

# ENHANCING IMBALANCED CREDIT CARD FRAUD DETECTION USING MULTILAYER PERCEPTION

DEEPALI GARG<sup>1\*</sup>

UMA SHARMA<sup>2</sup>

<sup>1</sup>BANASTHALI VIDYAPITH, NIWAI, RAJASTHAN, INDIA, EMAIL: [garg.deepali05@gmail.com](mailto:garg.deepali05@gmail.com)

<sup>2</sup>BANASTHALI VIDYAPITH, NIWAI, RAJASTHAN, INDIA, EMAIL: [uma.sharma@banasthali.in](mailto:uma.sharma@banasthali.in)

## Abstract

Traditional detection techniques often struggle with highly imbalanced datasets and subtle patterns in fraudulent behavior and Credit card fraud depicts significant challenges to financial institutions because of its rarity, unpredictability, and rapid evolution. This study shows a deep learning-based approach utilizing a Multilayer Perceptron (MLP) which is trained on a strategically balanced dataset with a 1:4 fraud-to-non-fraud ratio. Extensive preprocessing and feature engineering steps were undertaken, which includes the generation of temporal, behavioral, geospatial, and probability-based features. To resolve class imbalance and focus on hard-to-classify fraudulent samples, focal loss with class weighting was employed during training. The MLP model, incorporating dropout regularization and ReLU activations, was inculcated and evaluated using precision, recall, F1-score, and PR-AUC metrics. With achieved results of precision of 97%, recall of 85%, F1-score of 90% and PR-AUC of 89%, it demonstrated significant improvements over traditional models on the original imbalanced test set. These findings emphasized the importance of engineered features and specialized training strategies in enhancing the detection of rare and costly fraud events.

**Keywords:** credit card fraud detection (CCFD), multilayer perceptron (MLP), focal loss, weighted loss, class imbalance, data preprocessing, feature selections.

## INTRODUCTION

In a country like India where the frequency and quantity of digital transactions have increased significantly especially after demonetisation of 2016. These digital transactions are generally processed by credit or debit card. With the increase in transactions, frauds have also witnessed a spike which poses a challenging task for these online platforms and institutions. This field has thus gained attention by ML and business intelligence community to combat this digital fraud menace[1].

According to the Nilson report, 2019 [1], due to fraudulent activity worldwide, \$24.26 billion loss has occurred against a loss of \$34.66 billion in 2022. Such high fraudulent transactions have resulted in increasing interest in detection of various techniques among the researchers all over the world for detecting frauds. High strenuous mining data jobs are employed by E-commerce firms on the logs of their servers for detection of such frauds.

These logs consist of data, both fraudulent and non-fraudulent data, in the class label with the count of fraudulent data much less than the non-fraudulent data. The classifier might ignore them as noise due to low count of such transactions. Rule-based fraud detection tools have been deployed to identify fraudsters [2].

In the contemporary era of Artificial Intelligence (AI), we cannot completely trust on humans, mentioned in an article - 123 1988 Arabian Journal for Science and Engineering (2022) 47:1987–1997 To reduce problems which consists of high empirical risks, Rule based tools designed by fraud experts are deployed;

The extensive adoption of electronic/online services has led to a massive increase in no of credit card transactions throughout the world. Furthermore this growth increased credit card fraud multifold, which poses an rising threat to both financial institutions and consumers[4] [5] [6] According to Nielsen reports, global financial losses caused through credit card fraud were approximately USD 28.65 billion in 2019, USD 28.50 billion in 2020, and USD 32.34 billion in 2021 [7], [8], [9]. Moreover, these losses have tripled over the past decade as it was only USD 9.84 billion in 2011[10].

Machine Learning (ML) techniques, a subset of AI, have been widely adopted for credit card fraud detection (CCFD) to address this increasing concern to achieving competitive and, in many cases, state-of-the-art performance [11][12]. ML methods are generally divided into supervised, semi-supervised, unsupervised, and reinforcement learning paradigms [13]. Among these, supervised learning (SL) has been identified as the most used approach for CCFD tasks [14]. In SL, models are trained using labelled datasets in which each instance is associated with a predefined class label—typically indicates if a transaction is fraudulent or legitimate. This helps the model to learn the underlying relationships between input characteristics and output labels. [updated]

Neural networks have shown considerable efficacy in recent years for modelling complex and high-dimensional transaction data for fraud detection purposes [15], [16]. Models, inspired by the human brain design, can operate under both supervised and unsupervised learning schemes [17]. Deep learning (DL), a subfield of ML, characterized by neural networks with multiple hidden layers, has shown superior capabilities in automatically extracting hierarchical features and capturing intricate patterns within data. For example, Mienye and Sun [18] has proposed a deep learning-based ensemble framework which comprises long short-term memory (LSTM) and

gated recurrent unit (GRU) networks, which are integrated with a multilayer perceptron (MLP) as the base learner. Their approach exhibited superior performance compared to individual DL models and conventional ML algorithms, thereby reinforcing the potential of DL-based ensemble methods in credit card fraud detection.

A multilayer perceptron (MLP) is a form of neural network that is often employed for applications like fraud detection [19]. Data can be modelled into non-linear relationships using MLP, however it has certain problems when it comes to dealing with class imbalance concerns [20]. Among these shortcomings are the need for intricate hyperparameters to get the intended results, as well as overfitting to the majority class and underfitting to the minority class [21].

