Direct Research Journal of Engineering and Information Technology
Vol. 12 (1), Pp. 19-34, April 2024
ISSN: 2354-4155
DOI: https://doi.org/10.26765/DRJEIT17933661
Article Number: DRJEIT17933661

https://journals.directresearchpublisher.org/index.php/drjeit

Light Gradient Boosting Machine (LGBM) for Credit Card Fraud Detection in Financial Institution

Lateef Gbolahan Salaudeen*, Danlami Gabi, Garba Muhammad, and Hassan Umar Suru

Department of Computer Science, Faculty of Physical Sciences, Kebbi State University of Science and Technology, Aliero, P.M.B 1144, Aliero, Kebbi State, Nigeria.
Corresponding Author E-mail: gbolahan_salaudeen@yahoo.co.uk

Received 9 March 2024; Accepted 5 April 2024; Published 13 April 2024

ABSTRACT: The upsurge in fraudulent credit card deed is raising rancorous alarms on daily basis; as its globally causing multi-billion dollars' losses and instigates derogatory imprint which affects both financial institutions and customers. To these effects, many methods have been offered by scholars in diverse applications for curbs; that yielded near perfection results. Due to Machine learning (ML) approaches challenges and imbalance class distribution in most dataset imbibed for credit card fraud detection. The approach pervades over fitting and under-fitting results, that leads to poor generalization of outcomes. Because the classifier tends to predicts only majority class. To address this issue, an optimized performance metrics designed to handle data balancing either by using re-sampling methods or data augmentation approach is seemly. In this paper, accuracy score, Matthews's correlation coefficient (MCC), Cohen's Kappa and F1-Scoreareselected as the evaluation metrics to analyze the outcomes of four distinct ML model classifiers of LR, RF, Isolation Forest, and three DL models of MLP, ANN and CNN in addition to the proposed LGBM organized for credit card fraud detection. Two experiments were steered in this study on the imbalance kaggle dataset utilized. While, exploiting the Google Colab integrated Jupyter notebook cloud infrastructure as the program development settings with Python programming language for modelling. The foremost experiment is on baseline model probing LR and RF. The RF model excel in performance against the LR model was selected for the second experiment on balancing class models absorbing SMOTE oversampling methods. It is inferred that the proposed LGBM offered surpass performance across seven aspects of the evaluation metrics; out of the eleven instances deployed. The model renders an accuracy scores of (96%), least error rate of (0.4%), Recall (95%), prevalence (47%), Cohen Kappa (45%), F1-score (96%) and MCC (93%) against other ML and DL models betrothed respectively.

Keywords: Financial institution, fraud detection, machine learning, credit card fraud
Citation Salaudeen,L. G., Gabi, D., Muhammad,G., Suru, H. U. (2024). Light Gradient Boosting Machine (LGBM) for Credit Card Fraud Detection in Financial Institution. Direct Res. J. Eng. Inform. Tech. Vol. 12 (1), Pp. 19-34. https://doi.org/10.26765/DRJEIT17933661

INTRODUCTION

Recently, there have been reports over the damaging effects of mystifying forms of frauds, amidst credit card frauds (Ali et al., 2019; Falco, 2023); committed against credulous people, industries, public bodies, services and the environment signaling immoral lifelong impression (IPFSS, 2020; Horton, 2023). This malicious activity globally distresses millions of peoples' and organizations on daily basis, and institutes unquantifiable financial losses that raises critical concerns over it controls (Jain et al., 2022; Ramani et al., 2022; Aslam and Hussain, 2023; Shah and Makwana, 2023). However, conventional rule-based tactics which is a reactive method heaping on historical data for predictive analysis is often offers as counter measures and this is daunting by some restrictions (Shah and Makwana, 2023; Al-Smadi, 2021). Besides, fraudster being the crime instigator are

unceasing in espousing new methods towards the perpetrating of this unlawful acts (Ramani et al., 2022; Aslam and Hussain, 2023);their practices are obliging on influencing factors such as skimming, identity theft, phishing and social engineering fraud tactics that bends on merchant collusion, triangulation, data breaches, improper authentication of documents, technology advancement, improper card management, inadequate system security and system integration, application fraud, counterfeit card and corporate account takeover (CATO) with many others(Jain et al., 2022; Al-Smadi, 2021; Agarwal et al., 2021). Which makes the regularity process difficult and makes fraudster waxes stronger in evading the pre-existing countermeasures of Multi-Factor Authentication (MFA), magnetic stripes, three dimensional hologram (3DS), one-time credit card number generation, Tokenization, Biometrics, Code Verification Value (CVV), Address Verification System (AVS), Machine learning (ML) based fraud detection, and many others (Jendruszak, 2023; Al-Smadi, 2021); already instituted by financial institution in curbing the fraudulent credit card dealings. Therefore, there is need for cogent responsive system that can identify and deterred this fraudulent credit card scenario (Jain et al.,2019; Jain et al., 2022; Ke et al., 2017; Shah and Makwana, 2023); which (Tata Consultancy Services (TCS), 2003; White, 2023) extensively expounded. In which (Muharjan and Chudal, 2019) offered diagrammatic illustrations of it kinds for simplicity. While (Ali et al., 2019) study garnished with other forms of fraud affecting the financial institutions in relationship with telecom industry. Al-Smadi (2021) and Khalid et al., (2024) in their distinct studies offered the historical facts, statistical breakdown of annual cost implications instituted by credit card fraud, it mode of operation likewise other approaches deployed by financial institutions to mitigate its irregularities.

For decades, financial institutions have been in existence delivering extensive diversity of credit, deposits, lending and investment products services to both individuals and businesses (Hayes et al., 2023; Horton, 2023). Most of which focuses on providing services and account for the general public; others are more probable to serve only certain customers with more specialized offerings (Horton, 2023). Discharging the dutiful tasks of providing: banking services, capital formation, monetary supply regulation, pension fund services, and to as well contribute to the economic growth of nations (Aggarwal, 2024). With intents of profit maximization, improving customer trust in patronage via effecting satisfactory services that gears towards their retentions and in gaining new customers. But, these obligations are being subtly rattled with deciphering forms of frauds; pervaded by fraudsters in instigating hostile socio-economic implications; for motives best known to them' (Alghawi, 2019). Besides, the upsurge in digital payment approaches has amplified the menace of credit card fraud, making it easier for fraudsters to carry out their activities anonymously (Shah and Makwana, 2023). To that regard, several researchers' (e.g., Khalid et al., 2024; Aslam and Hussain, 2024; Aghware et al., 2023; Alraddadi, 2023; Shah and Makwana, 2023) have proposed models using statistical methods, data mining, machine learning and deep learning by improving on the accuracy result divulged and efficacy of credit card fraud detection. However, the outcomes of their approaches and models suffer from over-fitting and under-fitting challenges, binding by scarcity of real-world dataset for experimentation, imbalance data class distribution, high dimensionality and sparsity problem in dataset and real-time detection, complexities in the design of a genuine fraud detection models and interpretability of the models applied. All these limitations, makes research in this field extremely challenging and raise concerns as research gaps (Great Learning Team, 2023; Mienye and Sun, 2023). Therefore, there is need for more ideal approach for credit card fraud detection in financial institutions (Baker et al., 2022). Besides, one of the aim of this study is to provide answers to these two ruminating questions of:

Q1: What is the best approach to implement in taming the unceasing act of credit card fraud?

Q2: Who is liable for the cost implications instituted by fraudsters while delving stolen/misplaced credit card?

