© DEC 2025 | IRE Journals | Volume 9 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I6-1713053

A Machine-Learning Framework: Integrating MLP And SMOTE For Deceitful Payment Classifications

LATEEF G. SALAUDEEN[1], BABATOLA MOSES OMILODI[2], MICHAEL O. ASANBE[3], ODUNTAN ESTHER ODUNNAYO[4], OMOBOLANLE ESTHER AKINJISOLA[5], TEMITOPE MOSUNMOLA OLATUNJI[6], EMMANUEL ABIODUN[7]

[1, 2, 3, 5, 6, 7]*Department of Computer Sciences, College of Natural and Applied Sciences, Chrisland University, Abeokuta, Owode-Ajebo Road, Abeokuta, Ogun State Nigeria.*

[4]*Department of Computer Science, Federal Polytechnic, Ilaro, Ogun State, Nigeria*

Abstract- ***In this study, Multiple Layer Perceptron's (MLP) integrating Synthetic Minority Oversampling Technique (SMOTE) was offer as potential solution to the despicable problem of payment fraud. This model was design and realized on Google Colab platform embedding GPU, where Tensorflow was fit for deep learning (DL), and Scikit learn for machine learning (ML) model respectively. Python was the modeling language. Firstly, baseline experiment was conduct on orthodox ML models of Random Forest (RF), Logistics Regression (LR), Isolation Forest (iforest) with MLP for feature selection and engineering. While, probing kaggle dataset. This dataset is highly imbalance, a bait to the ML challenges suffering in the baseline trial. However, resampling method of SMOTE was applied in the second trial to balance the dataset, address over-fitting with under-fitting problem and improved on the utilized model performances. In testing for these models' efficacy, confusion matrix and performance evaluation metric were explored. This revealed the outcome of the balancing model trial, where the proposed MLP+SMOTE exercises superclass performance against other models. Presenting accuracy score of 0.95%, Error Rate of 0.05%. Recall of 0.98%, least False Positive Rate of 0.07%, True Negative Rate of 0.93%, Precision of 0.93%, Prevalence of 0.46%, Null Error Rate of 100%, Cohen kappa of 0.42%, F1-Score of 0.95% and Matthews Correlation Coefficient of 0.91% respectively. This result validates the developed model as amazing in performance, when compared with benchmark studies; and it is promising in the classification of deceitful payment transaction.***

Keywords: ***Payment card, Credit card fraud, Confusion Matrix, Performance Evaluation Metrics***

I. INTRODUCTION

Credit card fraud otherwise known as payment fraud; is an inclusive term, succinctly described as the use of any akin type of payment card in the purchase of goods and services with the intention of dodging payments. This transgression is link with a payment card theft by fraudster. In making unauthorized usage of another individual payment card credentials to charge purchases to an account for fraudster to keep. Besides, this act can be committed in two manners; either through online and offline fraud procedures; these (Al-Smadi, 2021; Salaudeen et al., 2024a) clarified in their respective study.

The threats arising from the upsurge of this fraudulent payment card deeds are baffling, ransacking and engraining on daily basis, due to the significance of credit card usage for transactions (Aslam and Hussain, 2024; Akinola et al., 2023). Credit card is a small plastic card issued to countless account owners pledging for appropriate financial services. This card act as scheme of payment, permissible and tenable across the globe to facilitates the procurement of merchandises (i.e., goods and services). At any grocery stores with the aid of virtual (online) card transaction in actualizing the intent of global cashless policy as economy enabler (Al-Smadi, 2021). This card however, has an overabundance benefit, including easy access to credit, purchase which offers guarantee method of payment through cardholders in abiding with cashless policy promulgation. More so, the prowess of the credit card is not limited to enhancing customer spending, rather support economic growths that avails with rewards and benefits of contactless payment, which encourages literacy. Besides, this prowess does not only motivate fraudsters to abuse the payment cards for selfish financial benefits, but as well provides the chances for them to re-strategies and spearheads their deceit act in launching several other forms of credit card fraud attacks. While, adopting new and indigenous methods of data breaches, identity theft, stolen credit card imprints and skimmers, corporate account take over (CATO), phishing and social

engineering fraud and many others. Al-Samdi (2021) study discussed, as fraudsters advance in their treacherous act in boycotting fraud prevention schemes. The implication of this doings infiltrates derogatory financial losses, cash back with other derisive effects. Perhaps, this triggers national security threat and vulnerabilities (Salaudeen eta., 2024b). To this effect, alertness is required in devising counter-measure. This study is organized in the following trend Section 2 discusses related works on payment fraud. Section 3 deliberates about materials and method, covering data collection, preprocessing, and tools used. Section 4 analyzes results and compares them with benchmark studies to establish findings. Finally, Section 5 concludes with insights and recommendations.

II. RELATED WORKS

In the previous work of Salaudeen et al., (2024a), Salaudeen et al., (2024b) and Salaudeen et al., (2025), the concepts of credit card fraud were explained. Where hybrid approach of deep learning models was channel towards the classification of credit card transaction. These works present eloquent results that can assist financial institution towards the determent of inferences of fraudulent credit card transaction.

Akinola et al., (2023) study deploy two ML models of LR and Isolation Forest to sort payment fraud. Kaggle dataset that suffered from imbalance in class distribution was apply. In evaluating their model performances. Precision, recall, F1-score and AUC-ROC curve were explored. The researchers had an oversight to address the challenge inbound with ML before presenting their findings. The research established LR model offering accuracy score of 99.91% for training data and 78% for testing data as best model performance. With precision, recall and F1-score of 0.95%, 0.56% and 0.70% correspondingly. Contrarily, Isolation Forest offers accuracy result of 99.8% for training data and 74% for testing data. While, its precision, recall and F1-score remained 0.49% distinctively.

Mienye and Sun (2023) study offers a robust DL method incorporating long short-term memory and gated recurrent neural networks as base learners in a stacking ensemble structure. In addition, hybrid SMOTE and edited nearest neighbor method was deploy to balance the dataset engaged in the study. Its outcome exhibited that the offer DL ensemble with the SMOTE-ENN method achieved a sensitivity and specificity result of 1.00% and 0.99% respectively, which is greater to the existing ML classifier in related study.

Alraddadi (2023) study advocates decision tree algorithm for payment fraud detection. A survey was conduct to examine learners' opinion towards fraud occurrences. Records of 102 learners across diverse institutions and countries round the globe was collect. The survey outcome shown that 96% of the learners are acquainted to how payment fraud occurs While 4.1% of them are not. Conversely, 82% specified their proclivity in training a tool based on the anticipated model to curtail payment fraud incidents.

In 2021, Fayyomi et al., study surveyed several approaches precisely six models, for identifying credit card fraud. The Scholar compared diverse ML models of LR, DT, RF, ANN, KNN, and K-means clustering in terms of their shortcomings and recompenses. Because not all their application scenarios are the same, as a scenario-based algorithm can be employed to decide which scenario is the best fit for that situation. The researchers also engaged diverse performance measures methods and algorithms to predict and show fraudulent transactions. Studies are refreshed and encouraged to improve the fraud detection basis to determine the weight that is suitable with cost factors, the tested accuracy, and detection accuracy. Surveys of this kind allow other researchers to build a hybrid approach most accurate for fraudulent credit card transaction.

Aghware et al., (2023) study offer ML model of a profile hidden Markov model and deep neural network and ensemble approach. The research shows that the ensemble method is effective in classifying the benign transactions with a precision of 97 percent.

Prasad et al., (2023) employs an ensemble technique to improve credit card fraud detection. The scholar focusses on optimizing model parameters, improving performance measures, and integrating deep learning to fix identification errors and reduce false negatives. DT, XGBoost, LR, RF, and SVM were used in this paper. The paper compares these algorithms across multiple evaluation metrics and

finds that DT performs best with a 100% recall value, followed by XGB, LR, RF, and SVM with 85%, 74.49%, 75.9%, and 69%, respectively. By combining multiple classifier ensembles and rigorously assessing their performance, this research impressively improves CCFD system efficiency. But the evaluation parameters expose the low performance of the model.

Devi and Parthibranjanray (2023) study deploy ML model of CNN along with Artificial Intelligence to explore kaggle dataset for payment fraud detection. The research outcome present accuracy score of 99.8%, which is quite high compared to preceding models like RF, LR and SVM in their yardstick literature. The study develops a webapp software, which have high rate of accuracy and precision for predicting fraud.

