Published by
NIGERIAN SOCIETY OF PHYSICAL SCIENCES
Available online @ https://journal.nsps.org.ng/index.php/jnsps

J. Nig. Soc. Phys. Sci. 6 (2024) 2037

Journal of the Nigerian Society of Physical Sciences

Deep convolutional neural network based synthetic minority oversampling technique: a forfending model for fraudulent credit card transactions in financial institution

L. G. Salaudeen*, D. Gabi, M. Garba, H. U. 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

Abstract

Fraudulent credit card transactions are committed by unauthorized individuals and organizations employing methods such as phishing and social engineering fraud tactics. Researchers propose several Machine Learning (ML) techniques to deter the challenges of credit card fraud. However, the ML approaches are endorsed with some challenges, which makes the detection of credit card fraud extremely difficult. This study proposes a Deep Convolutional Neural Network (DCNN) with Synthetic Minority Oversampling Techniques (SMOTE) as an ideal solution. Kaggle datasets with 284,807 records and 31 features were exploited. Implementation was performed on the Google Colab cloud-based platform, embedding a Jupyter notebook setting with Graphical Processing Units (GPUs). Two experiments were conducted; the first was probed to determine suitable models among baseline models: Logistic Regression (LR), Random Forest (RF), Isolation Forest, and a single Deep Learning (DL) model of Multiple Layer Perceptron (MLP). The baseline models yielded an overfitting accuracy score, with recall, specificity, precision, and F1-score all presenting 1.00% respectively. This outcome is not sufficient in establishing findings on imbalanced data distribution as it's biased. This led to the construction of a new ML model incorporating Light Gradient Boosting Machine (LGBM), with Artificial Neural Network (ANN) and the proposed DCNN+SMOTE for the second experimental phase alongside baseline models. Experimental results via simulation show the proposed DCNN+SMOTE yielded awesome superclass performance across the board, displaying 1.00% results respectively. Its Error Rate (ER) and Null Error Rate (NER) are 0.00% distinctly. Meanwhile, the False Positive Rate (FPR) yields a 0.001% result, lesser and better than the baseline models.

DOI:10.46481/jnsps.2024.2037

Keywords: Data augmentation techniques, Imbalance data-set, Deep learning, Credit card fraud, Confusion matrix

Article History :
Received: 09 March 2024
Received in revised form: 24 April 2024
Accepted for publication: 25 April 2024
Published: 12 May 2024

Communicated by: O. Akande

1. Introduction

In time memorial, fraudulent credit card transactions had been misery to global financial institutions; for its taunting their operational and developmental proceedings. Thus, leaving derogatory imprints of unquantifiable economic losses, customer frictions, reputation and infrastructure damages; that perhaps instills fears, psychological defects on victims (e.g. Cardholders, Merchant, and Card issuers); as it triggers national security threats and vulnerabilities [1–4]. To which cognizance is

*Corresponding author Tel. No.: +234-706-744-2771.
Email address: gbolahan_salaudeen@yahoo.co.uk (L. G. Salaudeen)

emphasize for defensive measures in ensuring regularities [5–7]. In this study, an introductory concept of credit card and credit card fraud is established [8]. Where World bank [9] study describes credit card together with its prowess and shortcomings, TATA consultancy services [10] and White [11] in separate studies abreast about the credit card fraud phenomenon ravaging financial institutions. Ayorinde [12] and Al-Smadi [13] describes a situation "where an individual uses another individual' credit card credentials (e.g. PIN, Cardholder name, etc.) for deceitful purposes without the card owners and the card issuer knowledge". Credit card fraud is broadly classified into two forms of online and offline fraud [12–14]; logically known as behavioral and application fraud [8, 14].

Application fraud befalls when individual obtained new credit cards from issuing companies using false personal credentials and then squander as much as possible within a short period of time. However, most credit card fraud is behavioral; these befalls when details of genuine cardholders are obtained fraudulently and purchases are made on real cardholder as liability incurred while payment are virtually made [8, 15]. This payment maybe for telephone sale, Airtime purchase, and e-commerce transactions where only the card details are required. Besides, Maharjan and Chudal [14] aided with an illustrative diagram depicting the credit card fraud contemporaries; with many others perturbing [4]. The persistency of these fraudulent types and sceneries against cardholders, merchant and financial institutions are trending on daily basis; and these had provoked forfending control measures of either reactive or proactive and other mitigation solution towards deterrent against their implications [4, 13, 16]. But, some pre-existing approaches bequeath by some scholar, fraud experts and financial institutions [17–19] towards easing its inferences causes more problems and tends to near perfection results oftentimes; due to advancement in Information Technology (IT), laxity in fraud detection system (FDS) and challenges of machine learning (ML) [16].