To address these questions, this paper conducts a series of comparative analysis experiments, and reports the results. In particular, this paper makes the following key contributions:

i. Institute predictive data analysis model using both machine and deep learning techniques that can classified fraudulent credit card transaction.

ii. Offered existing literatures on credit card frauds detection embedding machine and deep learning approaches towards credit card detection in financial institutions in order to understand their limitations.

iii. Propose LGBM as the suitable model for predicting fraudulent credit card transaction.

iv. Compares the performance of the proposed LGBM model with the existing schemes like Logistics Regression (LR), Random Forest (RF), Multiple layer Perception's (MLP), Artificial Neural Networks (ANN), Convolutional Neural Network (CNN) using kaggle credit card dataset; to establish models with best predictive results that determine fraudulent credit card fraud transaction.

v. The applied python programming language and libraries such as Pandas, NumPy, Scipy, Scikit learn,

Matplotlib, PySpark, seaborn, scatter plot, Plotly during the modelling stage on Google Colab platform. It is the easiest to use as it has a free notebook similar to Jupyternotebook found in anaconda3 distribution suite (Sharma, 2020). In this study, Scikit learn package is used for ML classification while Tensorflow is deployed for the deep learning.

Literature review

Machine learning just like statistical learning denotes "a set of tools for modeling and understanding complex datasets" (James et al., 2017). The ML is a subset of Artificial intelligence while the deep learning well rooted beneath ML (Hassan, 2016). These (Jovel and Greiner, 2023; Adeleke, 2022; Aggarwal, 2018) elusively described in their study.

Brownless, (2019); clarified on ranges of their learning method majorly classified into three forms of supervised, unsupervised, semi-supervised or Reinforcement learning algorithm with many others. Often times, number of scholars conducts experiments to achieve better results in taming the credit card frauds (Jain et al., 2022; Maniraj et al., 2019); while Yashvi et al. (2019) abreast with its six common tactics fraudsters imbibed in committing the offense. Predicting credit card fraud is recently centered on using either ML and DL or both models.

For instance, detecting fraudulent credit card transactions with supervised learning is able to accurately identify fraudulent transactions using two ideas of fraud prevention and detection analysis that can restrained the fraud sceneries.

Fraud prevention preceded the detection and its described as a measure taken to dissuade fraud from happening in the first instances. In contrary, fraud detection involves identification of fraudulent scenarios as quickly as possible before is perpetrates and/ or once preventive measure setup as failed (Ding et al., 2023).

Credit card fraud detection is describing as the process of classifying credit card transaction into groups of fraudulent and non-fraudulent classes for onwards data analysis to gather insight from them and makes critical decision in improving financial operational services, which can revamp customer trust and confidentiality (Shah and Makwana, 2023).

Jain et al. (2019) conducted a comprehensive review of various credit card fraud detection practices. Their study delved into the different methodologies and techniques utilized in the industry to combat fraudulent activities related to credit card transactions. while (Fayyomi et al., 2021) offers survey about several approaches in identifying credit card fraud. The scholar compared various ML methods such as LR, DT, RF, ANN, KNN, and K-means clustering in terms of their shortcomings and recompenses. Because not all the model application scenarios are the same, as a scenario-based algorithm can be hired to decide which scenario is the best fit for particular model. More so, the scholar engaged diverse performance evaluation metrics techniques and algorithms to predict and display fraudulent transactions. Studies are refreshed and encouraging to improve the fraud detection scope, and to determine the weight model that is suitable with cost factors, the tested accuracy, and detection accuracy. Surveys of this kind allow other researchers to build a single, ensemble, and hybrid approach most accurate for fraudulent credit card transaction detection (Malik et al., 2022; Alfaiz and Fati, 2022).

Sahithi et al. (2022) developed models that used a weighted average ensemble to combine LR, RF, KNN, Adaboost, and Bagging. The paper used the European Credit Card Company dataset. Their model had 99% accuracy, topping base models like RF Bagging (98.91%), LR (98.90%), Adaboost (97.91%), KNN (97.81%), and Bagging (95.37%). Their research shows that their ensemble model can detect credit card theft in this field. But, the feature selection process was not provided, which hinders productivity.

Qaddoura et al. (2022) in another study deliberated the effectiveness of oversampling methods: SMOTE, ADASYN, borderline1, borderline2, and SVM oversampling algorithms for credit card fraud detection. The researcher also engaged RF, LR, NB, KNN, SVM, and DT. The scholar discovered that oversampling can improve model performance, although the exact strategy depends on the ML algorithm. However, the applicability of the model in real-life situations can be affected due to the computational overhead. To this regard, (Table 1) was framed to showcase the summary of recent studies of 2023-2024 reviewed. Most of the scholar studies employed an open source dataset from Kaggle repository for their respective predictive and comparative data analysis; in which confusion matrix evaluation metrics were explored. It is obvious that most of the dataset betrothed by the scholars were obtained from an open source kaggle repository. This dataset is highly skewed and as well suffers from high dimensionality and sparsity and many others challenges towards the detection of credit card fraud. To which (Khalid et al., 2024; Gao, 2020; Mazumder, 2021) deliberates on the appropriate techniques to handle the imbalance data distribution via using of data augmentation techniques and re-sampling methods. *However, to answer the raised question one (Q1) of "*What is the best approach to implement in taming the unceasing act of credit card fraud?".

There is no particular suitable approach of ML and DL models that can be applied on credit card fraud detection, if real dataset is not available for experimentation. And the challenges of both ML and DL model regarding high dimensionality and sparsity problem is not regulated. Besides, the volume of the dataset utilize with features determines the efficiency performance of the models

Table 1: Overview of recent related work.

Literature Reference	Models	Dataset Source	Result	Remarks
Alraddadi (2023)	Decision Tree Algorithm (DCA)	Primary dataset. Questionnaire was administering. Qualitative and Quantitative method.	It is depicted that 95.9% of the respondents knew how credit fraud befalls. 4.1% of them did not. However, 81.6% expressed their willingness to practice a tool based on the projected model to prevents or detect credit card fraud incidents.	The Approach deploy cannot detect fraud during the transaction. More so, the algorithm is complex. Even a small change in data can distract the structure.
Shah and Makwana, (2023)	Five ML models of LR, DT, RF, NB and ANN	Review paper. Not specified	Dissimilartactics and methods used in credit card fraud detection, including traditional rule-based systems, machine learning algorithms, and deep learning models were explored.	Discuss the challenges associated with each approach and highlight the current state of the art in the field.
Devi and Parthibranj anray	CNN (Convolutional Neural Networks) , Machine Learning along with Artificial Intelligence	https://www.kaggle.com/mlg-ulb/creditcardfraud The data contained 284708 records and 31 features, 28 of which have been anonymized and are labeled V1-V28. The remain feature are the time, amount of transaction as well as label whether the transaction is fraudulent or not.	The results is overwhelming as the model reached a very high level of accuracy almost (99.8%) which is quite high compared to previous models like RF, LR and SVM	The work develops a webapp software has a high rate of accuracy and precision in predicting and detecting fraud detection. The software if integrated and expanded into commercial use can bring down fraud cases by a large extent.
Nalayini et al., (2023)	CNN with Smart matrix algorithm appropriate for large-sized real-time datasets	Kaggle	The pre-processing of the dataset is done using random under sampling for active training of the model. This pre-processing dataset is normalized for acquiring standardized input. The feature sequencing for feature selection is done by smart matrix algorithm. When compared to other ML methods such as Naïve Bayes and K-NN, the three layer CNN model performs better.	The performance is evaluated using confusion matrix, false alarm rate, sensitivity, Matthews correlation coefficient, balancing classification rate and F1-score
Madhavi et al., (2023)	Applied ML models of CNN	Kaggle	The research compared the performance of CNN model with RF and LR. Established that CNN model has best performance against other models	The study failed to states the percent of the CNN model.

Table 1 contd.