Madhavi et al., (2023) study just like previous study engaged CNN on dataset obtained from kaggle repository to identify and classified fraudulent credit card transaction into genuine and fraudulent classes and minimized the number of false alerts. The model performance was evaluated based on accuracy, precision, error rate, recalls and f1-score. The researcher further compared CNN model performance with RF and LR. It was discovered that CNN model shown the best result. However, the research did not state the percent of the CNN model.

Khalid et al., (2024) study engaged ensemble model that integrates SVM, KNN, RF, Bagging, and Boosting classifiers within a voting framework. The scholar's employs SMOTE under-sampling and the ensemble techniques to tackle the imbalance distribution class challenges. The method of the proposed model encompasses data pre-processing, feature engineering, model selection, and evaluation, with Google Colab computational capabilities facilitating efficient model training and testing. Comparative analysis among the proposed ensemble model, traditional ML models, and individual classifiers reveals the superior performance of the ensemble in mitigating challenges associated with credit card fraud detection. Across accuracy, precision, recall, and F1-score metrics, the ensemble outperforms existing models. This paper underscores the efficiency of ensemble methods as a valuable tool in the battle against fraudulent transactions. The results presented lay the groundwork for future advancements in the development of more resilient and adaptive fraud detection systems, which will become crucial as credit card fraud techniques continue to evolve.

Aslam and Hussain (2024) study measured the efficiency of six ML models of LR, RF, extra tree, XGB, LGBM and Categorical Boosting (CatBoost) using a publicly available dataset on credit card transaction performed by EU cardholders in 2023, comprising over 550,000 records. The study engaged the dataset to assess the performance of ML models in measuring accuracy, recall and F1-scores play confusion matrix; to achieve high accuracy and precision in the credit card fraud detection dataset, with a reported accuracy, recall and F1- score of 1.00 for both classes.

From the literature assessments carried out, it can be inferred that most researcher addresses the challenges of payment fraud. By identifying divergence in class distribution of any kaggle dataset applied. The datasets which are inbound with the challenges of from high dimensionality and sparsity. Most models deploy for regularities are outwit by ML challenges of unavailability of real-life dataset for experiment. Given these constraints, research in this domain remains particularly challenging, with unresolved gaps that call into question why financial institutions still struggle to effectively curtail payment fraud. However, there is need for an improved and more refined tactic for the detection of payment fraud by financial institutions (Salaudeen et al., 2025).

Khalid et al., (2024) and Salaudeen et al., (2024b) in their study advised on techniques that can be used to address the challenges inbound with kaggle dataset. Either through the exploration of data augmentation techniques or resampling methods and others. Besides, the methods involved in the existing studies are moderate for exponent results in taming the inferences of payment fraud. This study seeks to improve upon.

Al-Smadi (2021), Salaudeen et al., (2025) and Jayanthi et al., (2024) work extenuates on other methods for payment fraud prevention and detection promulgated by financial institutions and fraud expert's in classifying fraudulent financial transactions which suffers with some restrictions; this study deliberated.

© DEC 2025 | IRE Journals | Volume 9 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I6-1713053

2.1 Payment Fraud Detection and Prevention Tactics
In order to regulate the vagueness payment fraud. Credit card issuers with their financial institutions and fraud experts came up with an idea of diverse forms for fraud detection models. Using software's, processes, preventive and countermeasures tactics such as: magnetic stripes, three dimensional holograms (3Ds), Card Validation Codes (CVC), Multi-factor Authentication (MFA), Address Verification System (AVS), advance tracking and monitoring system, Biometrics and One-time password (OTP), and Tokenization as ways of mitigating payment frauds (Salaudeen et al., 2024a). In addition, the institutions evaluated the possibility of replacing payment cards with smart cards. However, their analysis found this transition to be prohibitively expensive due to the extensive Point of Sale terminals and the large number of payment cards already in circulation in the region. Instead, they anticipated detecting payment fraud using rule-based approaches or identifying anomalies in transaction across suspicious geolocations through IP addresses.
Some of these approaches are discourse below

i. Advance Credit tracking and Monitoring System:

Lake et al. (2023) quote Richard Best, finance expert at DontPayFull statement to deliberate credit monitoring services as a system that track any changes involving key credit activities. Credit monitoring services exertion was in line with credit reporting services. Where, Equifax, Experian and TransUnion are the three primary credit-reporting bureaus. They gather pertinent payment information and use it to produces reports. The report information includes payment history, account balances, available credit, account age, inquiries for new credit, and public records. These as well encompasses late payments, changes to credit limit, new accounts or account closures, and collections. It was used to detect change to payment report; one can receive an alert notifying of the nature change. Depending on the service subscribe, those alerts may come in real time, on a daily, weekly or monthly basis. If someone opens a new payment card account in your name, for instance, one will be notified from the credit monitoring service. With timely notifications. One can then take steps to stop the identity thief. These steps include contacting the credit card company, placing a fraud alert on your file or freezing your credit.

Pros of credit monitoring services

- Offer expedient access to credit scores and changes to one's credit
- Obliging for detecting fraud and managing credit health
- Allow members to take quick action to stop identity theft
- Acquires information that enable decisions making

Cons of Credit Monitoring Services

- It does not prevent errors from display up one's credit report
- Is not infallible form of identity theft protection
- Identity theft alert is tolerable after the act is committed
- Another frequent subscription to pay

ii. Rule-based Method: It was an ancient NLP method in which pre-defined linguistic rules are deploy to analyze and process textual data. Rule-based method includes relating a particular set of rules or patterns to capture specific structures, extract information to perform tasks such as text classification. Rule-based methods contain steady lexes and pattern matches (Geeksforgeeks, 2023).

Steps involves Rule-based method includes:

i. Rule Creation: This is based on desired tasks; domain-specific linguistic rules are created to involve grammar rules, syntax patterns, semantic rules or regular expressions.
ii. Rule Application: It is a pre-defined rules applied to the inputted data in capturing match patterns.
iii. Rule Processing: The text data is processed in accordance with the results of the matched rules to extract information, make decisions or other tasks and
iv. Rule Refinement: this deal with iterative refinement to improve accuracy and performance. Based on previous feedback, the rules are modified and updated when needed.

Pros of the Rule-based:

- Simply interpretable as rules are overtly defined

- Rule-based methods can help semi-automatically interpret some data in areas where data are not annotated (for example, NER (Named Entity Reorganization) tasks in a particular domain).
- Functions even with scant or poor training data
- Computation time is fast and it offers high precision
- Many times, deterministic solutions to various issues, such as tokenization, sentence breaking, or morphology, can be achieve through rules.

Cons of the Rule-based:

- Labor-intensive as more rules are needed to generalize
- Creating rules for complex tasks is laborious
- Needs regular maintenance
- May not perform well in handling variations and exceptions in language usage
- May not have a high recall metric

iii. Magnetic Stripes (Magstripe)

Pros of the Magnetic Stripes:

- Simple and widely accepted globally.
- Low production cost for cards.

Cons of the Magnetic Stripes:

- Easily cloned (skimming attacks).
- No dynamic security features (static data).
- Being phased out in favor of EMV chips.

iv. Three-Dimensional Holograms (3Ds)

Pros of 3Ds:

- Visually hard to replicate, deterring counterfeit cards.
- Enhances card authenticity verification.

Cons of 3Ds:

- Does not prevent digital fraud (e.g., online transactions).
- Expensive to produce.
- Can still be copied with advanced techniques.

v. Card Verification Code (CVC/CVV)

Pros of CVC/CVV:

- Enhances an extra layer of security for online dealings.
- Not stored in magnetic stripes or chips, reducing exposure.

Cons of CVC/CVV:

- Can be phished or stolen via malware.
- Useless if the card is physically stolen (if written on the back).

vi. Multi-Factor Authentication (MFA)

Pros of MFA:

- Stronger security by requiring multiple verification steps (e.g., password + OTP).
- Reduces unauthorized access even if one factor is compromised.

Cons of MFA:

- Can be inconvenient for users (e.g., delays in authentication).
- SIM-swapping attacks can bypass SMS-based MFA.

vii. Address Verification System

Pros of AVS:

- Helps verify cardholder billing address in online transactions.
- Reduces fraud in card-not-present (CNP) transactions.

Cons of AVS:

- Limited effectiveness (fraudsters can obtain real addresses).
- Can cause false declines if the address is mistyped.

viii. Biometrics (Fingerprint, Face Recognition)

Pros of Biometric:

- Highly secure (unique to each user).
- Difficult to spoof (compared to passwords/PINs).