## LITERATURE REVIEW

Recent studies in credit card fraud detection emphasize the challenges of imbalanced datasets and the importance of effective feature selection. Techniques like SMOTE, oversampling, and under sampling have been widely used to address class imbalance, while ensemble methods, particularly stacked models have shown improved predictive accuracy and robustness over traditional approaches [22].

Several ML methods can be employed for credit card fraud detection [23], [24]. Specifically, supervised learning algorithms which use labelled datasets with past transaction records to create ML models have proven to be quite successful in detecting new fraudulent transactions. These algorithms include Logistics regression(LR) [25], support vector machines (SVM) [26], decision trees (DT) [27], adaptive boosting (AdaBoost) [28], random forest (RF) [29] and artificial neural networks (ANN) [30].

Furthermore, even if we combine deep learning-based ensemble models with deep learning-based methods like MLP, it could produce more reliable models, although they are seldomly employed for CCFD.

Majority class is the class that comprises a large proportion of dataset whereas minority class comprises dataset with smaller proportion. Most ML algorithms are designed with the assumption that the dataset is more evenly balanced which makes Imbalance Classification of the dataset more challenging and lead to poor performance of algorithms.[31].

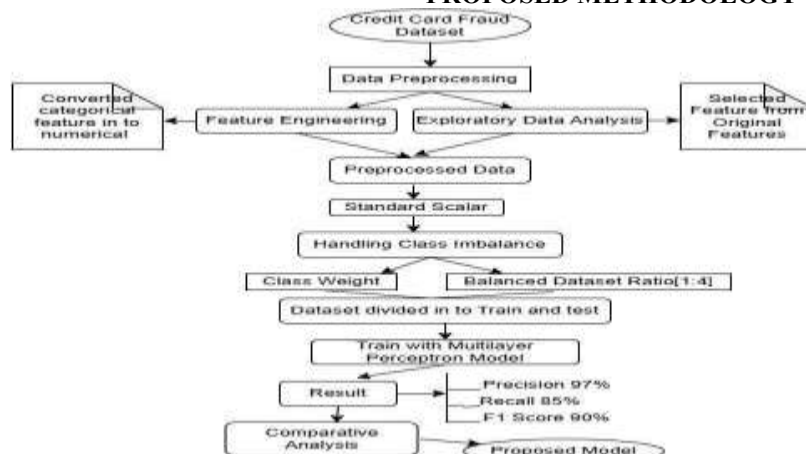
Although Deep learning (DL) is a subset of ML but it has recently dominated the ML field [32]. It mainly comprises a neural network with multiple layers and it has achieved excellent prediction performance of complex problems in CCFD[33]. Recurrent neural network (RNN) is one technique used in deep learning models and it has been employed for different sequential modelling-based ML tasks [34],[35]. Shen Etal. in his articles noted that algorithms which use RNNs, perform much better than the traditional ML model.

There are multiple types of RNN based models. The simple RNN model is prone to the vanishing gradient problem. The RNN is unable to manage relevant gradient issues from the model output end back to the layers near the input end in this case. [36][37]. LSTM and GRU-based RNNs are known to solve this vanishing gradient problem and have shown good performances in different sequence classification tasks [38],[39].

Some ML algorithms build models that uses low accuracy, high bias or high variance. Single base classifiers perform less effectively as compared to Ensemble learning classifiers which train multiple base classifiers and combine their outputs to get outstanding performance [40], [41].

A neural network comprises of three layers- the input layer, hidden layer and output layer. It is an effective neural network which is used in several domains and is termed as multilayer perceptron(MLP) [42]. In an MLP network , data flows from input to output layer as the neurons are the processing elements in the MLP and the neurons in each layer are connected to every neuron in the next layer. The input layer provides the network with input variables and following layer receives their inputs from the output of the previous layer. The base of the MLP is the hidden layer which is placed between the input and output. This layer processes the information which we give as input and transfers it to the output layer [43],[44].The MLP network enables the network to update its weights to minimize or reduce the output error and is usually trained using the backpropagation algorithm [45].

## PROPOSED METHODOLOGY



## Figure 1: Research Methodology

### Credit Card Fraud Dataset

The dataset was gathered from <https://www.kaggle.com/datasets/kartik2112/fraud-detection> on Kaggle. The dataset comprised of 1,852,394 transactions with 23 attributes, including amt, cc\_num, city\_pop, gender, city, lat, job, long, merch\_lat, is\_fraud, merch\_long and others. In order to identify that whether a transaction is false, the target variable is 'is\_fraud'. The data includes a vast range of transaction details, laying the base for effective fraud detection [46].

### Data Preprocessing

Data preprocessing is a vital step in the development of an effective credit fraud detection model, as it makes sure that the raw dataset is converted to a clean, structured and informative form which is suitable for ML algorithms. The following sub-points were undertaken during preprocessing:

*Date of Birth to Age conversion:* Where available, customer date of birth (DOB) data was converted into an age feature, which was afterwards converted into age probability ranges.

This helped in understanding age-related fraud tendencies and allowed better generalization by binning continuous age into probabilistic intervals.