Akinola et al., (2023)	Two ML models of LR and Isolation Forest (iforest) is engaged	https://www.kaggle.com/mlg-ulb/creditcardfraud The data contained 284708 records and 31 features, 28 of which have been anonymized and are labelled V1-V28. The remain feature are the time, amount of transaction as well as label whether the transaction is fraudulent or not.	In evaluating the model performance precision, recall, F1-score and AUC-ROC curve were used. From the study outcomes, accuracy score for LR algorithm yielded 99.91% for training data and 78% for testing data, while the precision, recall and F1-score were 0.95, 0.56 and 0.70 respectively. However, the accuracy score for iforest algorithm yielded99.82% for training data and 74% for testing data, while the precision, recall and F1-score were 0.49, 0.49 and 0.49 respectively. From the results obtained upon evaluating the dataset, finding established LR algorithm as the model with outclass performance against iforest algorithm.	The dataset suffers from imbalance distribution nature which the scholars failed to address before establishing their findings
Ding et al., (2023)	Ensemble learning classification Variational Autoencoder Generative Adversarial Network (VAEGAN) and propose a new oversampling method that generates convincing and diverse minority class data were used.	Kaggle	The experimental results prove that the oversampling method utilizing the improved VAEGAN is superior to the oversampling method of Generative Adversarial Network (GAN), Variational Autoencoder (VAE), and Synthetic Minority Oversampling Technique (SMOTE) in terms of Precision, F1_score, and other indicators. The oversampling method based on the improved VAEGAN effectively deals with the classification problem of imbalanced data.	The training set is enhanced by generating minority class fraud data to train the ensemble learning classification model.
Akinola et al., (2023)	Two ML models of LR and Isolation Forest (iforest) is engaged	https://www.kaggle.com/mlg-ulb/creditcardfraud The data contained 284708 records and 31 features, 28 of which have been anonymized and are labelled V1-V28. The remain feature are the time, amount of transaction as well as label whether the transaction is fraudulent or not.	In evaluating the model performance precision, recall, F1-score and AUC-ROC curve were used. From the study outcomes, accuracy score for LR algorithm yielded 99.91% for training data and 78% for testing data, while the precision, recall and F1-score were 0.95, 0.56 and 0.70 respectively. However, the accuracy score for iforest algorithm yielded99.82% for training data and 74% for testing data, while the precision, recall and F1-score were 0.49, 0.49 and 0.49 respectively. From the results obtained upon evaluating the dataset, finding established LR algorithm as the model with outclass performance against iforest algorithm.	The dataset suffers from imbalance distribution nature which the scholars failed to address before establishing their findings
Ding et al., (2023)	Ensemble learning classification Variational Autoencoder Generative Adversarial Network (VAEGAN) and propose a new oversampling method that generates convincing and diverse minority class data were used.	Kaggle	The experimental results prove that the oversampling method utilizing the improved VAEGAN is superior to the oversampling method of Generative Adversarial Network (GAN), Variational Autoencoder (VAE), and Synthetic Minority Oversampling Technique (SMOTE) in terms of Precision, F1_score, and other indicators. The oversampling method based on the improved VAEGAN effectively deals with the classification problem of imbalanced data.	The training set is enhanced by generating minority class fraud data to train the ensemble learning classification model.

Table 1 Contd

Jayanthi et al., (2024)	Five ML models of ANN, SVM, RF, DT and NB	Kaggle	ANN proved an astounding performance of 97.6% accuracy trailed by SVM 95.5%, RF 94.5%, DT 92.3%, and NB 88.9% with the confusion matrix signifying high accuracy true negative, false positive, and false negative of each sample.	ANNs are faster in detecting frauds through Bayesian network give better results with a shorter training period but they are comparatively slower.
Khalid et al., (2024)	Ensemble model that incorporates SVM, KNN, RF, Bagging, and Boosting classifiers within a voting framework	https://www.kaggle.com/mlg-ulb/creditcardfraud The data contained 284708 records and 31 features, 28 of which have been anonymized and are labelled V1-V28. The remain feature are the time, amount of transaction as well as label whether the transaction is fraudulent or not.	Across the evaluation metrics of 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 findings 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.	The findings lay the groundwork for future advancements in the development of more resilient and adaptive fraud detection systems, which will become crucial for credit card fraud detection techniques
Aslam and Hussain (2024)	Six ML models of LR, RF, Extra tree, XGB, LGBM and categorical Boosting (CatBoost)	https://www.kaggle.com/datasets/nelgiriyewithana/credit-card-fraud-detection-dataset-2023 The dataset comprises of 550,000 records of credit card transactions performed in Europe in 2023 by cardholders, all of which have been anonymized to secure the cardholders' privacy and keep their identities secret The dataset includes the following features: • Id: A one-of-a-kind identification that is assigned to every single transaction. • V1–V28: Anonymized features reflecting various transaction attributes (such as time, location, and so on). • Amount: the total dollar value of the transaction. • Class: A binary label that indicates whether the transaction is fraudulent, with a value of either (1) or (0).	The training accuracy and testing results of all the evaluation metrics in the confusion matrix such as: Accuracy, Recall, precision and F1-scores, allthe ML Models presented (100%) results. Except for LR that presented a close range results at both instances.	Both Logistic Regression and LightGBM demonstrate remarkable efficiency, as their training times are on the scale of seconds. They provide an appealing option for use cases requiring quick model creation and iteration, especially in real-time or time-sensitive fraud detection. On the opposite side of the continuum, models like Random Forest and XGBoost demonstrate extended training durations, surpassing several minutes.

Table 2: Description of ML and DL models Applied.

Techniques	Benefits	Drawbacks
Logistics Regression (LR)	• It is easier to implement, interpret, and very effective to train. • It makes no assumptions about distributions of classes in feature space.	• The non-linear issue cannot be fixed with logistic regression because it has a linear decision surface.
Random forest (RF)	• RF can be engaged for both Classification and Regression tasks. • It has ability to handle large datasets with high dimensionality. • It promotes the thoroughness of the model and prevents over fitting problem. • knowledge High accuracy. Having a distributed memory Ability to make machine learning. Parallel processing capability	• Although RF can be applied for both classification and regression function, it is not more appropriate for Regression tasks. • Difficulty of showing the problem to the network. The duration of the network is unknown (High processing time for large neural networks
Isolation Forest	• The model is often used in anomalous classification and detection problem	• iForest's detection performance converges quickly with a very small number of trees, and it only requires a small sub-sampling size to achieve high detection performance with high efficiency.
Decision Tree (DT)	• High flexibility. Explainable • Easy to understand and implement • Can handle nonlinear data as well • It is simple to grasp and put into action. • It can be extremely useful in resolving decision action problems. • High adaptability, which aids in considering all potential solutions to a problem. • There is minimal need for data cleaning.	• Cannot detect fraud during the transaction • The algorithm is complex. Even a small change in data can distract the structure. • This method has many layers, making it difficulty. • It may own an over fitting issue, which the RF algorithm mastery resolve. The DR Arithmetic intricacy may increase.
Artificial Neural network (ANN)	• It is adept to detecting the fraudulent deed during the transaction. • It has ability to learn from the past. It does not need to be reprogrammed. • Storing information on the entire network. Ability to work with incomplete data. • It is powerful and used to handle complex computational task	• High processing time in case of large neural networks. • Extreme training required. It is difficult to set up and operate. • Sensitivity to data format. • The unexplained demeanor of the network. • It requires powerful computer with specialized processing units such as Tensor Processing Unit (TPU) and Neural Processing Units (NPU).
	• It shares close characteristic with ANN, CNN • It has small number of hidden layer • It has short training time • Graphical processing unit (GPU) is sufficient	It is composed of an input layer, hidden layers, output layers, weights, biases, and activation functions. MLP and CNN are just an instance of neural network
Convolution Neural Network (CNN)	• The CNN model is a DL model capable of solving imaging types of tasks. • The CNN model is a feedforward network entailing input, convolutional, pooling, and output layers. The details of this model can be exploit in (Baker et al., 2022) study. • It has number of hidden layers • Longer training time • Tensor Processing Unit (TPU) is sufficient.	The max-pooling layer was used to minimize the complexity of the feature matrix and the network complexity. The convolutional layer is responsible for extracting features from the initial input • Computer vision task are accomplishing with use of CNN • Receives input data in form of pictures and videos and then processes this data.
Proposed Light Gradient Bosting Machine (LGBM)	• It is a kind of gradient boosting technique based on decision tree and is used to increase the efficiency of a given classification model and works with reduced memory usage. • It is used in various ML application tasks such as ranking, classification, etc. • It is based on two new techniques. The first one is called as Gradient based One Side Sampling (GOSS) and Second one is known as Exclusive Feature Bundling (EFB) (Ramani et al, 2022; Aslam and Hussain, 2024). • LightGBM can be utilized in credit card fraud detection to examine transaction data, encompassing attributes like transaction time, location, amount, and historical data.	• Developed to address the drawbacks of the histogram approach used in GBDT Gradient Boosting Decision Tree (GDBT) models. • The characteristics of LGBM model are achieved by methodologies of EFB and GOSS (Guolin et al., , 2017).

deployed. Most especially DL models often delivers a better performance once data that are abounds with the characteristics of big data is utilized for experiment.

