model (FPA+SNN)	Australian Dataset	0.9245	0.9259	0.9245	0.9242	0.9749	0.8484

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec932

Table 4 shows a comparison of results generated from our model **(**FPA+SNN) based on the Australian Dataset with that of BBOA-based models on the same dataset which clearly shows that the our proposed FPA+SNN model consistently outperforms the benchmark approaches across all evaluation metrics. Specifically, our proposed model achieved a higher accuracy of 0.9245 compared to BBOA+XGB-tree having 0.9106, BBOA+KNN having 0.8986, and BBOA+SVM has 0.8879, indicating superior overall classification capability. Precision and recall values for FPA+SNN are 0.9259 and 0.9245 respectively are also markedly higher, reflecting improved reliability in correctly identifying both fraudulent and legitimate transactions. Furthermore, the F1-score of 0.9242 surpassed those of the BBOA-based models, demonstrating a better balance between precision and recall. In terms of discriminative power, our proposed model attained significantly higher AUC-ROC of 0.9749, compared to values ranging from 0.9023 to 0.9160 for the competing models, while the MCC of 0.8484 further confirms stronger robustness on this imbalanced dataset. Overall, these results highlighted the success of the FPA+SNN framework in delivering superior and more stable fraud detection performance on the Australian dataset. To further ascertain the effectiveness and reliability our proposed model we further compared our model with some of the existing techniques from the literature (see Table 5).

Table 5 Comparison of our Proposed Model (FPA + SNN) with Boosted Grey Wolf Optimization

Article	Models	Datasets	Metrics					
			Accuracy	Precision	Recall	F1-score	AUC-ROC	MCC
[31]	Boosted Grey Wolf Optimization	European Credit Card 2013	0.9300	0.8700	0.9600	0.9200	-	-
		Simulated Credit Card (2019-2020)	0.9600	0.1000	0.9200	0.8100	-	-
[40]	XGBOOST & Bayesion Optimization	European Credit Card 2013	0.9996	0.9406	0.8740	0.8740	0.9879	-
		IEE-CIS CCD 2019	0.8325	0.8294	0.8378	0.8336	0.9088	-
Our Proposed Model	FPA + SNN	European Credit Card 2013	0.9781	0.9788	0.9781	0.9781	0.9985	0.9568
		Simulated Credit Card (2019-2020)	0.8605	0.8749	0.8605	0.8591	0.9199	0.7352

In table 5, we compared our proposed model (FPA+SNN) with Boosted Grey Wolf Optimization proposed by [31] on the European Credit Card Dataset 2013 and the Simulated Credit Card Dataset (2019-2020) revealed a notable performance difference. On European dataset 2013, our proposed model FPA+SNN significantly outperformed that of Boosted Grey Wolf Optimization approach higher accuracy of 0.9781 against 0.9300, alongside with significant improved on precision of 0.9788 against 0.8700. There is also a balanced recall of 0.9781 from FPA+SNN against 0.9600 obtained from Boosted grey wolf optimization with a superior performance of F1-score of 0.9781 against 0.9200. The AUC-ROC of 0.9985 and MCC of 0.9568 further confirmed the robustness and strong discriminative capability of our proposed model which were not reported by the compared method.

On other hand, simulated credit card dataset 2019-2020 with a Boosted Grey Wolf Optimization reported a higher accuracy of 0.9600, this is accompanied by extremely low precision of 0.1000 which indicated a high false-positive rate and poor reliability in fraud identification. In contrast, our proposed model exhibits a more balanced and practical performance, with substantially higher precision of 0.8749, recall of 0.8605 and F1-score of 0.8591. Furthermore, our model returned good AUC-ROC of 0.9199 and MCC of 0.7352. This proved that our proposed framework provides a balanced, robust and reliability across all the datasets, making it more suitable for real-world credit card fraud detection than the one compared with.