*Missing Value Check and Treatment:* A complete scan of the dataset revealed **no missing or null values**, thus eliminating the need for imputation or removal of records. This ensured model integrity without data loss.

*Amount Normalization:* Transaction amounts were standardized by converting them into real dollar values (if originally represented in sub-units or anonymized scales), allowing interpretable analysis and improved model learning.

*Redundant Feature Removal:* Certain features such as first name, last name, cc\_num and many other features, or user identifiers that did not contribute meaningfully to prediction were removed to reduce noise and prevent overfitting.

### Feature Engineering

Feature engineering aimed to derive meaningful predictors from the raw and pre-processed data to improve model performance. Both domain knowledge and data-driven techniques guided the creation of the following features:

*Geospatial Features:* Using location-based attributes, features were derived to calculate the *distance between transaction origin and user's registered location*, helping identify geographically unusual transactions.

*Temporal Features:* Additional time-based variables were extracted, such as:

- *Hour of transaction, weekday/weekend flag, and time since last transaction.*
- These were intended to model behavioral transaction patterns of both legitimate users and fraudsters.

### Probability-Based Encoding

- Categorical features like merchant\_category and amount were encoded using **probability ratio encoding**, where the probability of fraud for each category was calculated and used as the encoded value.

- This helped capture the inherent fraud tendency within each category more effectively than standard encoding.

These engineered features significantly enhanced the input space, allowing the model to detect subtle fraud signals often missed in raw features.

### Exploratory Data Analysis (EDA)

It is conducted to better understand the dataset, identify feature importance, and inform preprocessing and model training strategies. Key aspects of EDA included:

#### Class Imbalance Detection:

The dataset exhibited a severe imbalance, with fraud cases constituting less than 1% of the total. This highlighted the need for careful resampling or loss function adjustments.

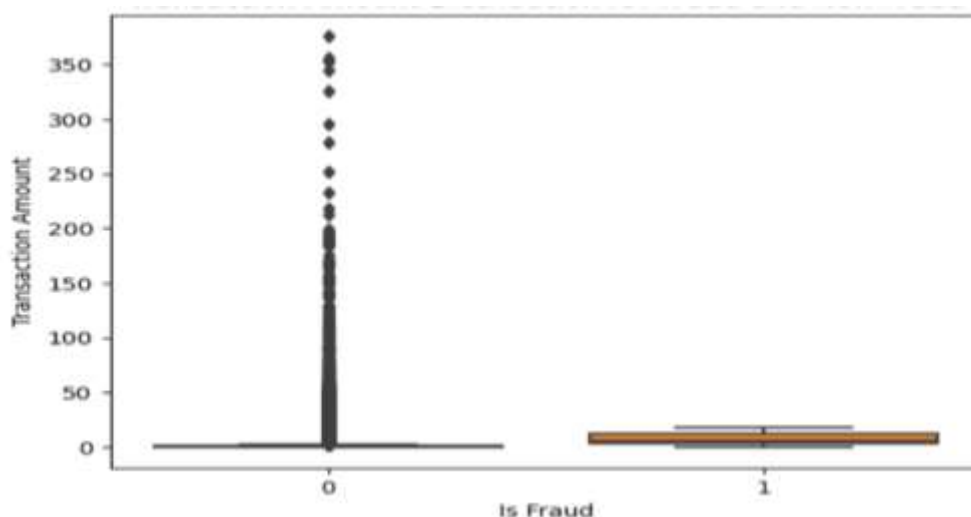


Figure 2: Transaction Amount Distribution of Fraud and Non-fraud

### Distribution and Outlier Analysis:

Distribution plots (e.g., histograms, box plots) were used to examine numerical features. Fraud cases often exhibited distinct patterns, such as higher transaction amounts or irregular timing.

### Categorical Variable Profiling:

Fraud ratios across categorical variables were analysed. Variables with highly skewed fraud distributions were prioritized for encoding using fraud-based probability encodings.

EDA provided critical insights into feature relevance and allowed strategic decisions regarding encoding, normalization, and modelling focus.

### Feature Scaling

Applied **Standard Scaler** to normalize feature values, ensuring consistent model input.

### Class Imbalance Handling

Credit card fraud datasets are highly imbalanced by nature, often containing less than 1% fraudulent transactions. This severe skew can lead machine learning models to become biased toward the majority class, resulting in high accuracy but poor recall for fraud detection. To address this, a hybrid class imbalance mitigation strategy was adopted:

#### Resampling Strategy – 1:4 Ratio Creation:

- The original dataset was rebalanced to create a **1:4 fraud-to-non-fraud ratio**, meaning for every fraud case, four legitimate transactions were retained.
- Under sampling of the majority class was preferred to avoid synthetic noise and preserve true fraudulent patterns.
- This ratio was selected based on empirical testing, balancing the trade-off between retaining useful majority class data and improving minority class representation.

### Class Weighting in Loss Function:

Instead of solely relying on resampling, **class weights** were applied in the loss function to penalize misclassification of minority (fraud) instances more heavily.

This was especially effective in the context of **Focal Loss**, where class weights ( $\alpha$ ) helped focus learning on harder-to-classify examples:

$$\text{Focal Loss} = -\alpha_t(1 - p_t)^\gamma \log(p_t)$$

Here,  $\alpha$  alpha is the weight assigned to class  $t_1$ , and  $\gamma$  is the focusing parameter.