Table 2 presented an analogy of the ML and DL models deployed I this research for predictive data analysis.

```
df = pd.read_csv('/content/creditcard.csv')

df.head()
```

	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

5 rows × 31 columns

```
df.info()

<class 'pandas.core.frame.DataFrame'>
RangeIndex: 89220 entries, 0 to 89219
Data columns (total 31 columns):
 #   Column  Non-Null Count  Dtype
```

Figure 1: Sample of The First Five Row Kaggle Credit Card Dataset utilized for Experiment

Table 3: Normal Non-Fraudulent Transaction Distribution Description.

Count	Mean	Std.	Min	25%	50%	75%	Max
89008	98	266	0.00	7.680	26.990	89.90	19656.55

Table 4: Fraudulent Transaction Distribution Description.

Count	Mean	Std.	Min	25%	50%	75%	Max
211.00	1.0.71	242.7	0.00	1.00	7.580	99.99	1809.68

MATERIALS AND METHODS

This section describes the methodological approached employ in this study which (Figure 1) presented the sample of the kaggle credit card transaction dataset utilized for experiments.

Dataset

The open-source dataset engaged for this study is obtained from Kaggle repository. It comprises of 89219 records and total of 31 features data column. The datasets encompass of 89008 normal transactions and 211 fraudulent transactions. The major purpose of this dataset is to make it easier to construct algorithms and models to detect possibly fraudulent transactions (Aslam and Hussain, 2024). The non-fraudulent transaction details is display in Table 3 via the construct of the python command: normal_df.Amount.describe (); which that of fraudulent transaction is also displayed in (Table 4) delving the python construct of fraud_df.Amount.describe ( ). With Figure 10 displaying the fraudulent and non-fraudulent class distributions. Upon conducting the Exploratory Data Analysis (EDA) procedure, a comparison of values and occurrence of each class was performed, and a pie chart was utilized to visualize the class distribution as shown in Figure 1*)*. The analysis revealed that the dataset is highly imbalanced,

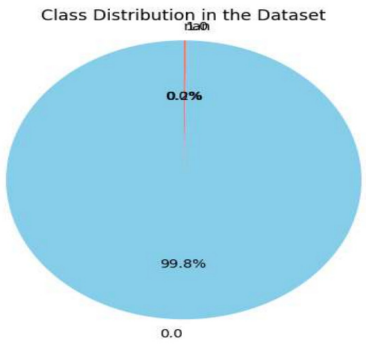


Figure 10: Imbalance Class distribution of dataset

with 99.89% non-fraudulent and 0.2% fraudulent cases, consistent with findings in prior studies (Khalid et al., 2024; Akinola et al., 2023). To address the imbalance, a baseline experiment was conducted on the dataset in section 3.4.1 to determine the best performing machine learning models, specifically LR and RF. Subsequently, a balancing model experiment using Synthetic Minority Oversampling Technique (SMOTE) was performed in section 3.4.2. This involved leveraging the best performing baseline model (RF) alongside other machine learning models such as Isolation Forest, proposed LGBM, and deep learning models including

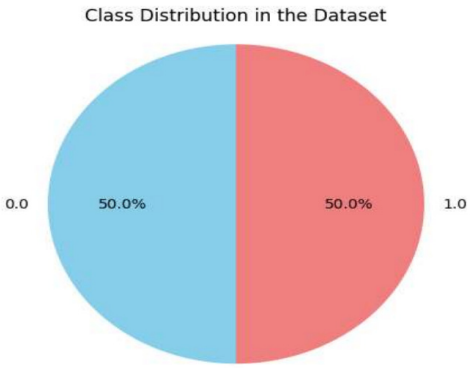


Figure 2: Class Balancing distribution dataset

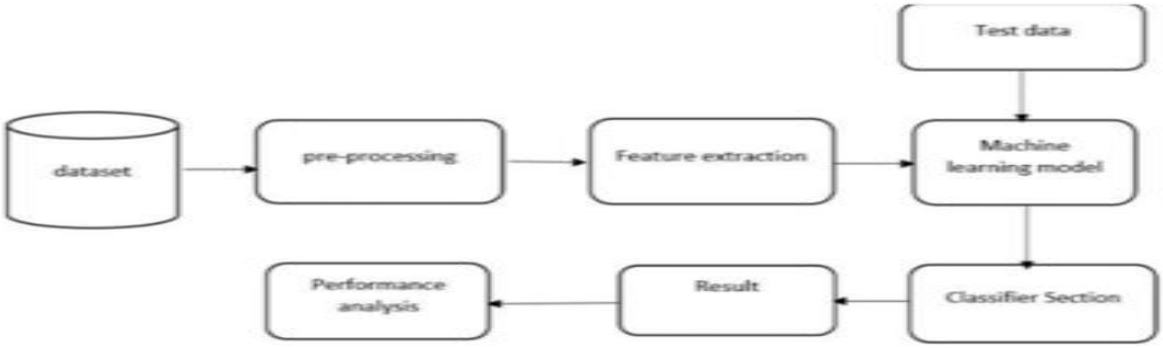


Figure 3: Proposed Methodology (Devi and Parthibranjanray, 2023).

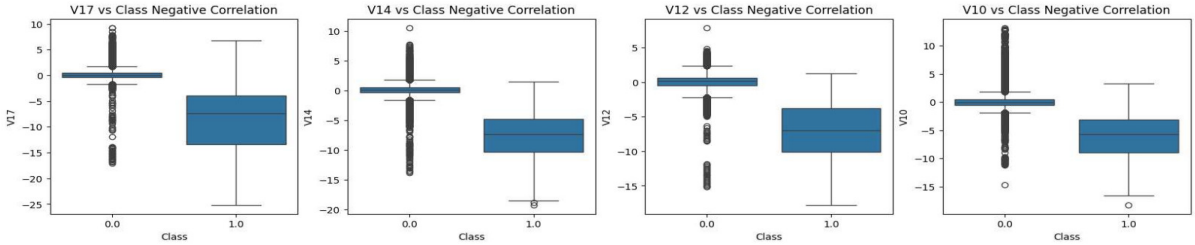


Figure 4: Negative Correlation with classes.