We further compared our model with that of (Abdul Salam et al., 2024) presented based on XGBoost with Bayesian Optimization across the European Credit Card Dataset 2013 and the Simulated Credit Card Dataset and revealed relative strengths of each approach. On the European Credit Card 2013 dataset, XGBoost with Bayesian Optimization achieved an exceptionally high accuracy (0.9996) and good AUC-ROC (0.9879); however, its lower recall and F1-score (both 0.8740) suggest reduced effectiveness in consistently detecting fraudulent transactions. In contrast, our proposed model attained a slightly lower accuracy (0.9781) but demonstrates a far superior balance between precision (0.9788) and recall (0.9781), yielding a higher F1-score of 0.9781, with strong AUC-ROC of 0.9985, and MCC of 0.9568, which is an indication of greater robustness on this highly imbalanced dataset.

On the Simulated Credit Card Dataset, XGBoost with Bayesian Optimization achieved moderate performance, with an accuracy of 0.8325, F1-score of 0.8336, and AUC-ROC of 0.9088. While our proposed model (FPA+SNN) consistently outperformed with higher accuracy of 0.8605, precision of 0.8749, with 0.8605 recall and F1-score of 0.8591, alongside an improved AUC-ROC of 0.9199 as well as MCC of 0.7352 which confirmed our model stability and reliability. Overall,

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec932

the comparison demonstrated that while XGBoost with Bayesian Optimization excels in raw accuracy on the European dataset, our proposed approach (FPA+SNN) delivered more balanced, discriminative, and practically reliable performance across all the datasets.

IX. CONCLUSION AND RECOMMENDATION

The comparative evaluation demonstrated strong effectiveness of our proposed framework across multiple credit card fraud transaction datasets. Specifically, on the Australian dataset, our model (FPA+SNN) has consistently outperformed BBOA-based models in all metrics, with higher accuracy, precision, recall, F1-score, AUC-ROC, and MCC, thereby confirmed its superior on imbalanced datasets. Further comparisons were made with Boosted Grey Wolf Optimization and XGBoost with Bayesian Optimization on the European Credit Card (2013) and Simulated Credit Card (2019-2020) datasets and the results revealed that, although some competing methods achieved high raw accuracy, they often suffered from poor balance between precision and recall. In contrast, our proposed model (FPA+SNN) maintained consistently high and well-balanced performance, evidenced by superior F1-scores, near-perfect AUC-ROC values, and strong MCC scores. This shows our model reliability, stability, and practical suitability for real-world credit card fraud detection across diverse and highly imbalanced datasets.

Despite the strong and consistent performance of our proposed model (FPA+SNN) across multiple real-world credit card transaction datasets, some research gaps warrant further investigation. Future work may focus on improving the quality of the dataset such as simulated transaction dataset so as to balance the dataset, which will address real-time fraud detection and reduce computational and time complexity to enhance scalability. Additionally, integrating other meta-heuristics approaches or explainable AI techniques (such as SHAP- Shapley Additive explanation or LIME- Local Interpretable Model-Agnostic Explanation) may improve model interpretability, and benchmarking against recent deep learning architectures such as graph-based and transformer models would further strengthen the framework. Extending the approach to multi-modal transaction data and other financial domains would also enhance generalization and practical applicability, aligning the model more closely with real-world deployment requirements.

REFERENCES

[1]. Y. Song, O. Escobar, U. Arzubiaga, and A. De Massis, “The digital transformation of a traditional market into an entrepreneurial ecosystem,” Review of Managerial Science, vol. 16, no. 1, pp. 65–88, 2022, doi: 10.1007/s11846-020-00438-5.

[2]. V. F. Rodrigues et al., “Fraud detection and prevention in e-commerce: A systematic literature review,” Electron Commer Res Appl, vol. 56, Nov. 2022, doi: 10.1016/j.elerap.2022.101207.

[3]. P. Sharma and S. Pote, “Credit Card Fraud Detection using Deep Learning based on Neural Network and Auto encoder,” Int J Eng Adv Technol, vol. 9, no. 5, pp. 1140–1143, 2020, doi: 10.35940/ijeat.e9934.069520.

[4]. W. Lovo, “JMU Scholarly Commons Detecting credit card fraud : An analysis of fraud detection techniques,” 2020.