### Avoiding Overfitting to Minority Class:

To ensure that balancing did not lead to overfitting on the minority class, techniques like dropout, validation-based early stopping, and shuffled batching were used during training.

### Evaluation on Original Distribution:

While the model was trained on the balanced dataset, evaluation was always performed on the original, imbalanced test set to simulate real-world performance.

This dual strategy of **resampling and class-weighted loss** enabled the model to learn meaningful fraud patterns without being overwhelmed by the abundance of legitimate transactions.

### Dataset Splitting

After preprocessing and class balancing, the dataset was partitioned into training and testing sets to allow model evaluation under realistic conditions:

#### Training-Test Split

80% of the rebalanced dataset (1:4 fraud to non-fraud) was used for model training, with the remaining 20% set aside for testing in an 80:20 split.

To ensure that the same class distribution was kept across both sets, the split was graded on the target variables.

The split was **stratified** on the target variable to ensure that the same class distribution was preserved across both sets.

### Random State Control:

During the splitting process we use random seed to ensure the reproducibility of results and consistency across experiments.

### Validation Strategy

Throughout training going forward split (typically 10-15 % of the training set) is used as a validation set for tracking overfitting and triggering early stopping.

This careful division ensures that the model was trained on indicative data and tested on previously unknown examples, which enables trustworthy performance metrics.

### Model Architecture: Multilayer Perceptron (MLP)

The MLP model, is a deep learning-based suggested model that is selected for its capability to capture complex model, and create non-linear relationships between features and the target label (fraud/non-fraud).

MLP or Multilayer Perceptron model is a type of feedforward artificial neural networks which comprises on three or more layers: an input layer, one or more hidden layers and an output layer. This type of structure allows MLPs to learn complex, non-linear relationships by progressively deriving hierarchical patterns from input data [47]. As

the data flows through the network, each layer transforms its input via weighted summations and activation functions, eventually producing the final prediction. Due to this structure, MLPs are majorly used in various applications such as classification, prediction, and pattern recognition [48].

**Table 1: Hyperparameter with values**

Parameter	Value
Model Type	Multilayer Perceptron
Class ratio(Fraud:Nonfraud)	1:4
Loss Function	Focal Loss
Optimizer	Adam
Learning Rate	0.001
Batch Size	32
Number of Epochs	20

**Table 2: Multilayer Perceptron Network Architecture**

Layer Type	Layer Index	Number of Nodes	Activation	Dropout Rate
Input Layer	1	43		
Hidden Layer 1	2	128	ReLU	0.4
Hidden Layer 2	3	64	ReLU	0.3
Hidden Layer 3	4	32	ReLU	0.2
Output Layer	5	1	Sigmoid	0

Table 2 architecture is empirically chosen for its strong performance on structured tabular data, its flexibility and its ability to generalize well across different fraud patterns.

#### Input Layer

Input layer acquires final feature vector as input (which includes engineered and scaled features)

#### Hidden Layers

In Hidden layers three fully connected (dense) layers are implemented with ReLU activation functions:

First Layer: 128 neurons with dropout (rate = 0.4)

Second Layer: 64 neurons with dropout (rate = 0.3)

Third Layer: 32 neurons with dropout (rate = 0.2)

To decrease overfitting and improve generalization on each layer Dropout regularization was applied.

#### Output Layer

To output the probability of the transaction being fraudulent Sigmoid activation function with a single neuron is used.

#### Loss Function

To give more importance to minorities instead of Binary Cross-Entropy we use **Focal Loss**.

Parameters used:  $\alpha = 0.25$  (class weight),  $\gamma = 2.0$  (focusing parameter).

#### Optimizer

For its adaptive learning rate capability **Adam optimizer** was selected it is set an initial learning rate of 0.0001.

For its strong performance on structured tabular data, it's flexibility and its ability to generalise well across varying fraud patterns.

#### Model Training Strategy



To optimize model performance while avoiding overfitting the training process was designed.

#### Epochs and Batch Size:

For 20 epochs with a Batch size of 32 which allows multiple weight updates per pass through the data for faster convergence this model was trained.

#### Early Stopping:

If no improvement was seen over several epochs training was monitored using validation loss and early stopping is also implemented which prevents unnecessary computations and overfitting.

#### Shuffled Batching:

Input data was shuffled at each epoch to avoid any hidden ordering bias during training.

To avoid any hidden ordering bias during training input data was shuffled.

#### Evaluation During Training:

To guide model improvement, metrics such as recall, precision and loss are monitored on the validation set at the end of each epoch.

To suggest model improvement various metrics such as precision, recall and loss is observed at the end of each epoch.

**Table 3: Model Training and Validation Performance with Selected Epochs**

Epoch	Training Accuracy	Training Loss	Validation Accuracy	Validation Loss	Observation
1	0.8753	0.0120	0.9398	0.0040	Model begins generalizing, but still underfitting; relatively high training loss.
10	0.9511	0.0021	0.9612	0.0014	Significant learning achieved; training and validation accuracy steadily improve.
15	0.9540	0.0018	0.9629	0.0013	Model approaches convergence; minimal gap between training and validation loss.
20	0.9570	0.0017	0.9633	0.0012	Optimal performance achieved; high stability with no sign of overfitting.