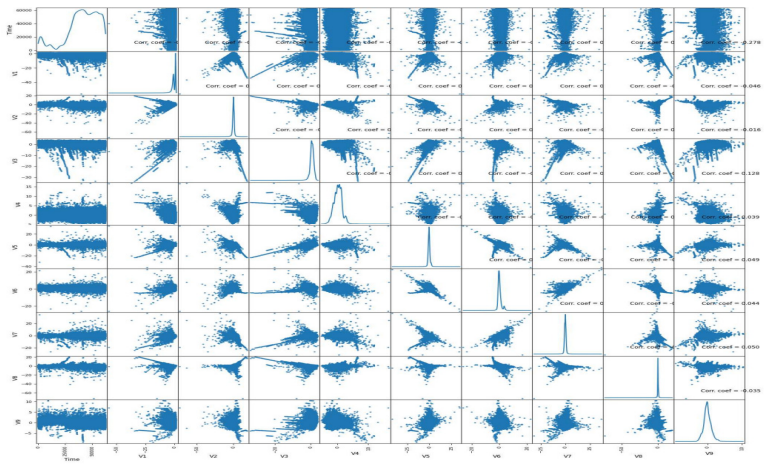


Figure 5: Scatter and Density Plot for the Credit Card Fraud Dataset

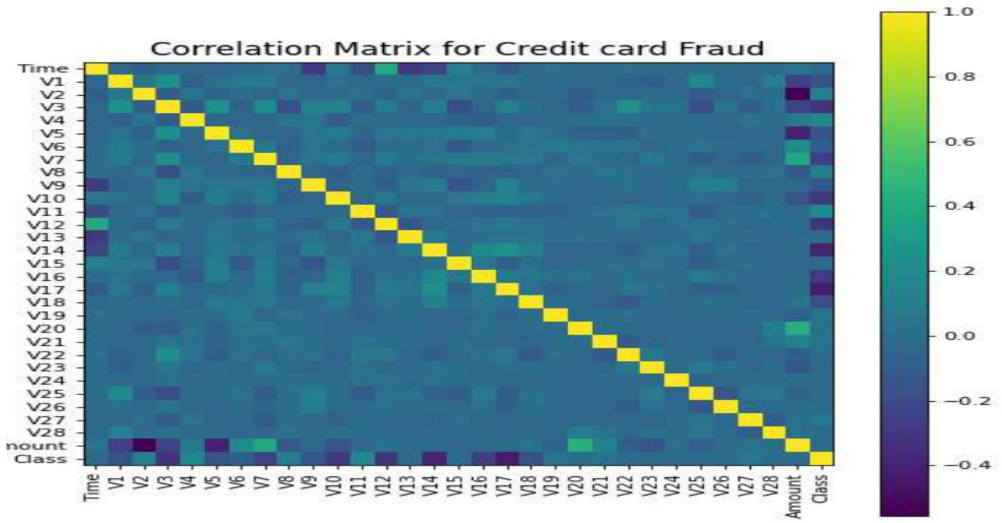


Figure 6: Correlation Matrix of the credit card fraud dataset

ANN, MLP, and CNN. Figure 2 illustrates the class distribution achieved through the balancing model.

Proposed methodology

This study absorbed the structure and implementation process enunciated in (Devi and Parthibranjanray, 2023) study for credit card fraud detection. The approach is simple with robust system architecture. They are as follows:- • Preprocessor • Feature Extractor • Machine and Deep Learning Models• Classifier • Performance Analysis • Result Display (Figure 3).

Exploratory Data Analysis (EDA) and Implementation Platform

This is achieved via pre-processing steps that encompasses: Data Cleaning, Encoding the categorical data, Feature Scaling, Data Re-sampling methods; Feature correlation and selection; Splitting of the dataset into training and testing sets with validations and Application of selected models (e.g. LR, RF, Isolation Forest, MLP, and others) for performance evaluation and comparison of the models to determine the one with outclass performance (Akinola et al., 2023; Devi and Parthibranjanray, 2023). During this procedure correlation matrix, class negative correlation and scatter with density plot for the credit card fraud dataset is visually presented (Figures 4, 5, 6).

This work has been implemented on a personal laptop with Intel i7-5600U CPU, 2.6GHz speed, 16 GB RAM, and a SSD hard disk. The memory consumption rate is 25%, at most, and hard disk utilization is almost 0%. Thus, the laptop is adequate for this study. In this study, Scikit learn package is used for machine learning classification while Tensorflow is deployed for the deep learning (Figure 6). The Python programming language utilized in this study engaged pre-processing library like Numpy, Pandas, Scikit-Learn, Matplotlib, Seaborn and many others which (Akinola et al., 2023) described in their study. Google Colab, Anaconda, Jupyter notebook and Google drive cloud infrastructure platforms were the utilized environments and it was extensively described in (Sharma, 2020).

Data sampling

After pre-processing, the subsequent step in the process involved in addressing the data imbalance problem through re-sampling data proliferate with data augmentation method (LinkedIn, 2023). This is one of the most commonly preferred approaches to deal with an imbalance dataset. These are broadly classified into two types of methods:

(a) Under-Sampling: In sampling, a random sample was picked from the major class, which were normal transactions (labeled as 0) in this case (89008). The number of random samples was determined according to the ratio required concerning the minority class. In this paper, for better model training, the entries for both classes were made equal by choosing a random sample equal to minority class entries and concatenating the data from both classes to have one dataset.

(b) Oversampling: In most cases, oversampling is preferred over the under-sampling techniques (Khalid et al., 2024).

It tends to remove instances from the data that perhaps carries some important information. This research applied SMOTE over-sampling method (Gao, 2020). SMOTE (Synthetic Minority Over-Sampling Technique): SMOTE is a statistical method for extending the number of

Table 5: Confusion Matrix.

		PREDICTED FRAUD		
	N	**0 (No)**	**1 (Yes)**	**Total (n)**
ACTUAL FRAUD	0 (No)	True Negative (TN) (m)	False Positive (FP) (o)	(m + o)
	1 (Yes)	False Negative (FN) (l)	True Positive (TP) (e)	(l + e)
	Total	(m + l)	(o + e)	(m + o) + (l+ e) ≡ (m+l) + (o+e)

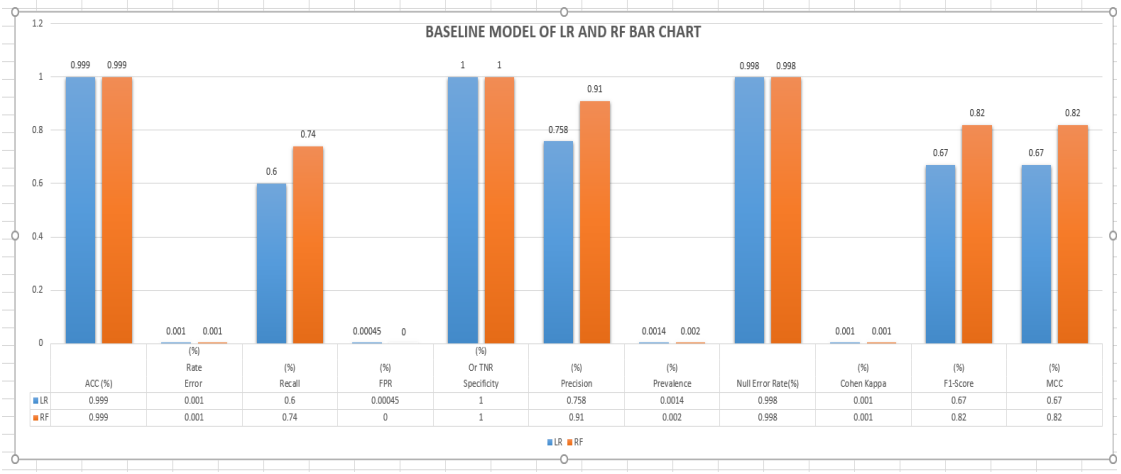


Figure 7: Bar chart with validation result table for baseline models of LR and RF

minority class instances in a balanced manner in a dataset. The component created new instances from existing minority cases that were provided as input (Khalid et al., 2024). So, for SMOTE, the fraud class (labeled as 1) with 211records was oversampled, equal to the normal transaction class to have identical entries for each class to train models optimally. And like under-sampling, both classes were merged to have one dataset. This algorithm helps to overcome the over-fitting problem posed by random oversampling. It is focused on the feature space to generate new instances with the help of interpolation between the positive instance (fraudulent class) that lie together. The sampling process involved two steps, delineated as follows:

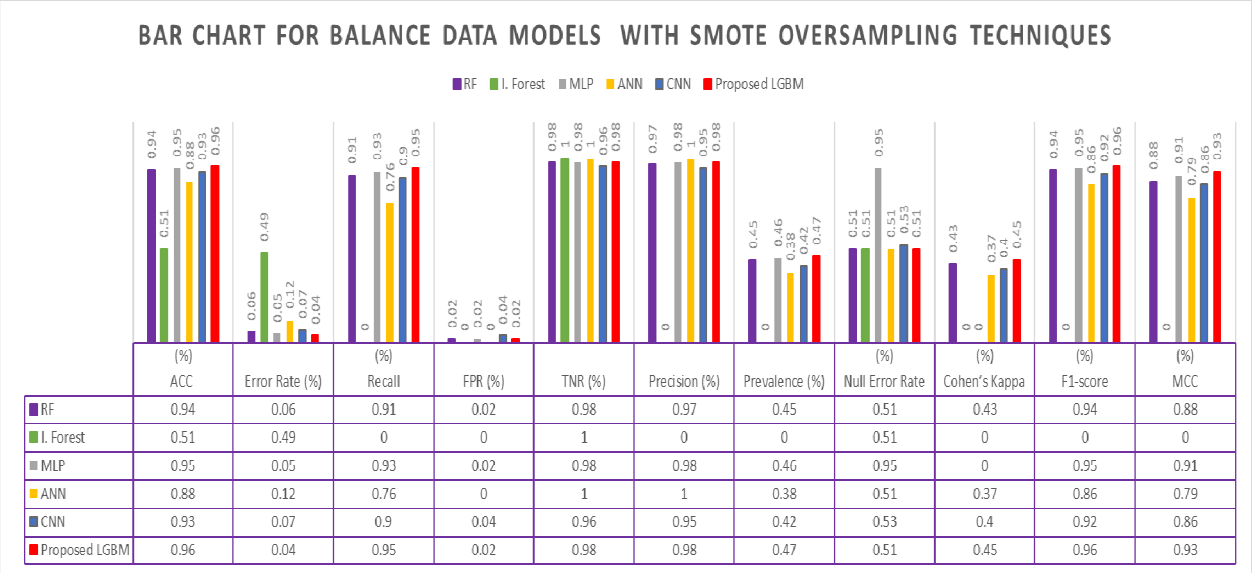
• Separate data records based on labels (normal and fraudulent classes)
• Apply the obligatory sampling technique to specific data
• Concatenate all data to have all data in a single dataset

Model training

Evaluation metrics

This can be establishing via the confusion matrix table of (Table 5); which reviews each tuples traits. A confusion matrix is a table that is often used to designate the performance of classification model (or "classifier") on a set of test data for which the true values are known. It permits the visualization of the performance of an algorithm. The confusion matrix standards and evaluation metrics contained therein are vigorous expounded in (Cicekli, 2022; Baker et al., 2022; Noviandy et al., 2023) distinct study. Besides, the Matthews correlation coefficient (MCC)method is inculcated for this study. This is influenced based on (Comotto, 2022) study. The article introduces two uncommon evaluation metrics for classification problem which are Brier Score (BS) and MCC for different perception of model evaluation in ensuring good result. Model evaluation is understood as the process of assessing how well ML models performs the specific task they are considered to do (Comotto, 2022); such as predicting the presence or eligibility of event.

Whenever a ML model is built, it is done at some point as there is need to evaluate it in order to ensure good result. In this study, only MCC is delved; Brier score will be exploring in the subsequent research to exploit it efficacy. MCC was invented in 1975 by Brian Matthews. It is a statistical tool used for model evaluation. Its job is to gauge or measure the differences between the predicted values and actual values and is equivalent to chi-square statistics for a 2*2 contingency table. The syntax for MCC formulation:



	(%) ACC	Error Rate (%)	(%) Recall	FPR (%)	TNR (%)	Precision (%)	Prevalence (%)	Null Error Rate	(%) Cohen's Kappa	(%) F1-score	(%) MCC
RF	0.94	0.06	0.91	0.02	0.98	0.97	0.45	0.51	0.43	0.94	0.88
I. Forest	0.51	0.49	0	0	1	0	0	0.51	0	0	0
MLP	0.95	0.05	0.93	0.02	0.98	0.98	0.46	0.95	0	0.95	0.91
ANN	0.88	0.12	0.76	0	1	1	0.38	0.51	0.37	0.86	0.79
CNN	0.93	0.07	0.9	0.04	0.96	0.95	0.42	0.53	0.4	0.92	0.86
Proposed LGBM	0.96	0.04	0.95	0.02	0.98	0.98	0.47	0.51	0.45	0.96	0.93

Figure 8: Bar Chart with Validation Result Table for Balance Data Models using SMOTE Over sampling Techniques

Matthews correlation coefficient

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

$$(worst\ value: -1, best\ value: +1)$$

Baseline models experiments

Based on the analysis, two machine learning models, Logistics Regression (LR) and Random Forest (RF), were utilized to examine the distribution of an imbalanced dataset, particularly focusing on the minority fraudulent class which represents the positive class. The confusion matrix of the baseline experiments is presented in (Table 5), while Figure 7 provides a visualization of the validation results for the baseline models.

Balancing models

The balancing model used in this study comprises the selected RF baseline model with outstanding performance, isolation forest, MLP, ANN, CNN and the proposed Light Gradient Boosting machine (LGBM). The experiment done presented the (Table 7) confusion matrix for balancing model after which Synthetic Minority Oversampling Techniques method (SMOTE) had been applied to overcome the class imbalance distribution of the kaggle dataset engaged (Gao, 2020).

RESULTS AND DISCUSSION

Baseline models results

The Table 6 depicts the baseline models. The (Figure 7) presents the visualization and the table for the experiment validation results.

Table 6: The Confusion Matrix for the Baseline models.

Models	TN	FP	FN	TP
LR	17794	8	17	25
RF	17799	3	11	31

From where its discovered that LR denoted in blue color and RF in orange color presented the same accuracy results of (99.9%), Error rate or misclassification of (0.1%), Null error rate (NER) of (99.8%), True negative rate (TNR) of (1.00%) and Cohen Kappa of (0.1%) respectively. This results is however biased, as the imbalance data utilized necessitate misclassification and poor performance of the ML results (Baker et al., 2022). The bases for adjudging this baseline models are the recall, FPR, precision, prevalence, F1-score and Matthews Correlation Coefficient (MCC). The visibility results establish that RF presented an outclass performance against LR. In this, the recall display results of LR (59.5%), RF (74%); for Precision LR (75.8%) while that of RF (91.2%), Prevalence LR is high with (0.14%) that of RF is less with (0.2%), FPR of LR (0.045%) and RF (0.02%). The F1-score and MCC of LR is (67%) respectively); while that of RF is (82%) distinctly which is superior.

```
Confusion Matrix:
 [[22  1]
 [ 2 18]]

Classification Report:
              precision    recall  f1-score   support

         0.0       0.92      0.96      0.94        23
         1.0       0.95      0.90      0.92        20

    accuracy                           0.93        43
   macro avg       0.93      0.93      0.93        43
weighted avg       0.93      0.93      0.93        43
```

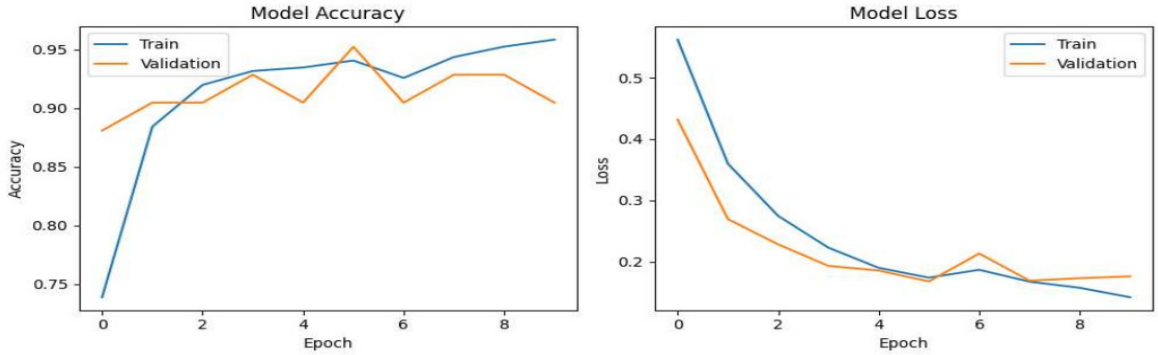


Figure 9: CNN Confusion Matrix display with Model Accuracy and Model Loss Screen Short

Based on the results findings, it has been established that the Random Forest (RF) model outperforms other baseline models in terms of performance evaluation. Therefore, the RF model has been selected for further experimentation in the second phase, where the imbalanced dataset distribution is addressed using the SMOTE oversampling method. In this phase, the RF model will be compared against other machine learning models such as Isolation Forest, the proposed Light Gradient Boosting Machine (LGBM) classifier, as well as deep learning models including Artificial Neural Networks (ANN), Multilayer Perception (MLP), and Convolutional Neural Networks (CNN). This comparison aims to provide a comprehensive understanding of the performance of the RF model in relation to other advanced models in handling the imbalanced dataset.