[5]. T. Pourhabibi, K. L. Ong, B. H. Kam, and Y. L. Boo, “Fraud detection: A systematic literature review of graph-based anomaly detection approaches,” Decis Support Syst, vol. 133, no. April, p. 113303, 2020, doi: 10.1016/j.dss.2020.113303.

[6]. R. Juniper, “COMBATTING ONLINE PAYMENT FRAUD Whitepaper,” 2024.

[7]. Y. T. Lei, C. Q. Ma, Y. S. Ren, X. Q. Chen, S. Narayan, and A. N. Q. Huynh, “A distributed deep neural network model for credit card fraud detection,” Financ Res Lett, vol. 58, no. PC, p. 104547, 2023, doi: 10.1016/j.frl.2023.104547.

[8]. D. Sachar, “Optimizing Transaction Fraud Detection: A Comparative Study of Nature-Inspired Algorithms for Feature Selection,” in 2025 IEEE Systems and Information Engineering Design Symposium, SIEDS 2025, Institute of Electrical and Electronics Engineers Inc., 2025, pp. 392–397. doi: 10.1109/SIEDS65500.2025.11021207.

[9]. Z. Li, M. Huang, G. Liu, and C. Jiang, “A hybrid method with dynamic weighted entropy for handling the problem of class imbalance with overlap in credit card fraud detection,” Expert Syst Appl, vol. 175, no. February, p. 114750, 2021, doi: 10.1016/j.eswa.2021.114750.

[10]. F. Carcillo, Y. A. Le Borgne, O. Caelen, Y. Kessaci, F. Oblé, and G. Bontempi, “Combining unsupervised and supervised learning in credit card fraud detection,” Inf Sci (N Y), vol. 557, pp. 317–331, May 2021, doi: 10.1016/j.ins.2019.05.042.

[11]. H. Tabrizchi and J. Razmara, “Credit card fraud detection using hybridization of isolation forest with grey wolf optimizer algorithm,” Soft comput, vol. 2, no. Ml, 2024, doi: 10.1007/s00500-024-09772-2.

[12]. F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, “Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms,” IEEE Access, vol. 10, pp. 39700–39715, 2022, doi: 10.1109/ACCESS.2022.3166891.

[13]. S. Bakhtiari, Z. Nasiri, and J. Vahidi, “Credit card fraud detection using ensemble data mining methods,” Multimed Tools Appl, vol. 82, no. 19, pp. 29057–29075, 2023, doi: 10.1007/s11042-023-14698-2.

[14]. A. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, “Credit card fraud detection in the era of disruptive technologies: A systematic review,” Jan. 01, 2023, King Saud bin Abdulaziz University. doi: 10.1016/j.jksuci.2022.11.008.

[15]. E. A. L. M. Btoush, X. Zhou, R. Gururajan, K. C. Chan, R. Genrich, and P. Sankaran, “A systematic review of literature on credit card cyber fraud detection

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec932

using machine and deep learning," PeerJ Comput Sci, vol. 9, pp. 1–66, 2023, doi: 10.7717/PEERJ-CS.1278.

[16]. J. Huang, "Credit Card Transaction Fraud Using Machine Learning Algorithms," vol. 116, no. Icesed 2019, pp. 82–91, 2020, doi: 10.2991/icesed-19.2020.14.

[17]. N. S. Alfaiz and S. M. Fati, "Enhanced Credit Card Fraud Detection Model Using Machine Learning," Electronics (Switzerland), vol. 11, no. 4, Feb. 2022, doi: 10.3390/electronics11040662.

[18]. S. Singh and A. Maheshwari, "Credit Card Fraud Detection," Proceedings - 2022 4th International Conference on Advances in Computing, Communication Control and Networking, ICAC3N 2022, no. October, pp. 209–213, 2022, doi: 10.1109/ICAC3N56670.2022.10074052.

[19]. S. Negi, S. K. Das, and R. Bodh, "Credit Card Fraud Detection using Deep and Machine Learning," Proceedings - International Conference on Applied Artificial Intelligence and Computing, ICAAIC 2022, no. Icaaic, pp. 455–461, 2022, doi: 10.1109/ICAAIC53929.2022.9792941.