The ML challenges of which encompasses scarcity of real-world dataset for experimentation, imbalance class distribution that requires recodification using data augmentation techniques and other approach for balancing [20–22]. High dimensionality and sparsity in dataset is extra problem, amongst real-time detection, and complexities in the design of a genuine fraud detection models. All these limitations, makes research in this field extremely challenging and raise concerns as research gaps [23, 24].

However, Al-Smadi [13] in a study suggested a secured online payment system relaying on Secure Socket Layer (SSL) for connections through webpages focusing chiefly on the processing of information to defend against online fraudulent credit card transaction via harnessing some of the pre-existing methodologies 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. These, the financial institutions had already implemented to restrict the vagueness of fraudulent credit card transactions [25]. Besides, the institutions are also considering the replacement of the credit card being the most populous medium of payment for merchandise; exposed to fraudulent witticism with Smart cards. However, based on their assessments, it was discovered to be very expensive due to the existence and widespread of Point of Sales (POS) network, and the massive numbers of credit cards in circulation across the globe [13].

To this effect, fraudulent credit card transaction was premise to be forfended via rule-based method or anomalies search in transactions [7, 26]. That is achievable through Internet Protocol (IP) address which can point to a suspicious geolocation; as the device with a never-seen configuration of software and hardware can raise red flags to defense against fraudulent credit card transaction [27]. The rule-based approach subtends to historical datasets to define a set of rules and system that can raise alarm if a new transaction that matches one of the rules is committed [28]. However, this approach is laboriously a manual process; restricted to reactive measures which lack flexibility and consistency and as well time consuming [28]. Besides, it is open handed to fraudster for oust based on advancement in technology using identity theft, skimming, triangulation, merchant collusion, phishing and social engineering fraud tactics [13], in deceiving financial institution customers and bypassing the auspicious prevention and detection measures implements by the financial institutions. In refuting this, several alternative approaches like statistical methods, data mining, machine learning and deep learning methods have been offered [7, 17, 19]; with single and hybrid approaches [28]. But models engaged via those techniques suffers from some restrictions [25].

Therefore, this research seeks a deep learning based approach in alliances with ML models to classify credit card transaction. Some of these learning models approach were elusively deliberated [29–32]. As this study proposes a Deep Convolutional Neural Network (DCNN) method as potential solution towards the mitigation of the inferences of credit card fraud against financial institutions. A publicly available kaggle dataset is engaged [14]; in analyzing the credit card fraud problem where two experiments are executed. Foremost, on baseline line models in Subsection 4.1 using imbalance data class distribution. Secondly, on balance data distribution in Subsection 4.2; while delving Synthetic Minority Oversampling Technique (SMOTE) applied on the diverse ML and DL classifiers like Logistic Regression (LR), Random Forest (RF), Light Gradient Boosting Machine (LGBM), Multiple layer perceptron's (MLP), Artificial neural network (ANN) and the propose DCNN. This research is concerns on behavioral or online fraud. The major contribution in this research are as follows:

1. To propose an effective credit card fraud detection model using DCNN with Synthetic Minority Oversampling Techniques (SMOTE) to address the persistency of imbalance dataset distribution challenges in the publicly available dataset during experimentation.
2. To compare the performance of various ML and DL models imbibed with the propose DCNN towards the classification of credit card transaction. And establish models with superlative performance.

The rest of this paper is organized as follows: Section 2; presents reviews on related studies on credit card fraud. Section 3 discusses the materials and methods that incorporate the method for data collection, proposed methodology, preprocessing, hardware and software utilized for study analysis. Section 4, presents analysis and result findings of experiments along with comparison discussion about the model performances. Section 5, round up with conclusion discussion as recommendation is suggests on further research studies.

2. Related works

In this section, exploration is delved on recent related studies. To which predated proposed systems and techniques for credit card fraud detection in financial institution is presented [12, 13, 25, 33]. Besides, fraud prevention and detection mechanism with ethics is germane for consideration before delving to address any fraudulent scenarios affecting financial institutions.