Balance models results

Figure 8 analysis results findings. Where its exemplified that RF is ascribed with purples colors, Isolation forest green color, MLP ashes color, ANN yellow color, CNN blue color and proposed LGBM orange color respectively; for easy description of the models recitals.

Accuracy score

From the Figure 9 illustration; the proposed LGBM model presented an outclass performance of (96%) followed by MLP (95%), RF (94%), CNN (93%), ANN (88%). Isolation forest is the model that offered the worst accuracy score of (51%).

Error Rate/Misclassification

The propose LGBM model gave the least misclassification result of (0.4%), in ascending order with other models like MLP (0.5%), RF (0.6%), CNN (0.7%), ANN (12%) and Isolation forest (49%).

Recall/Sensitivity

Here, the proposed model of LGBM Presented the best recall results of (95%)against MLP (93%), RF (91%), CNN (90%), ANN (76%); to which isolation forest displays (0.00%) results to be christened the model with worst recall result.

False positive rate (FPR)

Under this evaluation metrics, the model like RF, MLP and proposed LGBM displayed the same results of (0.2%) respectively. While isolation forest with ANN offered (0.00%) and CNN is discovered to be the model with presented the highest FPR result of (0.4%).Specificity/ true negative rate (TNR)

In this evaluation metrics, Isolation forest and ANN presented overwhelming results of (100%) as the best

model with specificity. While RF, MLP, and proposed LGBM offered (98%) results respectively to be the second inline; and CNN (96%) as the third model with close range result.

Precision

ANN is discovered as the model with the highest results of (100%), followed by both MLP and the proposed LGBM presenting (98%) distinctly. RF is the third in the hierarchy offering (97%), CNN (95%) close par result and isolation forest (.00%) to still be the worst model under this stance.

Prevalence

The proposed LGBM presented the highest prevalence results of (47%) in close range with MLP (46%), RF (45%) and CNN (42%). ANN presented the lowest prevalence of (38%) while Isolation forest (0.00%) retains the worst performances.

Null Error Rate (NER)

The MLP presented the highest and best NER result of (95%), CNN offered (53%)as the second model. While, RF, isolation, ANN and proposed LGBM offered same NER results of (51%) respectively; to be the third in the hierarchy.

Cohen's Kappa

The proposed LGBM model presented an outclass performance of (45%), followed in ascending order of (43%) ascribed to RF, CNN (40%), and ANN (37%). Isolation forest and MLP presented the worst results here both presenting (0.00%) results distinctly.

F1-Scores

The proposed LGBM presented an outclass performance with (96%), followed by MLP (95%) and RF (94%) in close range. CNN (92%), ANN (86%) and Isolation forest (0.00%) as the worst performance model.

Matthews Correlation Coefficient (MCC)

The proposed LGBM model presented an outclass performance results of (93%), followed in close range with MLP (91%), RF (88%), CNN (86%), ANN (79%) and Isolation forest (0.00%)as the model with the degrading performance result.

Conclusion and Recommendation

It is surmised that the proposed LGBM offered an outshine performance across seven aspects of the evaluation metrics; out of the eleven instances deployed. The model has an accuracy scores of (96%), least error rate or misclassification of (0.4%), Recall (95%), prevalence (47%), Cohen Kappa (45%), F1-score (96%) and MCC (93%) against other ML models of RF and Isolation forest, and deep learning models of ANN, MLP and CNN. The reason for it excelling performance lays with few numbers of transaction dataset utilized. Retrospectively, the deep learning models could have presented an outclass performance if big dataset are delved as the models performs better with large dataset. However, in terms of FPR, the deep learning model of CNN presented the highest results of performance of (0.4%) compared to the other models that are glued with least similar outcomes distinctly. Isolation forest and ANN presented superclass TNR evaluation performance of (100%) against other models. In terms of precision, ANN gave (100%) while MLP offered the highest NER results of (95%) against other models. The ML and DL techniques applied help identify fraudulent activities (Aslam and Hussain, 2024). This study provides a comparative analysis of Regression, boosting models and deep learning, including LR, RF, Light GBM, and ANN, MLP, and CNN. The study is useful for beginner researchers to understand the performance of the ML models for fraudulent transaction detections using a public dataset.

In the future work, an enhance hybrid deep learning method is advised forexploit towards the detection of fraudulent credit card deeds. The evaluation of these machine learning models can be performed using multiple datasets. Also, the deep learning models can be applied for credit card fraud detection using the same dataset, along with other datasets, to compare the performance of machine learning and deep learning models in order to have more lucid results that can enable financial institutes averts the sacrilege of financial losses incurred monumentally due to credit card fraud scenarios.

REFERENCES

Aghware, F.O, Yoro, R. E, Ejeh, P.O, Odiakaose, C. C, Emordi, F. U, and Ojugo, A.A.(2023). "DeL Clust E: Protecting Users from Credit-Card Fraud Transaction via the Deep-Learning Cluster Ensemble", (IJACSA) International Journal of Advanced Computer Science and Applications, 14(6), (2023), 94-100. www.ijacsa.thesai.org

Alfaiz, N.S., and Fati, S. M., (2022). "Enhanced Model using Machine Learning",(2022). Electronics, 11,662. https://doi.org/10.3390/electonics11040662

Alghawi, N. (2019). A Study on SIM Box or Interconnect Bypass fraud, Dissertation Submitted in fulfilment of the requirement for the degree of M.Sc. Informatics, The British University, Dubai, U.A.E.

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, 2(1): (2023), 187-195. https://journals.unizik.edu.ng/index.php/ujeas

Alraddadi, A. S.(2023). "A Survey and a Credit Card Fraud Detection and Prevention Model using the Decision Tree Algorithm",