Cons of Biometric:

- Requires specialized hardware (e.g., fingerprint scanners).

- Privacy concerns over biometric data storage.
- Potential for false rejections/acceptances.

ix. One-Time Password (OTP)

Pros of OTP:

- Dynamic and expires quickly, reducing reuse attacks.
- Effective against phishing (if not intercepted in real-time).

Cons of OTP:
Vulnerable to SIM-swapping or man-in-the-middle attacks.
User inconvenience (delays in receiving SMS/email).

x. Tokenization

Tokenization Pro:

- Replaces sensitive card data with a unique token, reducing exposure.
- Works well for online and mobile payments (e.g., Apple Pay, Google Pay).

Tokenization Con:

- Requires integration with payment processors.
- Does not prevent fraud if the token itself is stolen (rare but possible).

Table 8 presented the summary table for Counter-measure approaches deployed by financial institution in mitigating the inference of credit card fraud.

III. MATERIALS AND METHOD

The Figure 1 presented structure for proposed methodology framework similar to research methodology. The research methodology is a systematic approach applied in solving a research problem, which outline steps and logic behind the research procedure. It is prescriptive and includes defined steps, of why a problem is significant to be solve and how these could be accomplished. Research methodologies are best suitable for studies with clear objectives, constraints, and repeatable processes. Contrarily, the methodology framework is organized to help stayed focused on this study and ensures that each segment of the study scope is built on the previous ones. The methodology framework is prescriptive as well; it was anticipated to be adaptive to tackle the challenges of payment fraud in financial institutions. Framework is better suited for this thesis because it supports flexibility and adaptability. Both research methodology and framework are integrated for conducting well-structured research which this study adopted. The methodology framework began with the formulation of research topic, after which the problem is identify and defined while establishing the research objectives. After extensive literature review that was necessitated through the developed research plan concurrently. In this study, dataset applied was describe in section 3.1 with data Pre-processing in section 3.2, while exploring the Google Colab platform; on which binary classification task is entrenched. Foremost, on the baseline models discussed in section 4.1 using imbalances dataset on two ML models of LR and RF to determine the better performing models. Subsequently, balancing model experiment was presented in section 4.2 delving both the ML and DL models with propose enhanced hybrid MLP+SMOTE model; to present it superclass performance against other models deploy in this study. The experimentation results were engraining based on the discoveries of the confusion matrix and performance evaluation metrics.

© DEC 2025 | IRE Journals | Volume 9 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I6-1713053

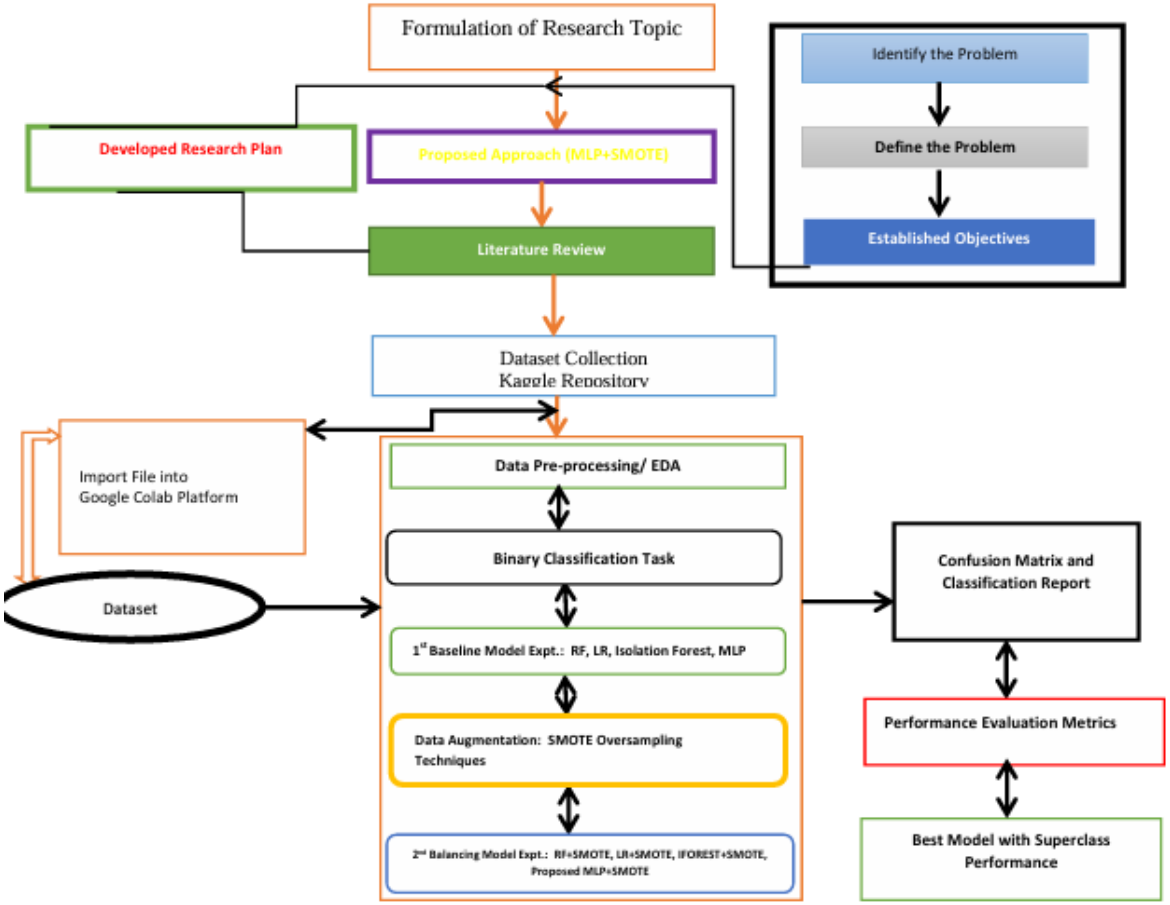

Figure 1: Proposed Methodology Framework

3.1DataCollection:

Table 1 Sample of the Kaggle Credit Card Dataset Utilized for this study

	Time	V1	V2	V3	V4	V5	V6	V7	V8
0	0	-1.359807	-0.072781	2.536347	1.378155	-0.338321	0.462388	0.239599	0.098698
1	0	1.191857	0.266151	0.166480	0.448154	0.060018	-0.082361	-0.078803	0.085102
2	1	-1.358354	-1.340163	1.773209	0.379780	-0.503198	1.800499	0.791461	0.247676
3	1	-0.966272	-0.185226	1.792993	-0.863291	-0.010309	1.247203	0.237609	0.377436
4	2	-1.158233	0.877737	1.548718	0.403034	-0.407193	0.095921	0.592941	-0.270533

© DEC 2025 | IRE Journals | Volume 9 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I6-1713053

dataset = pd.read_csv ('/content/creditcard.csv')
dataset.head ( )

5 rows * 31 columns
dataset.info ( )
<Class 'pandas.core.frame.Dataframe'>
RangeIndex: 89220 entries, 0 to 89219
Data columns (total 31 columns):
Column Non-Null Count Dtype

Table 2 and Table 3 display the summary of the dataset utilized exploring python programming command: normal_df.Amount.describe ( ); that produces for the non-fraudulent transaction distribution description. While, the python construct of fraud_df.Amount.describe ( ); display for fraudulent transaction distribution description. These is achieved under the pre-processing procedure. It was discovered that the dataset is highly skewed. Therefore, binary classification is recommended in handling the dataset (Akinola et al., 2023; Aslam & Hussain, 2024). In this study, contribution was on the conduct of baseline experiment in section 4.1 and balance model experiment in section 4.2 respectively.

Table 2: Non-Fraudulent Dataset Transaction Distribution Description

Count	Mean	Std.	Min	25%	50%	75%	Max
284315	88.3	250.11	0.00	5.65	22.0	77.05	25691.16

Table 3: Fraudulent Transaction Dataset Distribution Description

Count	Mean	Std.	Min	25%	50%	75%	Max
492	122.21	256.68	0.00	1.00	9.25	105.89	2125.87

3.2 Data Pre-processing:
It is a data preparation, analysis and model building activities stage, where many pre-processing tools and python programming language constructs are engaged to build model on datasets for transformation exploit (Devi & Parthbranjanray, 2023). This study absorbed and integrated the structure and implementation process enunciated in (Akinola et al., 2023) study for credit card fraud detection as depicted in Figure 2; this is embedded in the proposed methodology framework of Figure 1. The approach is simple with robust system architecture. The Exploratory Data Analysis (EDA) procedure is entrenching after dataset collection is obtain. Akinola et al., (2023) presented the pre-processing steps channel for this study as described in subsections 3.2.1, 3.2.2, 3.2.3, 3.2.4 and 3.2.5 below.