These structured values shown in the Table3 training process ensured that the final model was robust, generalizable, and capable of detecting fraud under real-world conditions.

## RESULT

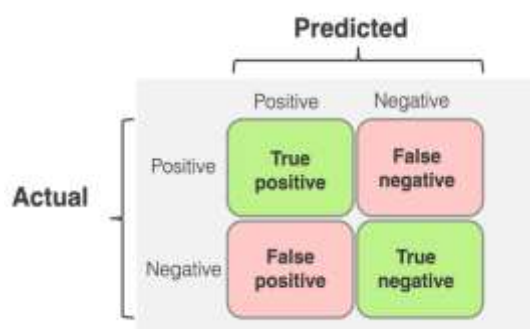
The model was accessed based on the untouched test set using various performance metrics to identify its ability to identify fraud:

#### Confusion Matrix Analysis

To analyse classification behaviour of the model, True Positive (TP), True Negative (TN) and False Positive (FP), False Negative (FN) is calculated. TP, TN, FP, FN are calculated to identify classification conduct.

#### Performance Evaluation

The consequential phase of this research contains identification of the effectiveness of the CCFD model. This performance testing targets to identify the model [39] suitability for practical use. Multiple evaluation parameters are used which includes Accuracy (Ac), Recall (Re), Precision (Pr), F1 Score (F1), and Area Under the Curve (AUC) [49].



**Figure 2: Confusion Matrix**

These parameters in figure 2 provides effectiveness and reliability of the classification model using comprehensive assessment. The formulas for each parameter are provided in Equations 11 - 15[49].

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+TN+PN} \quad (11)$$

$$\text{Precision} = \frac{TP}{TP+TF} \quad (12)$$

$$\text{Recall} = \frac{TP}{TP+TN} \quad (13)$$

$$\text{F1 Score} = \frac{2 \times \text{Precision} \times \text{recall}}{\text{precision} + \text{recall}} \quad (14)$$

**Precision:** Measures the proportion of predicted frauds that were actually fraudulent. A high precision (97%) indicates low false positives.

**Recall:** Measures the ability to detect actual frauds. The recall (85%) shows the model's effectiveness in catching fraud.

**F1-Score:** Harmonic mean of precision and recall (90%), reflecting a good balance between detection and error control.

**PR-AUC Curve:** Applied to measure the model's effectiveness in distinguish between the two classes across thresholds.

All metrics were computed on the **original imbalanced test set**, not the balanced training set, to reflect real-world deployment conditions. The result shows in below table 3:

**Table 3: Classification Report for Class 1**

Precision	Recall	F1-score
97%	85%	90%

This evaluation strategy that shows as above table 3 ensured that the model's reported performance metrics were both comprehensive and practically meaningful.

#### Proposed Model

The proposed deep learning-based fraud detection system, trained on a strategically balanced and feature-rich dataset, achieved strong results across all evaluation metrics. Its robustness in handling class imbalance, ability to learn from complex feature interactions, and generalizability to unseen transactions position it as a feasible method for detecting real-time credit card fraud transaction in high-risk financial environments.

## RESULTS AND DISCUSSION

This section presents the experimental findings of the proposed **enhanced MLP-based credit card fraud detection model**, which integrates class rebalancing, class weights, and a custom Focal Loss function to improve performance on imbalanced data.

The proposed **Multi-Layer Perceptron (MLP) model** demonstrated strong performance in identifying fraud transactions, with an overall **accuracy of 96.29%**. The model's performance was assessed across both **Class 0 (Non-Fraudulent Transactions)** and **Class 1 (Fraudulent Transactions)** using key classification metrics:

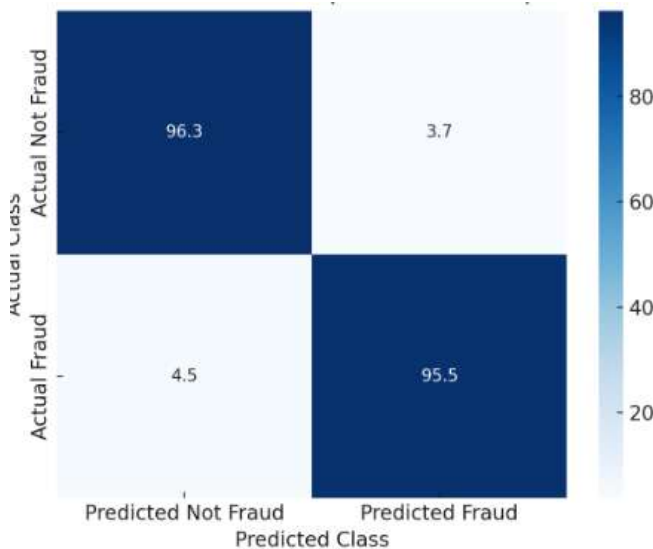
The model's effectiveness was assessed using a classification report generated based on the test data. Key performance metrics such as **precision**, **F1-score**, **recall** and **accuracy** were considered, particularly focusing on the **fraud class**, which is the most critical in fraud detection systems. The results are summarized in Table 4.