[20]. R. Chhabra, S. Goswami, and R. Kumar, "A voting ensemble machine learning based credit card fraud detection using highly imbalance data," Multimed Tools Appl, vol. 83, no. 18, pp. 54729–54753, 2024, doi: 10.1007/s11042-023-17766-9.

[21]. K. I. Alkhatib, A. I. Al-aiad, M. H. Almahmoud, and O. N. Elayan, "Credit Card Fraud Detection Based on Deep Neural Network Approach," no. May, 2021, doi: 10.1109/ICICS52457.2021.9464555.

[22]. F. K. Alarfaj, I. Malik, H. U. Khan, N. Almusallam, M. Ramzan, and M. Ahmed, "Credit Card Fraud Detection Using State-of-the-Art Machine Learning and Deep Learning Algorithms," IEEE Access, vol. 10, pp. 39700–39715, 2022, doi: 10.1109/ACCESS.2022.3166891.

[23]. G. Zioviris, K. Kolomvatsos, and G. Stamoulis, "Credit card fraud detection using a deep learning multistage model," Journal of Supercomputing, vol. 78, no. 12, pp. 14571–14596, 2022, doi: 10.1007/s11227-022-04465-9.

[24]. R. Bin Sulaiman, V. Schetinin, and P. Sant, "Review of Machine Learning Approach on Credit Card Fraud Detection," Human-Centric Intelligent Systems, vol. 2, no. 1–2, pp. 55–68, 2022, doi: 10.1007/s44230-022-00004-0.

[25]. T. K. Dang and T. Ha, "A Comprehensive Fraud Detection for Credit Card Transactions in Federated Averaging," SN Comput Sci, vol. 5, no. 5, 2024, doi: 10.1007/s42979-024-02898-y.

[26]. M. Abdul Salam, K. M. Fouad, D. L. Elbably, and S. M. Elsayed, "Federated learning model for credit card fraud detection with data balancing techniques," Neural Comput Appl, vol. 36, no. 11, pp. 6231–6256, 2024, doi: 10.1007/s00521-023-09410-2.

[27]. Y. Alghofaili, A. Albattah, and M. A. Rassam, "A Financial Fraud Detection Model Based on LSTM Deep Learning Technique," Journal of Applied Security Research, vol. 15, no. 4, pp. 498–516, 2020, doi: 10.1080/19361610.2020.1815491.

[28]. T. T. Nguyen, H. Tahir, M. Abdelrazek, and A. Babar, "Deep Learning Methods for Credit Card Fraud Detection," p. 8, 2020.

[29]. D. Sehrawat and Y. Singh, "Auto-Encoder and LSTM-Based Credit Card Fraud Detection," SN Comput Sci, vol. 4, no. 5, Jul. 2023, doi: 10.1007/s42979-023-01977-w.

[30]. I. Benchaji, S. Douzi, B. El Ouahidi, and J. Jaafari, "Enhanced credit card fraud detection based on attention mechanism and LSTM deep model," J Big Data, vol. 8, no. 1, Dec. 2021, doi: 10.1186/s40537-021-00541-8.

[31]. M. Ayoub, T. Abdelhamid, and J. Khalid, "Granular computing framework for credit card fraud detection," May 01, 2025, Elsevier B.V. doi: 10.1016/j.aej.2025.02.019.

[32]. S. E. Sorour, K. M. AlBarrak, A. A. Abohany, and A. A. A. El-Mageed, "Credit card fraud detection using the brown bear optimization algorithm," Alexandria Engineering Journal, vol. 104, no. May, pp. 171–192, 2024, doi: 10.1016/j.aej.2024.06.040.

[33]. M. Abdel-Basset and L. A. Shawky, "Flower pollination algorithm: a comprehensive review," Dec. 01, 2019, Springer Netherlands. doi: 10.1007/s10462-018-9624-4.

[34]. W. Xu, Y. Wang, D. Yan, and Z. Ji, "Flower Pollination Algorithm for Multi-Objective Fuzzy Flexible Job Shop Scheduling," Xitong Fangzhen Xuebao / Journal of System Simulation, vol. 30, no. 11, pp. 4403–4412, Nov. 2018, doi: 10.16182/j.issn1004731x.joss.201811042.