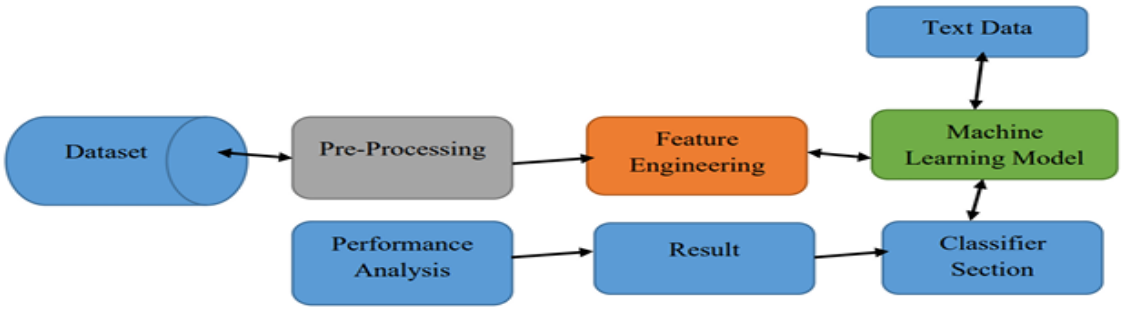

Figure 2: Proposed Architecture of (Devi and Parthibranjanray, 2023)

3.2.1 Data Cleaning:
It is part of the pre-processing step where missing values and outliers are handles. By removing duplicate values, removing irrelevant data, Standard Capitalization, Correcting and converting data types, correcting formatting, and Language Translation (Devi and Parthibranjanray, 2023).

3.2.2 Encoding the categorical data:
This is the task of converting to numerical variables and it was ably deliberated in (Akinola et al., 2023) study. Figure 3 depicts the datasets feature together with the Classes' Negative Correlation illustrations.

© DEC 2025 | IRE Journals | Volume 9 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I6-1713053

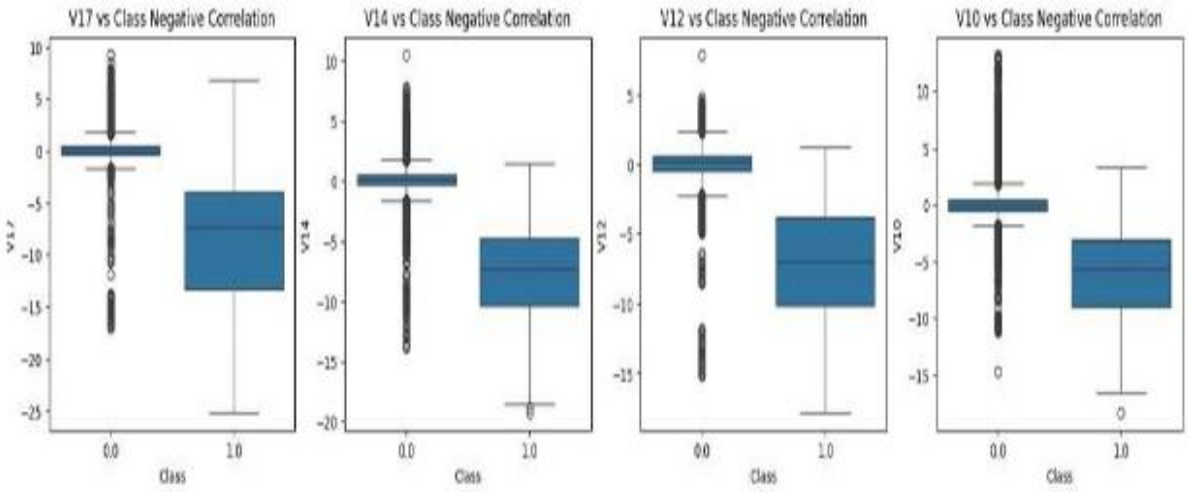

Figure 1: Figure 3: Negative Correlation with classes

3.2.3 Feature Scaling:

Here, feature standardization is exhibited. Where, comparison is done between values in Table 2 and 3, and where the occurrences of each class are count to plot a pie chart that generate a visualization of imbalance class distribution in the kaggle dataset applied for this study as depicted in Figure 4. The fraudulent class categorization is 0.2%, which is the minority class, while the non-fraudulent class distribution is the 99.8% that is referred to as the majority class.

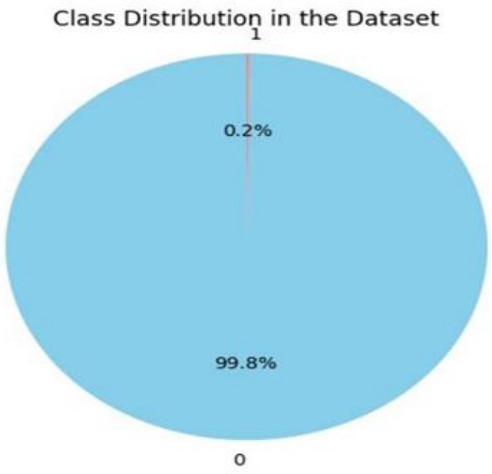

Figure 4: Imbalance Class Distribution of Kaggle Dataset

3.2.4 Data Re-Sampling:

This is well discussed in (Salaudeen et al., 2024a; Salaudeen et al., 2024b). Oversampling techniques of SMOTE is explored to balance the irregularity in skewed dataset (i.e., imbalance distribution); while addressing the challenges of over-fitting and under-fitting inbound in kaggle datasets (Khalid et al., 2024).

3.2.5 Feature correlation and selection:

A correlation matrix is a statistical tool that depicts the relationship between two variables in a dataset. It uses a table where each cell contains a correlation coefficient that indicates the strength and direction of the relationship. Figure 5 showed the generate Correlation Matrix, where the features of the dataset utilized are visible on both the horizontal (y-axis) and vertical (x-axis) sides of the graph with an inscription of Time, V1, V2, V3……. V28, Amount and Class. The plot painted indicator shown at right hand side; showcased varieties of colors in Yellow, Deep Green, Grey, Pink, Light Blue, Deep Blue and others with number indicators attached. From the graph plot, the diagonal side portrays a straight yellow line color touching the edge sides of the graph. This represented that there was high correlation between the feature “Time” and “Class”. The number indication of 1.0 yellow represented high or strong correlation, 0.8 represent very strong correlation, 0.6 strong correlation, 0.4 Good correlation, 0.2 Weak correlation, 0.0 Neutral correlation, -1.0 not strong correlation, -0.2 poor correlation, -0.4 bad correlation. Besides, positive numbers indicate positive correlations. While, negative numbers indicate negative correlations. In summary, the closer the number is to 1 (or -1): the stronger is the correlation.

On the other side, Figure 6 depicts the conjoined Scatter and density plots of the credit card dataset utilized in this study. The scatter plot, otherwise

© DEC 2025 | IRE Journals | Volume 9 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I6-1713053

known as scatter chart or Scatter graph; uses cluster dots, histogram, frequency flow, heap map and many other representations to represent values for two different numeric variables. The position of each cluster dots with symbols representations on the horizontal and vertical axis indicates values for an individual data points. Besides, scatter graph is often used to observed relationship between variables. While, the density plot on the other hand; is a special case of scatter plot. It shows how numerical data binned into two intervals is distributed through the X-axis and the Y-axis.