**Table 4: Classification Report of Proposed Model**

Class	Precision	F1-score	Recall
<b>Fraud</b>	<b>0.97</b>	<b>0.90</b>	<b>0.85</b>
<b>Non-Fraud</b>	0.96	0.98	0.99

For **Class 0 (Non-Fraudulent Transactions)**, the model attained a **precision of 96%**, an **F1-score of 98%** and a **recall of 99%**, indicating that the model was highly effective in correctly identifying genuine transactions with minimal misclassification. The high recall suggests that nearly all legitimate transactions were correctly classified, ensuring a low rate of false positives.

For **Class 1 (Fraudulent Transactions)**, the model attained a **precision of 97%**, meaning the model was model was 97% correct when predicting a fraudulent transaction. However, the **recall for fraud cases was 85%**, indicating that while the model successfully detected a significant proportion of fraudulent transactions, some fraud instances were still missed. The **F1-score for fraud detection was 90%**, highlighting a balanced performance between recall and precision.

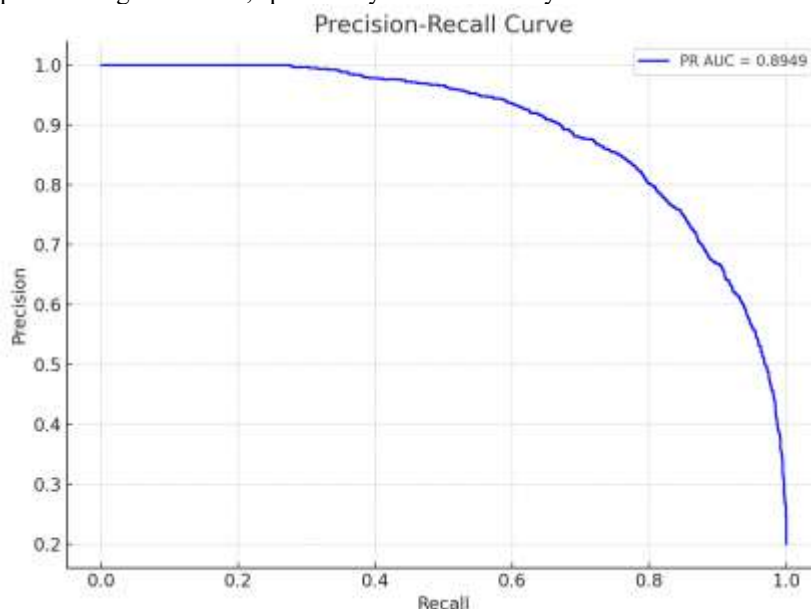


**Figure 3: Normalized Confusion Matrix of Proposed Model**

The normalized confusion matrix, as illustrated in Figure 3, demonstrates the classification performance of the proposed model. The model accurately identified 96.3% of legitimate transactions and 95.5% of non-transactions. The misclassification rates remain low, with only 3.7% of non-fraud cases and 4.5% of fraud cases incorrectly predicted. These results highlight the model's proficiency in discriminating between non-legitimate transactions and legitimate transactions, even under class imbalance conditions.

#### Precision-Recall Curve Analysis

Given the skewed distribution of the dataset, a **Precision-Recall (PR) curve** was used instead of the traditional ROC curve to better analyse the classifier's performance. The PR curve offers a more informative view by plotting precision against recall, specifically for the minority class.



**Figure 4: PR-AUC curve of the Proposed Model**

The PR-AUC curve in Figure 4 for the proposed model shows a **reliably high precision over a wide spectrum of recall values**, showing that the proposed model not only captures fraudulent transactions effectively but also minimizes the count of false alarm. The **high area under the PR-AUC curve** confirms the model's robustness and discrimination power when applied to fraud detection tasks. This also demonstrates the advantage of integrating **Focal Loss** and **class weights** into the MLP training process.

To mitigate the challenge of **class imbalance**, a **1:4 fraud-to-non-fraud ratio** was implemented during data preprocessing. This ensured that fraudulent transactions were adequately represented without over-sampling, leading to an improvement in fraud recall. **Feature scaling using Standard Scaler** helped stabilize the training



process and improve model convergence. Additionally, a **custom focal loss function** was applied to assign higher penalties to misclassified fraud cases, enhancing the model's sensitivity to fraudulent transactions and improving its detection capability.

The model architecture included **three dense layers (128-64-32 neurons) with ReLU activation functions**, designed to learn intricate transaction patterns. **Dropout layers (0.4, 0.3, 0.2) were integrated** at different stages to reduce overfitting and improve generalization. The model was optimized with the Adam optimizer at a learning rate of 0.001, resulting in consistent learning and performance improvements across training epochs.

## CONCLUSION

This research demonstrates that a carefully constructed deep learning model, when combined with advanced preprocessing, engineered features, and appropriate imbalance handling, can substantially improve credit card fraud detection. By transforming raw transaction data into behaviourally and statistically rich feature sets, the model learned to capture nuanced patterns in fraudulent activity. The use of focal loss, coupled with a rebalanced training dataset, allowed the model to prioritize rare fraud cases without sacrificing generalization to legitimate transactions. The proposed model demonstrates substantial improvement in detecting fraudulent transactions, achieving a recall of 0.85, precision of 0.97, F1-score of 0.90, and an AUC of 0.99—clearly outperforming the baseline MLP model, which exhibited a recall of only 0.10 and an PR-AUC of 0.89. These improvements indicate that integrating preprocessing techniques with tailored loss functions significantly enhances the model's sensitivity to the minority class. These results validate the applicability of deep neural networks in high-risk financial applications and highlight the need for domain-informed feature design and class imbalance mitigation. Despite the promising results, certain limitations remain. The model evaluation was confined to a single primary dataset, and the resampling strategy used static class ratios. Future work may extend this framework by integrating sequential models such as LSTM or Transformer architectures to exploit temporal dependencies in transactional sequences, further enhancing fraud detection capabilities.