[35]. Z. A. A. Alyasseri, A. T. Khader, M. A. Al-Betar, M. A. Awadallah, and X. S. Yang, "Variants of the flower pollination algorithm: A review," in Studies in Computational Intelligence, vol. 744, Springer Verlag, 2018, pp. 91–118. doi: 10.1007/978-3-319-67669-2_5.

[36]. X.-S. Yang, "Flower Pollination Algorithm for Global Optimization," Dec. 2013, doi: 10.1007/978-3-642-32894-7_27.

[37]. K. Yamazaki, V. K. Vo-Ho, D. Bulsara, and N. Le, "Spiking Neural Networks and Their Applications: A Review," Brain Sci, vol. 12, no. 7, pp. 1–30, 2022, doi: 10.3390/brainsci12070863.

[38]. J. D. Nunes, M. Carvalho, D. Carneiro, and J. S. Cardoso, "Spiking Neural Networks: A Survey," IEEE Access, vol. 10, pp. 60738–60764, 2022, doi: 10.1109/ACCESS.2022.3179968.

[39]. A. Tavanaei, M. Ghodrati, S. R. Kheradpisheh, T. Masquelier, and A. Maida, "Deep learning in spiking neural networks," Neural Networks, vol. 111, pp. 47–63, 2019, doi: 10.1016/j.neunet.2018.12.002.

[40]. M. Abdul Salam, K. M. Fouad, D. L. Elbably, and S. M. Elsayed, "Federated learning model for credit card fraud detection with data balancing techniques," Neural Comput Appl, vol. 36, no. 11, pp. 6231–6256, 2024, doi: 10.1007/s00521-023-09410-2.

[41]. T. K. Dang and T. Ha, "A Comprehensive Fraud Detection for Credit Card Transactions in Federated Averaging," SN Comput Sci, vol. 5, no. 5, 2024, doi: 10.1007/s42979-024-02898-y.

ISSN No: -2456-2165 https://doi.org/10.38124/ijisrt/25dec932

[42]. B. Alshawi, "Utilizing GANs for Credit Card Fraud Detection: A Comparison of Supervised Learning Algorithms," Engineering, Technology and Applied Science Research, vol. 13, no. 6, pp. 12264–12270, 2023, doi: 10.48084/etasr.6434.

[43]. H. C. Du, L. Lv, H. Wang, and A. Guo, "A novel method for detecting credit card fraud problems," PLoS One, vol. 19, no. 3 March, pp. 1–26, 2024, doi: 10.1371/journal.pone.0294537.

[44]. W. Liu, X. Wang, and W. Peng, "State of the Art: Secure Mobile Payment," IEEE Access, vol. 8, pp. 13898–13914, 2020, doi: 10.1109/ACCESS.2019.2963480.

[45]. A. Cherif, A. Badhib, H. Ammar, S. Alshehri, M. Kalkatawi, and A. Imine, "Credit card fraud detection in the era of disruptive technologies: A systematic review," Jan. 01, 2023, King Saud bin Abdulaziz University. doi: 10.1016/j.jksuci.2022.11.008.

[46]. R. Bin Sulaiman, V. Schetinin, and P. Sant, "Review of Machine Learning Approach on Credit Card Fraud Detection," Human-Centric Intelligent Systems, vol. 2, no. 1–2, pp. 55–68, 2022, doi: 10.1007/s44230-022-00004-0.

[47]. G. Zioviris, K. Kolomvatsos, and G. Stamoulis, "Credit card fraud detection using a deep learning multistage model," Journal of Supercomputing, vol. 78, no. 12, pp. 14571–14596, 2022, doi: 10.1007/s11227-022-04465-9.

[48]. Q. Zhu, "On the performance of Matthews correlation coefficient (MCC) for imbalanced dataset," Pattern Recognit Lett, vol. 136, pp. 71–80, Aug. 2020, doi: 10.1016/j.patrec.2020.03.030.