Tanouz *et al.* [34] deploys ML models of DT, RF, LR, and NB to address the problem of credit card fraud; with focus on imbalance datasets. The research displayed that RF approach performed better, scoring 96.77%. LR, NB, and DT classifier had accuracy scores of 95.16%, 95.16% and 91.12% respectively. The details of the investigation depicted that RF is effective at credit card fraud detection, which is vital to financial security.

Ramani *et al.* [35] the research provides detail analogy about diverse supervised and unsupervised ML models for detecting fraudulent credit card activities. In this study, two ML models of CatBoost and LGBM are proposed. The performances of these models is compared with approaches of Auto Encoder (AE), LR, K-Means Clustering (KMC) and Neural Network (NN). It was established that CatBoost and LGBM presented high accuracy in fraud detection. Accuracy score, precision, and recall are the performance evaluation metrics exposed in this study that determine whether the given credit card transaction is fraudulent or legitimate. LGBM outperforms LR, NN. AE, KMC, and CatBoost as it offers 99% accuracy score. Meanwhile, the accuracy score of NN based techniques is 96%, while LR presented 77%, ae 96%, KMC 93%, CatBoost 98% and LGBM 99% respectively. It is established that both CatBoost and LGBM presented an outclass performances against other models. The limitation of this research is that it was not compared with other bench mark studies and dataset utilized is obtained from UCI ML repository different from kaggle dataset other scholars [16, 19, 25] and many other engages in their respective studies.

El Naby *et al.* [5] study engaged DL methods as an effective way to detect fraudulent credit card transactions. The researchers offer model for predicting Kaggle's credit card dataset. The proposed model is OSCNN (Over Sampling with Convolution Neural Network) which is based on oversampling preprocessing and Convolution Neural Network (CNN). The MLP was also applied to the dataset. Comparing the MLP-OSCNN results, it is proving that the proposed model achieved better results with 98.9% accuracy.

Akinola *et al.* [19] study focused on the use of only two ML model of LR and Isolation forest towards the detection of fraudulent credit card transactions, as kaggle dataset is imbibed in this study. In measuring the scholars model performances: accuracy score, precision, recall, F1-score and Area Under Curve-Receiver Operating Characteristic Curve (AUC-ROC) were used. The research experimental outcome is juxtaposed on training and testing datasets. The study accuracy score result for LR model yielded 99.91% for training data and 78% for testing data. While, the precision, recall and F1-score were 95%, 56% and 70% respectively. Moreover, the accuracy score for the isolation forest yielded 99.82% for training data and 74% for testing data. While, it precision, recall, and F1-score were 49%, 49% and 49% respectively. This finding established LR model as the best performance model against isolation forest model. The study limitation is ascribed to the accuracy score which suffers from overfitting challenges and biased in presentation. As the scholars fails to balance the kaggle dataset engaged before establishing cognizance findings.

Sahithi *et al.* [36] 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.

Khalid *et al.* [25] study engages ML models using proposed ensemble method to enhance credit card fraud detection. This ensemble models integrates SVM, K-Nearest Neighbor (KNN), RF, Bagging and AdaBoosting classifiers. The ensemble method is imbibed to suppressed the challenges of unbalance dataset distribution in credit card dataset by implementing under-sampling and synthetic oversampling techniques (SMOTE). Where comparative analysis studies are performed between the proposed ensemble models (PM1, PM2), traditional ML models and individual classifier to disclose the superior performance evaluation model that could mitigate the challenges ascribed with credit card fraud detection. The performance evaluation of accuracy score, precision, recall and f1-score is delved on the kaggle dataset employed for analysis in the study. The experimental outcomes depict the outclass performances of ensemble models of PM, PM1, PM2 superior against other traditional ML models during the several experiments. With outstanding computational efficiency between the training and testing time. When the proposed model is compared with bench mark studies the accuracy score of ensemble model (PM+SMOTE) is 99.96%, PM1 93.68%, PM2 94.74%. Precision of PM+SMOTE is 99. 96%, PM193.99%, PM2 94.92%. Recall PM+SMOTE is 99.96%, PM1 93.68%, PM2 94.74%. The F1-score of PM+SMOTE is 99.96%, PM1 93.67%, PM2 94.73%; these are in contention with bench mark studies. The limitation of the study is ascribed to the unavailability of real-life dataset to validate the model consistency over implementation; and the complexities in Google Colab model implementation environments over memory space allocation