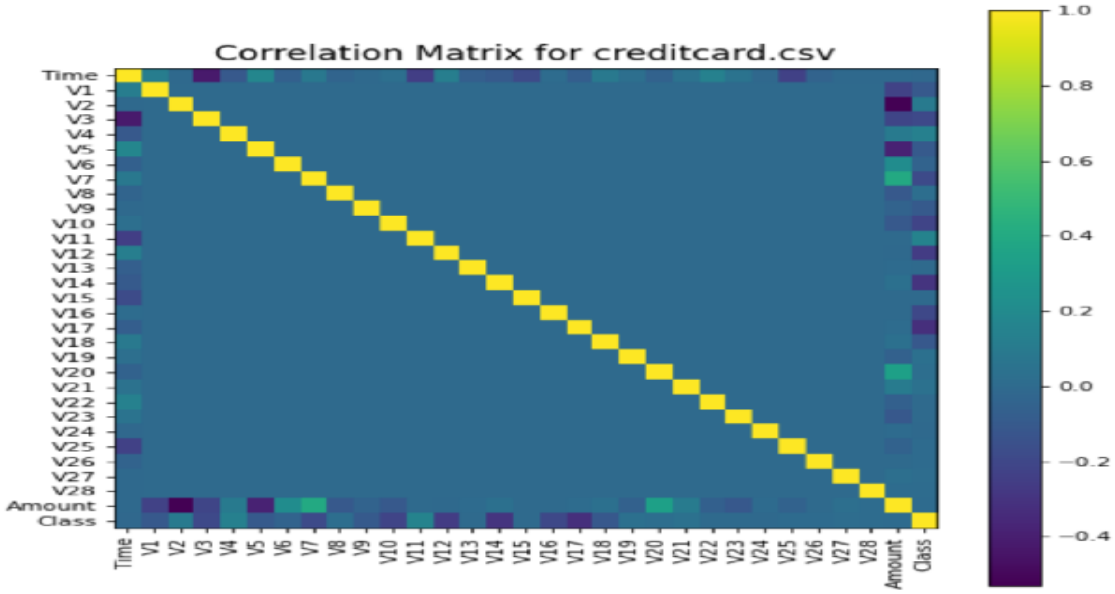

Figure 5: Correlation Matrix for kaggle Credit Card Dataset

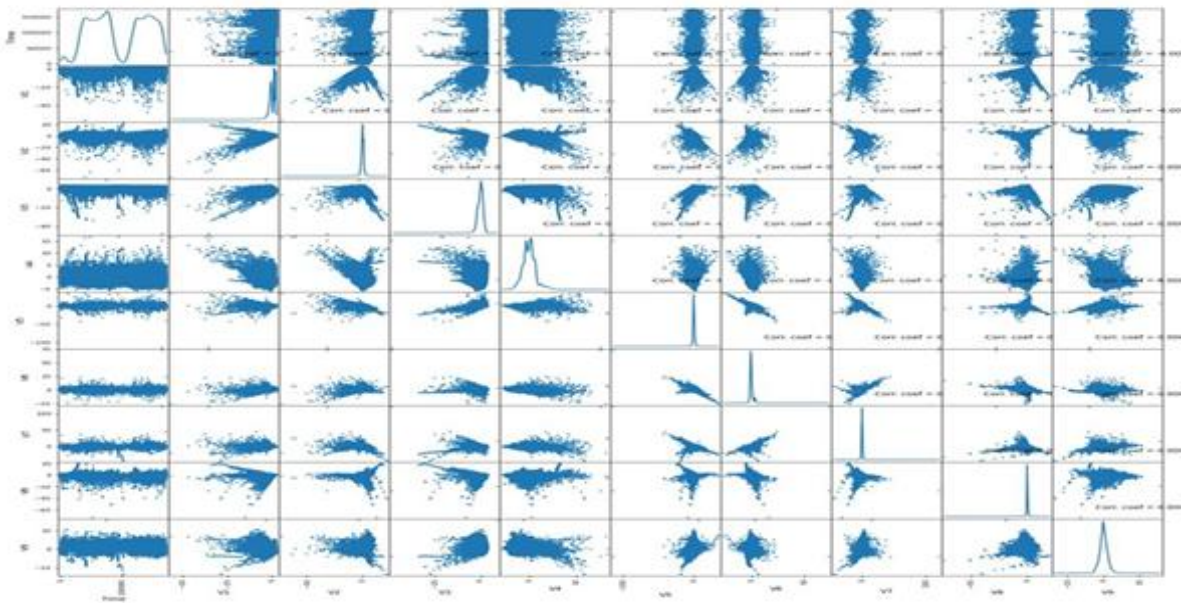

Figure 6: Scatter and Density Plot of Kaggle Credit Card Dataset

3.3 Implementation Hardware and Software used:

This study employed Python for executing computational tasks on a personal laptop equipped with an Intel i7-5600U CPU (2.6GHz), 16GB RAM, and an SSD. The system demonstrated efficient resource usage, with peak memory consumption at 25% and negligible hard disk utilization. For machine learning (ML) classification, the Scikit-learn library was used, while TensorFlow facilitated deep learning (DL) implementations. Key Python librarie including NumPy, Pandas, Matplotlib, Seaborn, and others were leveraged for data preprocessing and visualization, as detailed in (Akinola et al., 2023). The development

environment relied on Google Colab, integrated with Jupyter Notebook and Google Drive's cloud infrastructure, following methodologies outlined in Sharma (2020).

3.4 Machine Learning Approach engaged for this study

James et al., (2017) related statistical learning to ML "a set of tools for modeling and comprehending multifaceted datasets". ML is a subsection of artificial intelligence, which encompasses deep learning that operates as a more specified categorized extension. These distinctions were thoroughly examined in Salaudeen et al., (2024) and Salaudeen et al., (2024b) distinct study.

Brownlee (2019) further categorized ML methodologies into three primary paradigms: supervised, unsupervised, and semi-supervised/reinforcement learning, among others.

In this study, inclusive ML and DL methods are explore:

- Traditional ML models: LR, RF, and iForest
- Neural network-based approaches: Multilayer Perceptron (MLP)
- SMOTE and
- Proposed MLP+SMOTE which is discussed

.

3.4.1 Logistics Regression

This is a statistical ML method widely used for binary classification tasks, involving payment fraud detection (Salaudeen et al., 2025; Akinola et al., 2023). While primarily employed for classification, LR can also predict categorical outcomes by analyzing relationships between dependent and independent variables. Fayyomi et al., (2021) further elucidated the foundational concepts and applications of LR in the comprehensive literature review.

3.4.2 Random Forest

This is one of the greatest robust ensemble ML methods, demonstrating exceptional efficacy in payment fraud detection. Due to its ability to handle imbalanced datasets and feature interdependencies. Recent studies, such as Salaudeen et al. (2024), highlight its superior performance in fraud classification, while Fayyomi et al., (2021) provided a detailed schematic analysis of RF's operational framework, elucidating its decision-tree aggregation mechanism.

For this study, the hyperparameter tuning strategy for the RF model was adapted from (Pavan, 2024; Salaudeen et al., 2025) which emphasized optimization techniques like grid search and cross-validation to enhance model accuracy and generalization. Notably, RF's effectiveness in fraud detection is further validated by comparative studies showing its outperformance over single decision trees and other ensemble methods like AdaBoost, particularly in metrics such as precision, recall and F1-scores.

3.4.3 iforest

This algorithm is a focused unsupervised learning method designed for anomaly detection tasks. As the name suggests, it operates on the principle of isolating anomalies by leveraging their inherent characteristics of being "few and different" from normal instances (DataCam, N.d). The algorithm constructs an ensemble of isolation trees (iTrees), where anomalies are identified as data points requiring fewer splits to be isolated indicated by shorter average path lengths in the tree structures.

Key parameters governing iForest's performance include:

- The number of trees in the ensemble
- The sub-sampling size for each tree

Research by Cortes (2019) demonstrates that iForest achieves strong detection performance with remarkable efficiency, converging quickly with relatively small ensembles and minimal sub-sampling requirements. The algorithm's parameter optimization framework, was discussed in (Pavan, 2024), was adopted for this study.

3.4.4 Multi-Layer Perceptrons (MLPs)

It is a form of feedforward artificial neural network with at least three layers involving input layer, one or more hidden layers, and an output layer (Salaudeen et al., 2024). It uses non-linear activation functions such as ReLU, sigmoid, tanh to learn difficult patterns. MLPs are universal function approximators, meaning they can model any incessant function given adequate neurons and layers. It Embedding Layers (often used in NLP/Recommendation Systems) can be integrated into MLPs to transform categorical/discrete inputs

into dense vector representations, improving model performance.

3.4.5 Synthetic Minority Oversampling Technique

SMOTE is a popular resampling method; engaged in handling dataset distribution challenge (Khalid et al., 2024; Noviandy et al., 2023). SMOTE generates synthetic models interpolating between existing minority-class occurrences. SMOTE works through the

- Selection of a minority class occurrence.
- Discover its k-nearest neighbors from the similar class.
- Generate new synthetic occurrences along the line segments linking the original point and its neighbors.
- Helps prevent overfitting compared to naive oversampling.