## REFERENCES

1. Karthik, V. S. S., Abinash Mishra, and U. Srinivasulu Reddy. "Credit card fraud detection by modelling behaviour pattern using hybrid ensemble model." *Arabian Journal for Science and Engineering* 47.2 (2022): 1987-1997.
2. Li, Zhenchuan, et al. "A hybrid method with dynamic weighted entropy for handling the problem of class imbalance with overlap in credit card fraud detection." *Expert Systems with Applications* 175 (2021): 114750.
3. Lebichot, Bertrand, et al. "Incremental learning strategies for credit cards fraud detection." *International Journal of Data Science and Analytics* 12.2 (2021): 165-174.
4. Zhang, Xinwei, et al. "HOBAs: A novel feature engineering methodology for credit card fraud detection with a deep learning architecture." *Information Sciences* 557 (2021): 302-316.
5. Bakhtiari, Saeid, Zahra Nasiri, and Javad Vahidi. "Credit card fraud detection using ensemble data mining methods." *Multimedia Tools and Applications* 82.19 (2023): 29057-29075.
6. Yang, Ming-Hour, et al. "Contactless credit cards payment fraud protection by ambient authentication." *Sensors* 22.5 (2022): 1989.
7. Wang, Jiacheng, et al. "Approx-SMOTE federated learning credit card fraud detection system." *2023 IEEE 47th Annual Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 2023.
8. Abd El-Naby, Aya, Ezz El-Din Hemdan, and Ayman El-Sayed. "An efficient fraud detection framework with credit card imbalanced data in financial services." *Multimedia tools and applications* 82.3 (2023): 4139-4160.
9. Alarfaj, Fawaz Khaled, et al. "Credit card fraud detection using state-of-the-art machine learning and deep learning algorithms." *Ieee Access* 10 (2022): 39700-39715.
10. Islam, Md Amirul, et al. "An ensemble learning approach for anomaly detection in credit card data with imbalanced and overlapped classes." *Journal of Information Security and Applications* 78 (2023): 103618.
11. Dang, Tran Khanh, et al. "Machine learning based on resampling approaches and deep reinforcement learning for credit card fraud detection systems." *Applied Sciences* 11.21 (2021): 10004.
12. Mienye, Ibomoiye Domor, and Nobert Jere. "A survey of decision trees: Concepts, algorithms, and applications." *IEEE access* (2024).
13. Dong, Shi, Yuanjun Xia, and Tao Peng. "Network abnormal traffic detection model based on semi-supervised deep reinforcement learning." *IEEE Transactions on Network and Service Management* 18.4 (2021): 4197-4212.
14. Btoush, Eyad Abdel Latif Marazqah, et al. "A systematic review of literature on credit card cyber fraud detection using machine and deep learning." *PeerJ Computer Science* 9 (2023): e1278.
15. Bin Sulaiman, Rejwan, Vitaly Schetinin, and Paul Sant. "Review of machine learning approach on credit card fraud detection." *Human-Centric Intelligent Systems* 2.1 (2022): 55-68.