Table 1. Normal non-fraudulent 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 2. Fraudulent Transaction 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

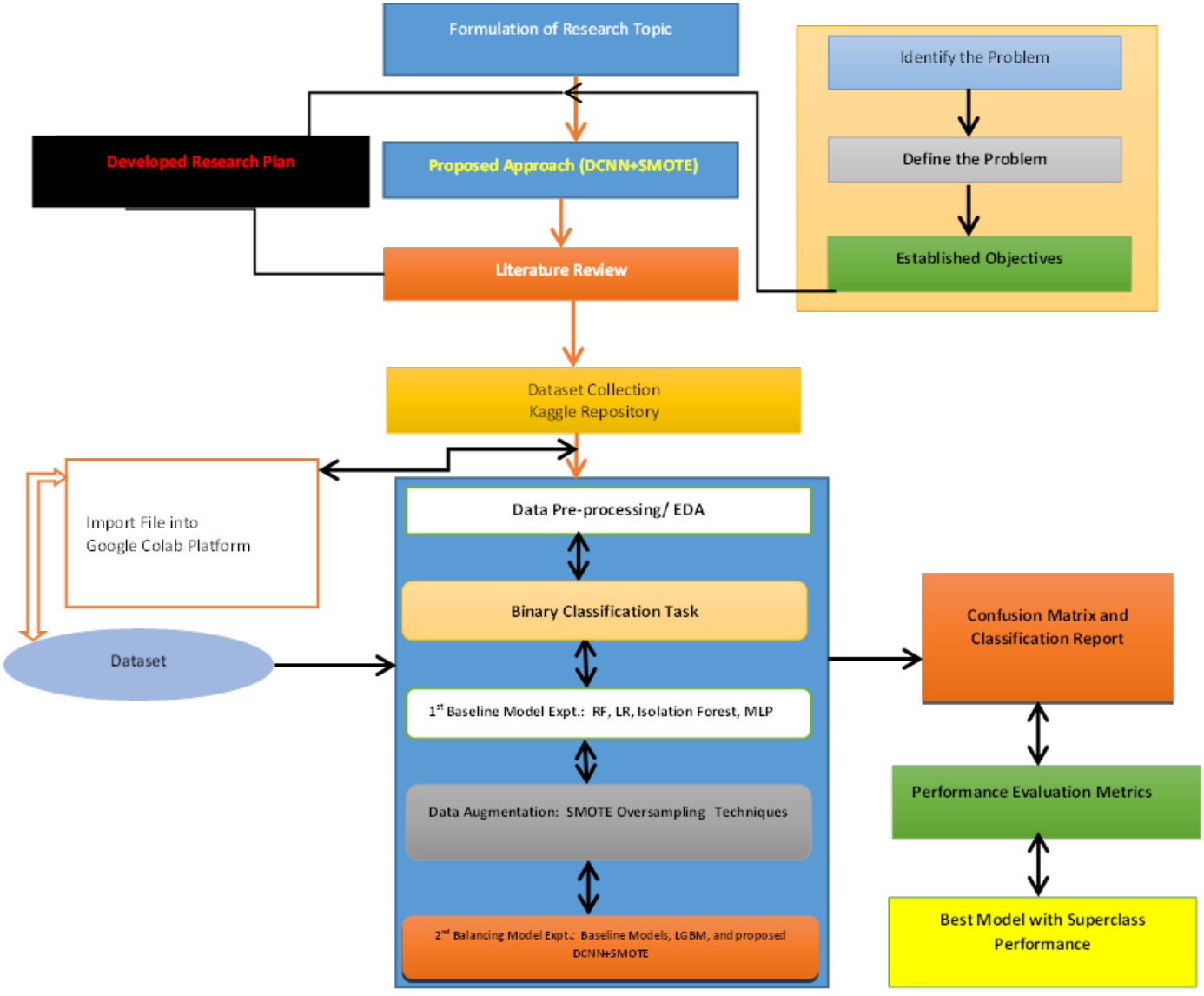

Figure 1. Proposed Methodology.

Table 3. The confusion matrix for the baseline models.