3.4.6 Proposed Multiple Layer Perceptron's (MLP) Based Synthetic Minority Oversampling Techniques (SMOTE)

MLPs (like other neural networks) performs poorly on datasets, as they favor the majority class. However, the use of SMOTE before training to balance the dataset was explain under section 4 in subsection 4.2 to improve the model performances for payment card detection. SMOTE helps MLPs learn better decision boundaries by providing more minority-class examples. Embedding layers (if used) can further enhance feature representation. The likely challenges encounter was that SMOTE might tend to introduce noise if minority class instances are not well clustered. Besides, it can lead to overfitting if synthetic samples dominate training. More so, SMOTE increases dataset size, making MLP training slower.

MLPs with integration of SMOTE considerably improve performance on imbalanced datasets by ensuring the model realizes sufficient minority-class instances. However, proper validation and tuning (e.g., adjusting SMOTE's sampling ratio, MLP architecture) are crucial for optimal results. For structured data, adding embedding layers can further enhance feature representation, making the model more robust.

3.5 Performance Evaluation Metrics

A Confusion Matrix Table is use during the performance evaluation. It is table use to describe the performance of classification model on a set of data for which the true values were known (Salaudeen et al., 2024a; Cicekli, 2022). It permits the imagining of the performance of an algorithm or models. It as well reviews each tuples traits of True Negative, False Positive, False Negative, True Positive and performance evaluation of any models employ during experimentation in either binary classification task or multi-class. Its pictorial diagram is visible in (Salaudeen et al., 2024b).

- True Negative – It refers to the number of correct guesses that an occurrence is negative. It is predicted "No", and they are not fraudulent
- False Positive - is the number of incorrect guesses that an occurrence is positive. It is predicted "Yes", but they are not actually fraudulent. This are otherwise known as Type 1 error
- False Negative - are the amount of incorrect of guesses that an occurrence is negative. It is predicted "No" but they are actually fraudulent. This is otherwise known as Type 11 Error
- True Positive- are the number of correct guesses that an occurrence is positive, that is fraudulent.

i. Accuracy: It was often use to determine how well a model performed. It is determine using the syntax:

$$\text{Accuracy} = TP + TN / TP + TN + FP + FN \quad (1).$$

ii. Misclassification: It describes how frequently the classifier is wrong?

$$\text{Mist.} = FP + FN / TP + TN + FP + FN \quad (2).$$

It can be calculate using the formula: Mist. = 1 - Accuracy.

iii. Recall: When it is actually "Yes", how frequently does it predict yes?

$$\text{Recall} = TP / TP + FN \quad (3).$$

iv. False Positive Rate: how frequently does it predict yes? When it is truly "No"

$$\text{FPR} = FP / TN + FP \quad (4).$$

v. Specificity: how frequently does it predict no? When it is truly no

$$\text{Specificity (TNR)} = TN / \text{Actual No} \quad (5).$$

It can as well be calculated using Specificity = 1 - FPR. It is otherwise known as True Negative Rate

© DEC 2025 | IRE Journals | Volume 9 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I6-1713053

vi. Precision: When it envisages yes, how frequently is it correct?

Prec. = TP / TP +FP (6).

vii. Prevalence: How frequently does the yes condition really happen in the sample?

Prev. = Actual fraud (Yes or Positive)/Total No. of actual and predicted classifier (7).

viii. NULL ERROR RATE: Describes how frequently one would be wrong if you always projected the majority class.

NER = TN+FP/ TP+TN+FN+FP (8).

ix. F1 Score: This is a weighted average of the true positive rate and precision

F1-Score = (2* (Precision* Recall)/(Precision + Recall))*100 (9).

x. Matthews Correlation Coefficient (MCC) = ((TP*TN) -(FP*FN)/ √ (TP +FP) *(TP+FN) *(TN*FP*(TN+FN)) (10).

IV. RESULTS

The results for the baseline and balancing models' experiments were present under this section.

4.1 Discussion on Baseline Models

The value generated for the during the baseline trials is showed in Table 4. However, Matthew's Correlation Coefficient was not use during the result presentation due to lack of appropriateness in model performance over kaggle dataset (Comotto, 2022). Table 5 shows the baseline results without SMOTE in tandem to produce Figure 7. This displays the bar chart for the baseline model experiment.

Table 4. The Confusion Matrix for the Baseline models

Models	TN	FP	FN	TP
LR	63	35	19	56845
RF	79	19	7	56857
I.forest	241	251	251	284064
MLP	72	57	4	71069

Table 5: Baseline Model Validation Results Without SMOTE

Models	ACC	ER	Recall	FPR	TNR	Precision	Prevalence	F1-Score	NER	Cohen's Kappa
LR	1.00	0.001	1.00	0.357	0.643	1.00	0.998	1.00	0.002	0.998
RF	1.00	0.001	1.00	0.194	0.806	1.00	0.998	1.00	0.002	0.998
I.Forest	1.00	0.002	1.00	0.510	0.490	1.00	0.997	1.00	0.002	0.998
MLP	1.00	0.001	1.00	0.442	0.560	1.00	0.998	1.00	0.002	0.998

© DEC 2025 | IRE Journals | Volume 9 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I6-1713053

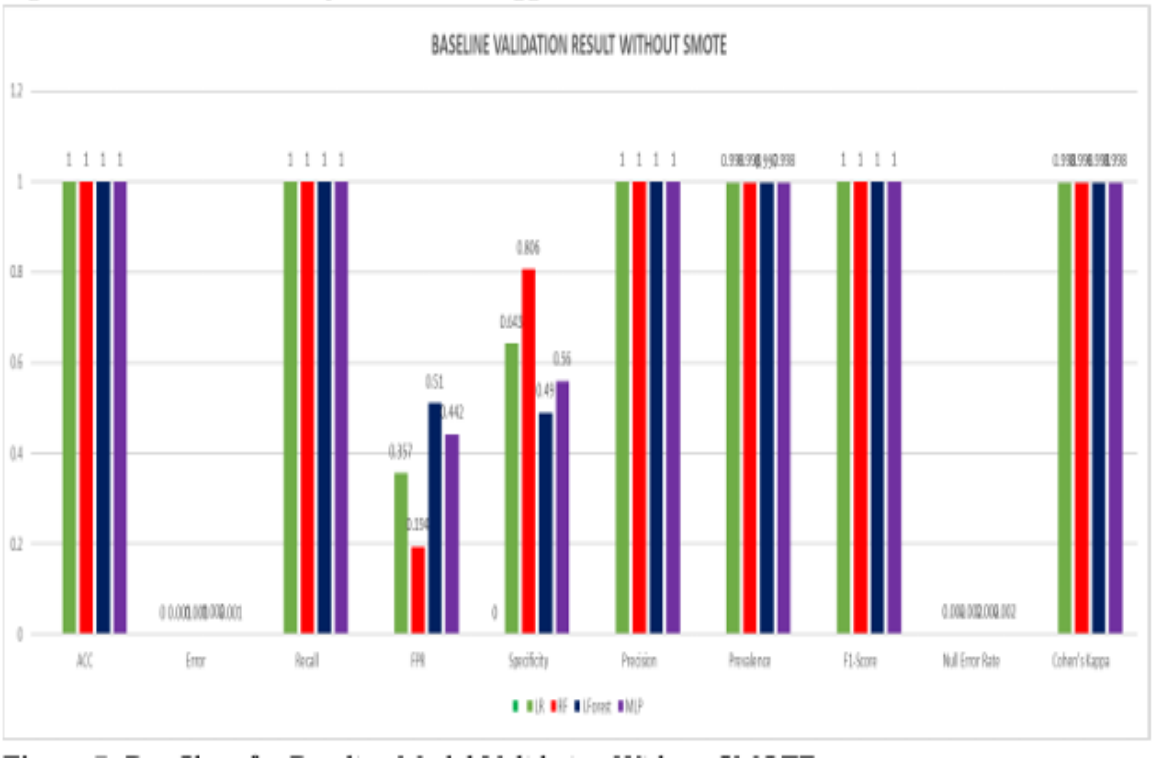

Figure 7: Bar Chart For Baseline Model Validation without SMOTE

From the investigation report in Table 4. It was obvious that accuracy, recall, precision and F1-score results of the baseline models are 1.00% respectively. This affirms the model superclass outcomes distinctively. However, the result makes it difficult to inaugurate the best model performance. Another metrics was considered where Null error rate of 0.002% was present. With Prevalence and Cohen's Kappa offered 0.998% of distinct result.