16. Osegi, E. N., and E. F. Jumbo. "Comparative analysis of credit card fraud detection in simulated annealing trained artificial neural network and hierarchical temporal memory." *Machine Learning with Applications* 6 (2021): 100080.
17. Wang, Pin, En Fan, and Peng Wang. "Comparative analysis of image classification algorithms based on traditional machine learning and deep learning." *Pattern recognition letters* 141 (2021): 61-67.
18. Mienye, Ibomoye Domor, and Yanxia Sun. "A deep learning ensemble with data resampling for credit card fraud detection." *Ieee Access* 11 (2023): 30628-30638.
19. Joloudari, Javad Hassannataj, et al. "Effective class-imbalance learning based on SMOTE and convolutional neural networks." *Applied Sciences* 13.6 (2023): 4006.
20. de Zarzà i Cubero, Irene, Joaquim de Curtò i Díaz, and Carlos T. Calafate. "Optimizing Neural Networks for Imbalanced Data." (2023).
21. Riffi, Jamal, et al. "Credit card fraud detection based on multilayer perceptron and extreme learning machine architectures." *2020 International Conference on Intelligent Systems and Computer Vision (ISCV)*. IEEE, 2020.
22. Garg, Deepali, Uma Sharma, and Umesh Kumar. "Enhancing Credit Card Fraud Detection: Feature Utilization Challenges and Stacked Model Approaches."
23. Ni, Lina, et al. "Fraud feature boosting mechanism and spiral oversampling balancing technique for credit card fraud detection." *IEEE Transactions on Computational Social Systems* 11.2 (2023): 1615-1630.
24. Fanai, Hosein, and Hossein Abbasimehr. "A novel combined approach based on deep Autoencoder and deep classifiers for credit card fraud detection." *Expert Systems with Applications* 217 (2023): 119562.
25. Itoo, Fayaz, Meenakshi, and Satwinder Singh. "Comparison and analysis of logistic regression, Naïve Bayes and KNN machine learning algorithms for credit card fraud detection." *International Journal of Information Technology* 13.4 (2021): 1503-1511.
26. Hussain, SK Saddam, et al. "Fraud detection in credit card transactions using SVM and random forest algorithms." *2021 Fifth international conference on I-SMAC (IoT in social, mobile, analytics and cloud)(I-SMAC)*. IEEE, 2021.
27. Mienye, Ibomoye Domor, Yanxia Sun, and Zenghui Wang. "Prediction performance of improved decision tree-based algorithms: a review." *Procedia Manufacturing* 35 (2019): 698-703.
28. Randhawa, Kuldeep, et al. "Credit card fraud detection using AdaBoost and majority voting." *IEEE access* 6 (2018): 14277-14284.
29. Lin, Tzu-Hsuan, and Jehn-Ruey Jiang. "Credit card fraud detection with autoencoder and probabilistic random forest." *Mathematics* 9.21 (2021): 2683.
30. Asha, R. B., and Suresh Kumar KR. "Credit card fraud detection using artificial neural network." *Global Transitions Proceedings* 2.1 (2021): 35-41.
31. Ebiaredoh-Mienye, Sarah A., et al. "A machine learning method with filter-based feature selection for improved prediction of chronic kidney disease." *Bioengineering* 9.8 (2022): 350.
32. Ho, Cowan, et al. "A promising deep learning-assistive algorithm for histopathological screening of colorectal cancer." *Scientific reports* 12.1 (2022): 2222.
33. Nguyen, Giang, et al. "Machine learning and deep learning frameworks and libraries for large-scale data mining: a survey." *Artificial Intelligence Review* 52 (2019): 77-124.
34. Alhumoud, Sarah Omar, and Asma Ali Al Wazrah. "Arabic sentiment analysis using recurrent neural networks: a review." *Artificial Intelligence Review* 55.1 (2022): 707-748.
35. Zhong, Zhihang, et al. "Real-world video deblurring: A benchmark dataset and an efficient recurrent neural network." *International Journal of Computer Vision* 131.1 (2023): 284-301.
36. Shen, Feng, et al. "A new deep learning ensemble credit risk evaluation model with an improved synthetic minority oversampling technique." *Applied Soft Computing* 98 (2021): 106852.
37. Tsantekidis, Avraam, Nikolaos Passalis, and Anastasios Tefas. "Recurrent neural networks." *Deep learning for robot perception and cognition*. Academic Press, 2022. 101-115.
38. Benchaji, Ibtissam, et al. "Enhanced credit card fraud detection based on attention mechanism and LSTM deep model." *Journal of Big Data* 8 (2021): 1-21.
39. Xie, Yu, et al. "Learning transactional behavioral representations for credit card fraud detection." *IEEE Transactions on Neural Networks and Learning Systems* (2022).
40. Mishra, Sashikala, et al. "Improving the accuracy of ensemble machine learning classification models using a novel bit-fusion algorithm for healthcare AI systems." *Frontiers in Public Health* 10 (2022): 858282.
41. Mienye, Ibomoye Domor, et al. "Enhanced prediction of chronic kidney disease using feature selection and boosted classifiers." *International conference on intelligent systems design and applications*. Cham: Springer International Publishing, 2021.
42. Bikku, Thulasi. "Multi-layered deep learning perceptron approach for health risk prediction." *Journal of Big Data* 7.1 (2020): 50.
43. Moodi, Yaser, Mohammad Ghasemi, and Seyed Roohollah Mousavi. "Estimating the compressive strength of rectangular fiber reinforced polymer-confined columns using multilayer perceptron, radial basis function, and support vector regression methods." *Journal of Reinforced Plastics and Composites* 41.3-4 (2022): 130-146.

44. Agahian, Saeid, and Taymaz Akan. "Battle royale optimizer for training multi-layer perceptron." *Evolving Systems* 13.4 (2022): 563-575.
45. Mienye, Ibomoye Domor, and Yanxia Sun. "A deep learning ensemble with data resampling for credit card fraud detection." *Ieee Access* 11 (2023): 30628-30638.
46. Afriyie, Jonathan Kwaku, et al. "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions." *Decision Analytics Journal* 6 (2023): 100163.
47. Rojas, Matías Gabriel, Ana Carolina Olivera, and Pablo Javier Vidal. "Optimising Multilayer Perceptron weights and biases through a Cellular Genetic Algorithm for medical data classification." *Array* 14 (2022): 100173.
48. Safari, Ehram, and Mozhdeh Peykari. "Improving the multilayer Perceptron neural network using teaching-learning optimization algorithm in detecting credit card fraud." *Journal of Industrial and Systems Engineering* 14.2 (2022): 159-171.
49. Priatna, Wowon, et al. "Optimizing Multilayer Perceptron with Cost-Sensitive Learning for Addressing Class Imbalance in Credit Card Fraud Detection." *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)* 8.4 (2024): 563-570.
- 50.