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

and internet difficulty time lapses during program code execution.

Maharjan and Chudal [14] carried out a comparative analysis on different learning techniques to analyze credit card fraud challenges using kaggle dataset. Where, four ML models of SVM, LR, NB and Decision Trees (DT) are used. However, ten performance metrics parameters were employed to establish the research result outcomes. These includes the accuracy, preci-

Table 4. Baseline model validation results.

Models	ACC	Error Rate	Recall	FPR	Specificity Or TNR	Precision	Prevalence	F1-Score	Null Error Rate	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

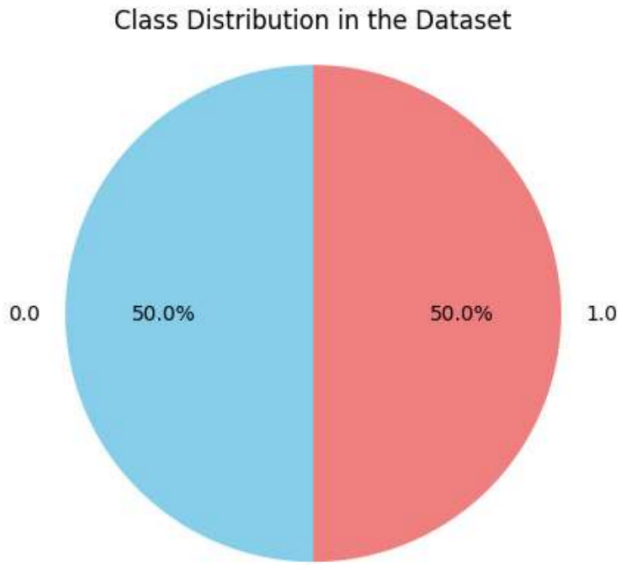

Figure 2. Balancing credit card dataset with SMOTE data augmentation techniques.

sion, true positive rate (TPR), false positive rate (FPR), recall, AUC-ROC, kappa statistics, speed of detection. SVM model exhibited the best accuracy score of 99.93% while other models presented above 95% which is pretty good. Therefore, SVM is established as the best performance models. The limitation of this study are in tandem with Akinola *et al.* [19] research.

Salaudeen *et al.* [16] predates the study trends, as it imbibes three DL models of ANN, MLP and conventional Convolutional Neural Network (CNN) with three other ML models of RF, LR, and proposed LGBM; in addressing unbalance class distribution challenges in credit card kaggle dataset hired. A comparative data analysis is carried out during the experimental stages on models imbibed. With eleven performance evaluation metrics to validates models with best performances against their contemporaries. It was established that the proposed LGBM outshine in seven categories of the metrics deployed. Having accuracy score of 96%, least error rate of 0.4%, recall 95%, prevalence 47%, cohen kappa 45%, f1-score 96% and Matthews Correlation Coefficient (MCC) of 93%. The reason for the LGBM excellent performance against other models lays with the few numbers of transaction dataset utilized. Otherwise, the DL models would have presented better outcome if big data were considered for the study.

From the literature survey on related studies, it is deduced that most researchers suggested addressing the challenges of

Table 5. Confusion matrix for balancing models.

	TN	FP	FN	TP
LR	40	3	4	38
RF	42	1	4	38
Isolation Forest	43	0	42	0
MLP	42	1	3	39
LGBM	42	1	2	40
ANN	43	0	10	32
DCNN+SMOTE	995	0	1	1

imbalance class distribution, with high dimensionality and sparsity and many others challenges in the kaggle dataset utilized in their respective studies. Besides LinkedIn [20], Gao [21], Mazumbder [22] and Prasad *et al.* [37] presented an approaches of data augmentation techniques that may assist in curtailing the imbalance class distribution problem in diverse research fields if applied appropriately. This research study, is an improvement over Salaudeen *et al.* [16], Akinola *et al.* [19] and Khalid *et al.* [25]studies. As the propose DCNN validation results in subsection 4.2 is compared with the benchmark studies to exercise it dominancy in performance toward taming fraudulent credit card transactions, when absorbed and implemented by the financial institution.

3. Material and methods

This section describes the procedural approach employ in this study.