This regiment the baseline experiment decision to FPR and TNR evaluation metrics. These were unfitting yardstick for presenting results in binary classification problem. RF was learned to generate the least FPR result of 0.194%, followed by LR with 0.357%, MLP with 0.442% and iforest 0.510% respectively. Under the specificity, RF presented the highest results of 0.806%, followed by LR with 0.643%, MLP with 0.560% and iforest that presented the least close-range specificity results of 0.490%. Based on this finding, it was glaring that RF is the best baseline model with outstanding result performances. The dataset applied for the conduct of the trial was highly skewed. However, second trial is delved using SMOTE to balance dataset. This was utilized to present cogent and more alluring results; that can assist financial institution in regulating the menace of payment fraud.

4.2. Balancing model Trial using SMOTE

The Table 6; presented the confusion matrix table for the balancing model exploring kaggle dataset. Table 7 depicted the SMOTE methods that validates results of the model with the proposed hybrid MLP+SMOTE model. Figure 8, presented the diagram for the balance models using SMOTE for which discussion is rooted.

Table 6: Confusion Matrix for Balancing Models with SMOTE

	TN	FP	FN	TP
LR +SMOTE	40	3	4	38
RF +SMOTE	42	1	4	38
Isolation Forest +SMOTE	43	0	42	0
MLP+SMOTE	42	1	3	39

© DEC 2025 | IRE Journals | Volume 9 Issue 6 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I6-1713053

Table 7: Balance Models with SMOTE Oversampling Validation Results

Models	ACC (%)	ER (%)	Recall (%)	FPR (%)	TNR (%)	Prec. (%)	Prevalence (%)	NER	Cohen Kappa (%)	F1-score (%)	MCC (%)
LR+SMOTE	0.92	0.08	0.93	0.09	0.91	0.90	0.45	0.52	0.4	0.92	0.84
RF+SMOTE	0.94	0.06	0.97	0.09	0.91	0.90	0.45	0.54	0.4	0.93	0.88
Isolation Forest +SMOTE	0.51	0.49	0.00	0.5	0.51	0.00	0.00	1.00	-0.5	0.00	0.00
Proposed MLP+SMOTE	0.95	0.05	0.98	0.07	0.93	0.93	0.46	0.53	0.42	0.95	0.91

Figure 8: Bar Chart for Balance Model Using SMOTE Oversampling Techniques

Accuracy

The proposed MLP+SMOTE model presented an optimized accuracy score of 0.95% in close range with RF+SMOTE of 0.94%, LR+SMOTE 0.92%, and Isolation Forest of 0.51% that serves as the worst mode offering least results.

Misclassification/ Error Rate (ER)

MLP+ SMOTE model offered smallest error rate (ER) of 0.05% that is the best result under this evaluation metric. This is followed by RF+SMOTE, presenting 0.06%, LR+SMOTE 0.08% and iforest offering 0.49%, which depicts the worst error rate result.

Recall

The proposed MLP+SMOTE displayed the best recall results of 0.98% in close range with RF+SMOTE 0.97%, LR+SMOTE 0.93%. WHILE, Isolation Forest was still visible as the worst performance model presenting 0.00%.

False Positive Rate (FPR)

The MLP integrating SMOTE presented the least outcome of 0.07% with both RF+SMOTE and LR+SMOTE displaying the same result of 0.09% for the FPR. The Isolation Forest evaluation metrics still maintain the spot of the worst performing model with 0.5%.

True Negative Rate (TNR)
MLP embedding SMOTE model offered the highest TNR result of 0.93%. While LR+SMOTE and RF+SMOTE model coherently displayed same results of 0.91%. whereas, Isolation Forest presented 0.51 results to act as the worst performing model under the TNR evaluation metrics.

Precision
The results under precision evaluation metrics are not quite different from that TNR earlier presented. Here, the proposed MLP+SMOTE model presented 0.93% with LR+SMOTE and RF+SMOTE models logically respectively displayed 0.90%. While isolation forest, presented a disgusting 0.00% to serve as the worst model under the precision evaluation metrics.

Prevalence:
The proposed MLP+SMOTE model presented the highest prevalence result of 0.46; this was preceded by both LR+SMOTE and RF+SMOTE offering same result of 0.45%. while, Isolation Forest presented 0.00% results.

Null Error Rae (NER)
The isolation forest displayed the highest NER rate of 1.00% result; these was preceded by RF+SMOTE model of 0.54%; proposed MLP+SMOTE model of 0.53 with LR +SMOTE presenting 0.52% respectively.

Cohen Kappa
Under this evaluation metrics, the proposed MLP+SMOTE model presented 0.42% results as the best and the highest outcome. Whereas, RF+SMOTE and LR+SMOTE distinctly presented same results of 0.4%. While Isolation Forest presented an outrageous result of -0.5% to be a firmly ascribed as the worst performance model.

F1-score
The prosed MLP+SMOTE presented the highest results which is the best F1-score results of 0.95%; in precedence of RF+SMOTE model offering 0.93%, LR+SMOTE model 0.92% respectively. While iforest generate 0% result. This made it the weakest evaluation metric models under this binary classification.

Matthews's Correlation Co-efficient (MCC
The proposed MLP+SMOTE model rendered the best results here; presenting 0.91 in close range with RF+SMOTE model that offers 0.88%, LR+SMOTE model 0.84% and iforest of 0.00% to be the worst model.

4.3 Proposed Model Comparison alongside Benchmark Study

From the eleven performance, evaluation metrics delve on kaggle dataset applied. It was discovered that the proposed MLP+SMOTE model performed excellently well across ten evaluation metrics parameters. MLP+SMOTE show accuracy result of 0.95%, Misclassification of 0.05%. Recall of 0.98%, least False Positive Rate result of 0.07%, True Negative Rate of 0.93%, Precision of 0.93%, Prevalence of 0.46%, Null Error Rate of 100%, Cohen kappa result of 0.42%, F1-score of 0.95% with Matthews Correlation Coefficient of 0.91% respectively. These results validate the developed model as amazing in performance, when compared with benchmark study of (Akinola et al., 2023; Singh et al., 2024; El Naby et al., 2021). The research outcome is promising in the classification of payment fraud. Besides, the entire balancing model training SMOTE provides outstanding performance against the benchmark studies except for the iforest +SMOTE in this field of payment fraud detection. In preceding study of Bokhare et al., (2023), hybrid MLP+SMOTE model was applied to predict heart failure using TensorFlow. The research experimental result shows that the system predicts heart illness by 91.55% accuracy using neural networks (Bokhare et al., 2023). However, this study presents an improve result over (Bokhare et al., 2023) study. This is based on the dataset utilize for this study and how the model was being optimized against the previous study.

Table 8: Summary Table for Counter-measure approaches used by financial institution to mitigate the inference of credit card fraud

Method	Pros	Cons
Advanced Tracking	Real-time detection, reduces false declines	Costly, privacy concerns, false positives
Magnetic Stripes	Widely accepted, low cost	Easily cloned, outdated

3D Holograms	Hard to counterfeit visually	Useless online, expensive
CVC/CVV	Extra online security	Phishable, useless if card stolen
MFA	Stronger security	Inconvenient, SIM-swap risks
AVS	Verifies billing address	Limited effectiveness, false declines
Biometrics	Highly secure, unique	Hardware needed, privacy risks
OTP	Dynamic, expires quickly	SIM-swap/MITM risks, delays
Tokenization	Secure digital payments, reduces data exposure	Requires integration, token theft (rare)

V. CONCLUSION AND RECOMMENDATION

Extensive literature review was carried out in this study. Has it provided the pros and cons of different counter-measure approaches instituted by card issuer and financial institutions. Methodological framework and analysis were delved on kaggle dataset. Exploring machine and learning models of LR, RF, iForest, and proposed MLP+SMOTE respectively. A baseline model experiment was initially performed to probe the ML models. However, unfitting results is established, because of imbalance in class distribution of kaggle dataset applied. As it suffers from overfitting and under-fitting challenge that led to poor generalization of the outcome (Khalid et al., 2024; Cheon et al., 2021). The classifier tends to predicts only the majority class (i.e., the negative and non-fraudulent class. Additional experiment was performed in which resampling approach of SMOTE is applied. The results from this trial were the best performance. It was justified based eleven performance evaluation metrics parameters. MLP integrating SMOTE outshined in ten-parameter category. However, the study does not consider confidence intervals or statistical tests (e.g., t-tests) in validating the significance of the proposed model's performance over baselines based, on the fact that is not applied in the existing literatures (Khalid et al., 2024). This will be considered in the future study. This study advises financial institution to embrace the application of a proactive and improve counter-measures towards the defense of their customer against payment fraud. Since, fraudster keeps create diverse practices to ouster (outsmart) or break security measure set in place. This study however, encourage for more enhance hybrid deep or machine learning approaches in taming the occurrences of fraudulent credit card transaction. The subsequent work in this regard, should be tried exploiting MCC evaluation metric in binary classification task, because its improve model performances, and good is for addressing challenges of imbalance in dataset distribution. More so, a layered security model combining EMV chips, tokenization, biometrics, and MFA can be advantage to provide the strongest protection. Real-time monitoring and AI-based anomaly detection for further enhance fraud prevention.