Engineering, Technology and Applied Science Research, 13(4): (2023), 11505-11510.
Aslam, A., and Hussain, A.(2024) “A performance Analysis of Machine Learning Techniques for Credit Card Fraud Detection”, Journal on Artificial Intelligence. (2024). Doi:10.32604/jai.2024.047226.
Baker, M.R., Mahmood, Z. N., and Shaker, E. H.(2022) “Ensemble Learning with Supervised Machine Learning Models to Predict Credit Card Fraud Transactions”, Revue d' Intelligence Artificielle, 36 (4): (2022), 509-518. Journal homepage: http://iieta.org/journals/ria
Brownlee, J. (2019)). 14 Different Types of Learning in Machine Learning, Blog, Retrieved from: https://machinelearningmastery.com/types-of-learning-in-machine-learning/.
Cicekli, I.(2022) “Classification Model Evaluation and Selection and ensemble Methods” Data Mining, (2022). https://www.lec07_Classification_ModelEvaluation_Ensemble.pdf
Comotto, F.(2022) “Evaluation Metric: leave your Comfort Zone ant try MCC and Brier scope”, (2022, Jan 8). https://towardsdatascience.com/evaluation-metrics-leaves-your-comfort-zone-and-try-mcc-and-brier-score-86307fb1236a
Devi, R.R., and Parthibranjanray (2023) “Credit Card Fraud Detection using AI/ML/CNN”, IRE 1704172 Iconic Research and Engineering Journalsire, 6(9): (2023), 242-249 | ISSN: 2456-8880
Ding, Y., Kang, W., Feng, J., Peng, B., and Yang., A.(2023) “Credit Card Fraud Detection Based on Improved Variational Autoencoder Generative Adversarial Network”, IEEE Access, Vol 11, (2023), 83680- 83691. Digital Object Identifier 10.1109/ACCESS.2023.3302339
Falco, A, “Understanding the Threat of Card Transaction Fraud and its Impact on the Financial Ecosystem”, (2023, February 21). https://www.waylay.io/articles/understanding-the-threat-of-card-transaction-fraud-and-its-impact-on-the-financial-ecosystem
Fayyomi, A. M, Eleniyan, D., Eleniyan, A. (2021)). A Survey Paper On Credit Card Fraud Detection Techniques, International Journal of Scientific and Technology Research, 10 (9): 72-79. http://www.ijstr.org/
Gao, J.(2020). “Data Argumentation in Solving Data Imbalance Problems”, Degree Project in Computer Science and Engineering, Second Cycle, 30, credits StockHolm, Sweden (2020).
Great Learning Team, “Credit Card Fraud Detection (2023). https://www.mygreatlearning.com/blog/credit-card-fraud-detection/
Ke et.al, (2017). “LightGBM: A Highly Efficient Gradient Boosting Decision Tree” , 31st Conference on Neural Information Processing Systems (NIPS 2017), Long Beach, CA, USA.
Hassan, P.(2016). “Artificial Learning, Machine Learning and Deep Learning: Know the Difference” (2016, December 17). https://blogs.systweak.com/artificial-learning-machine-learning-and-deep-learning-know-the-difference/
Hayes, A., Anderson, S., Kvilhaug, S.C., (2023). What is a financial institution? Investopedia. https://www.investopedia.com/terms/f/financialinstitution.asp
Horton, M.(2023) “Different types of Financial Institutions”, Investopedia, (2023, September 19). Retrieved from: https://www.ivestopedia.com/ask/answer/061615/what-are-major-categories-financial-institutions-and-what-are-their-primary-role.asp
International Public Sector Fraud Forum [IPSFF], “Guide to Understanding the Total Impact of Fraud”, Cabinet Office and Commonwealth Fraud Prevention Centre, (2020, February). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/778306GuideTounderstandingtheTotalimpactoffraud.pdf
Jain, S., Dubey, S., Tiwari, N., Jain, Y., Shalan, A.(2022). “A Novel Trio-Hybrid for Detecting Fraudulent Credit Card Transactions”, ACI’22: Workshop on Advances in Computation Intelligence, its Concepts Applications at ISIC (2022), May 17-19, Savannah, United State
Jain, Y., Tiwari, N., Dubey, S., and Jain,S. (2019), “ A comparative analysis of various credit card fraud detection techniques”, Int J Recent TechnolEng 7 (2019) 402–407.
James, G., Witten, D., Hastie, T., and Tibshirani, R.(2017) “An Introduction to Statistical Learning with Applications in R”, Springer New York Heidelberg Dordrecht London, (2017). DOI 10.1007/978-1-4614-7138-7
Jayanthi, G., Deepthi, p., Rao, N.B, Bharathiraya, M., LogaPriya, A.(2024) “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), 12 (125). https://ijisae.org/index.php/IJISAE/archieve/view/4504
Jendruszak, B.(2023) “Credit card fraud detection: The Guide”. Seon (2023, July 14). https://seon.io/resources/credit-card-fraud-detection/
Jiang, S.; Wang, J.; Dong, R.; Xia, M. (2023). Credit Card Fraud Detection Based on Unsupervised Attentional Anomaly Detection Network. Systems 2023, 11, 305. https://doi.org/10.3390/systems11060305
Jovel, J. and Greiner, R. (2021)). An introduction to Machine Learning Approach for Biomedical Research. https://www.frotiersin.org/articles/10.3389/fmed.2021.771607/full
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), 8, 6. https://doi.org/10.3390/bdcc8010006
Madhavi, M., Reddy, K.R.V, Swetha, B., and Kumar, R.B.(2023). “Credit card Fraud Detection using CNN”, IJRTI, 8 (4): (2023). 845-854. www.ijrti.org
Malik, E.F., Khaw, K. W., Belaton, B., Wong, W. P., and Chew, X. (2022). ‘Credit card fraud detection using a new hybrid machine learning architecture,’ Mathematics, 10(9): p. 1480, Apr. 2022, DOI: 10.3390/math10091480.
Maniraj, S.P., Saini, A., Sarkar, S. D, Ahmed, S. (2019). Credit Card Fraud Detection Using Machine Learning and Data Science, International Journal of Engineering Research and Technology (IJERT), 8(9): 110-115. www.ijert.org
Mazumder, S. (2021). “5 Techniques to Handle Imbalanced Data for a Classification Problem”, (2021, June 21). https://www.analyticsvidhya.com/blog/2021/06/5-techniques-to-handle-imbalance-data-for-a-classification-problem/
Mienye, I. D., Sun, Y.(2023) “A Deep Learning Ensemble with Data Resampling for Credit Card Fraud Detection”, Applied Research IEEE Access, vol. 11, (2023), 30628-30638. DOI 10.1109/ACCESS.2023.3262020.
Nalayini, C.M, Katiravan, J., Sathyabama, A. R., Rajasuganya, P. V., and Abirami, K.(2023). “Identification and Detection of Credit card fraud using CNN”, Application of Computational Intelligence in Management and Mathematics, (2023), 267-280.
Noviandy, T. R., Idroes, G. M., Maulana, A., Hardi I., Ringga E.S., and Idroes, R.(2023). “Credit Card Fraud Detection for Contemporary Financial Management Using XGBoost-Driven Machine Learning and Data Augmentation Techniques”, Indatu Journal of Management and Accounting, 1(1): 2023. https://heca-analitika.com/ijma
Prasad, P.Y.; Chowdary, A.S.; Bavitha, C.; Mounisha, E.; Reethika, C. (2023). 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.
Ramani, K., Sunetha, I., Pushpalatha, N., and Harsih, P.(2022). “Gradient Boosting Techniques for Credit Card Fraud Detection”, Journal of Algebraic Statistics, 13(3): (2022), 553-558. https://publishoa.com ISSN:1309-3452
Sahithi, G.L.; Roshmi, V.; Sameera, Y.V.; Pradeepini, G.(2022) “Credit Card Fraud Detection using Ensemble Methods in Machine Learning”. In Proceedings of the 2022 6th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 28–30 April (2022); pp. 1237–1241. [CrossRef]
Shah, A., and Makwana,Y., (2023). Credit Card Fraud Detection, ResearchGate https://www.researchgate.net/publication/369857378_Credit_Card_Fraud_Detection?enrichId=rgreq-eabeb7230eb249e80a2f00e3159b130d-XXXandenrichSource=Y292ZXJQYWdlOzM2OTg1NzM3ODtBUzoxMTQzMTI4MTEzOTQwMjE5OEAxNjgwODUwMTg3OTU1andel=1_x_2and_esc=publicationCoverPdf
Sharma, A.(2020) “Free GPUs for Everyone! Get Started with Google Colab for Machine learning and Deep learning”, (2020).

https://www.analyticsvidhya.com/blog/2020/03/google-colab-machine-learning-deep-learning/

Tata Consultancy Services (TCS), (2003, June). Understanding credit card frauds, cards business review#2003–01, http://www.tcs.com/

White, A. (2023)). Here's how credit card fraud happens and tips to protect yourself. https://www.google.com/amp/s/www.cnbc.com/amp/select/credit-card-fraud/

Adeleke, A. J. (2022). Development of an Automated Real-Time Credit Card Fraud Detection System, A Project Submitted in The Department of Computer Science and Mathematics, College of Basic and Applied Sciences in Partial Fulfilment of the Requirements for The Award of the Degree of Bachelor of Science, Mountain Top University, Ibafo Ogun State, Nigeria.

Aggarwal (2024)). Financial Institution: Types, Roles and Advantages. https://www.shiksha.com/online-course/articles/financial-institutions-types-roles-and-advantages

Aggarwal, C. C., (2018). Neural Network and Deep Learning, A Springer Textbook, IBM T. J. Watson Research Center, International Business Machines,Yorktown Heights, NY, USA. ISBN 978-3-319-94462-3 ISBN 978-3-319-94463-0 (eBook), https://doi.org/10.1007/978-3-319-94463-0

LinkedIn, (2023)). How you can address class imbalance in Binary Classification task? https://ww.linkedin.com/advice/0/how-can-you-address-class-imbalance-binary-classification-yxkve.