Interest of Conflicts:
There are no conflicts of interest in this study, as all authors agreed to its submission.

REFERENCES

[1] Aghware FO, Yoro R E, Ejeh P O, Odiakaose C C, Emordi F U, Ojugo, A A. DeLClustE: Protecting Users from Credit-Card Fraud Transaction via the Deep-Learning Cluster Ensemble, (IJACSA) International Journal of Advanced Computer Science and Applications, 2023, Vol. 14 No.6, pp. 94-100. www.ijacsa.thesai.org

[2] Akinola K E, Aina D A, Oyede O, Braimoah J A (2023). Credit Card Fraud Detection Using Logistics Regression and Isolation Forest Algorithm, UNIZIK Journal of Engineering and Applied Sciences, 2023, Vol. 2 No.1, pp. 187-195. https://journals.unizik.edu.ng/index.php/ujeas

[3] Alraddadi, B. A Survey and a Credit Card Fraud Detection and Prevention Model using the Decision Tree Algorithm, Engineering, Technology & Applied Science Research,2023, Vol. 13 No.4, pp. 11505-11510. http://www.etasr.com/

[4] Al-Smadi, B. Credit card security system and fraud detection algorithm, Ph.D. dissertation, College of Engineering and Science, Louisiana Tech University, USA, 2021. https://digitalcommons.latech. edu/cgi/viewcontent.cgi?article=1947&context =dissertations.

[5] Aslam A, Hussain A. A performance Analysis of Machine Learning Techniques for Credit

Card Fraud Detection", Journal on Artificial Intelligence. 2024. https://doi.org/10.32604/Jai.2024.047226

[6] Bokhare A, Bhagat A, Bhalodia, R. Multilayer Perceptron's for heart Failure Detection using SMOTE Techniques, Springer Nature. 2023. Retrieved from: Multi-layer Perceptron for Heart Failure Detection Using SMOTE Technique | SN Computer Science (springer.com)

[7] Brownlee J. 14 Different Types of Learning in Machine Learning, Blog, 2019. https://machinelearningmastery.com/types-of-learning-in-machine-learning/

[8] Cheon M J, Lee D H, Joo S H, Lee O. Deep learning based hybrid approach of detecting fraudulent transactions Journal of theoretical and applied information technology 31st august 2021. Vol. 99 No.16, pp. 4044-4054. Http://www.jatit.org/

[9] Cicekli I. Classification Model Evaluation and Selection and ensemble Methods, Data Mining. 2022. https://www.lec07_Classification_ModelEvaluation_Ensemble.pdf

[10] Comotto F. Evaluation metric: leave your comfort zone ant try MCC and brier scope.2022.

[11] Cortes, D. An Introduction to Isolation Forest. [Blog].2019. https://cran.r-project.org/web/packages/isotree/vignettes/An_introduction_to_isolation_forest.html#:testisolation%20%forest20is%20an%20unsupervised%2ffeatures%2fcolumn%20at%20random

[12] DataCam. Hyperparameter turning of Isolation forest. Nd. https://www.campus.datacamp.com/courses/anomaly-detection-in-python-/isolation-forests-with-pyod?ex=9

[13] Devi R R, & Parthibranjanray. A., Credit Card Fraud Detection using AI/ML/CNN, IRE 1704172 Iconic Research and Engineering Journalsire,2023, 6(9): 242-249 | ISSN: 2456-8880

[14] Ding Y, Kang W, Feng J, Peng B, Yang A. Credit Card Fraud Detection Based on Improved Variational Autoencoder Generative Adversarial Network", IEEE Access, 2023, Vol. 11, No.2023, pp. 83680-83691. https://doi.org/10.1109/ACCESS.2023.3302339

[15] El-Naby A, Hemdan, E E, El-Sayed A. Deep Learning Approach for Credit Card Fraud Detection, 2nd IEEE, International Conference on Electronic Engineering, Menoufia University, Egypt, ICEEM.2021. https://doi.org/978-1-6654-1842-3/21/$31.00

[16] Fayyomi A M, Eleniyan D, Eleniyan, A. A survey paper on credit card fraud detection techniques, International Journal of Scientific & Technology Research, 2021, 10 (9): 72-79. http://www.ijstr.org/

[17] Geeksforgeeks. Rule based approach in NLP. 2023. https://www.geeksforgeeks.org/rule-based-approach-in-nlp/

[18] James G, Witten D, Hastie T, Tibshirani R. An Introduction to statistical learning with applications in R, Springer New York Heidelberg Dordrecht London, 2017. https://doi.org/10.1007/978-1-4614-7138-7

[19] Jayanthi G, Deepthi P, Rao N B, Bharathiraya M, Loga Priya, A. A comparative study on machine learning and fuzzy logic-based approach for enhancing credit card fraud detection, International Journal of Intelligent Systems and Applications in Engineering, 2024, Vol. 12 No. 125. https://ijisae.org/index.php/IJISAE/archieve/view/4504

[20] Khalid A R, Owoh N, Uthmani O, Ashawa M, Osamor J, Adejoh J. Enhancing credit card fraud detection: an ensemble machine learning approach", Big Data Cogn. Comput. 2024, Vol. 8 No. 6. https://doi.org/10.3390/bdcc8010006

[21] Lake R, Huffman L, Tang K. Best credit monitoring services for 2023". [Blog]. 2023. Retrieved from: Best credit monitoring services for 2023 | CreditCards.com

[22] Madhavi M, Reddy K RV, Swetha B, Kumar, R B. Credit card fraud detection using CNN, IJRTI, 2023, Vol. 8 No.4, pp. 845-854. www.ijrti.org

[23] Mienye I D, Sun Y. A deep learning ensemble with data resampling for credit card fraud detection", Applied Research IEEE Access,2023, Vol. 11, pp. 30628-30638. https://doi.org/10.1109/ACCESS.2023.3262020

[24] Noviandy R T, Idroes G M, Maulana A, Hardi I, Ringga E S, Idroes, R. Credit card fraud detection for contemporary financial management using XGBoost-driven machine

learning and data augmentation techniques, Indatu Journal of Management and Accounting,2023, Vol.1 No.1. https://heca-analitika.com/ijm

[25] Pavan P. Random Forest Hyperparameter Tuning in Python: Complete Guide with Examples. 2024.https:// www.upgrade.com/blog/random-forest--hyperparameter-turning/

[26] Prasad P Y, Chowdary A S, Bavitha C, Mounisha, E, & Reethika C. A comparison study of fraud detection in usage of credit cards using machine learning, In Proceedings of the 7th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 11–13, April 2023; pp. 1204–1209.

[27] Salaudeen L G, Gabi, D, Muhammad, G, & Suru, H. U. A boosted deep convnet embedding long short-term memory with synthetic minority oversampling techniques as foiling model for payment card fraud, Journal of International Financial Trends. 2025 Vol.1, No.1, pp.61-89. DOI: https://doi.org/10.55578/jift.2506.005

[28] Salaudeen L G, Gabi, D, Muhammad, G, & Suru, H. U. Light gradient boosting machine (LGBM) for credit card fraud detection in financial institution, Direct Res. J. Eng. Inform. Tech. 2024a, Vol. 12 No.1, pp. 19-34. https://doi.org/10.26765/DRJEIT17933661

[29] Salaudeen, L G, Gabi, D, Muhammad G, & Suru, H U. Deep convolutional neural network (DCNN) based synthetic minority oversampling techniques: a forfending model for fraudulent credit card transactions in financial institution, Journal of Nigerian Society of Physical Sciences (NSPS). 2024b. https://doi.org/10.46481/jnsps.2024.2037

[30] Sharma, A., Free GPUs for Everyone! Get Started with Google Colab for Machine Learning and Deep Learning. 2020. Retrieved from: https://www.analyticsvidhya.com/blog/2020/03/google-colab-machine-learning-deep-learning

[31] Singh S, Ninje, H, Ajinkya F, Neware R. Credit card fraud detection using a hybrid machine learning algorithm. 2024. https:///doi.org/10.20944/preprint2024021206.v1