3.1. Data collection

The dataset used in this study is obtained from Kaggle repository, via the link https://www.kaggle.com/mlg-ulb/creditcardfraud [14, 16]. This dataset is created by European bank in September 2013 and publicly available in CSV format. Encompassing 284807 records, grouped into (non-fraudulent) and (fraudulent) classes. Table 1 and 2 presented it summary via the python command constructs: normal df.Amount.describe(); that displays non-fraudulent transaction and fraud_df.Amount.describe (); to display the fraudulent transaction. Where the number of transactions for fraudulent class is 492 at 0.2% and 284,315 for non-fraudulent class at 99.8% respectively. However, the dataset has 31 numerical features presented in V1-V28 in Principal Component Analysis (PCA) form [14]. Among the feature is 'Amount' in transaction and other feature that can used for instance-dependent that is cost-sensitive to learning from the credit card. The feature such

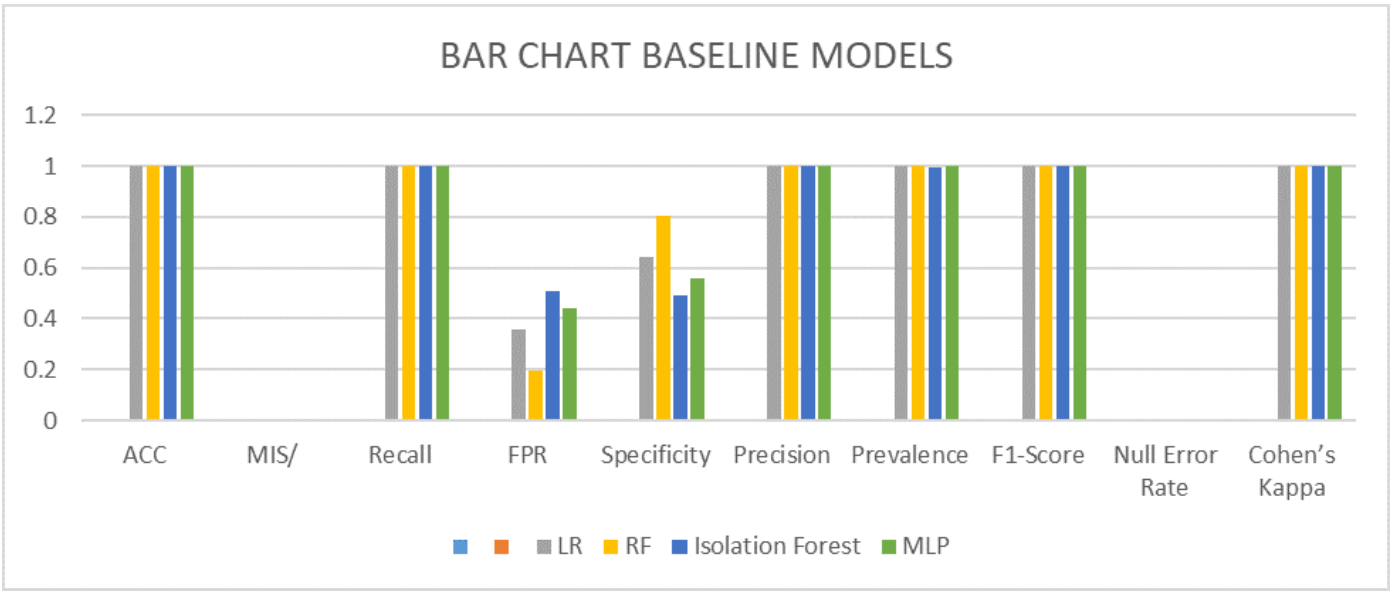

Figure 3. Bar chart for baseline model validation.

as 'Time' contains the seconds elapsed between each transaction and the first transaction in the dataset. The feature, 'Class' is the response variable and it takes value 1 in case of fraud and 0 non-fraud. These is achieved under the pre-processing procedure. Its discovered that the dataset is highly imbalanced. Therefore, binary classification is recommended for treating the dataset [19, 25].

3.2. Research methodology

At Pre-processing/ Exploratory Data Analysis (EDA) state, data preparation, analysis and model building were carried out.; which Figure 1 depicts for clarity. The dataset imbibed is house in the open- source kaggle repository described in Subsection 3.1 above, after which it was splits into training and testing set for validation. Series of ML and DL models were applied for comparative analysis studies. While, Python programing language (PPL) libraries and command constructs utilized deliberated [19]. The EDA procedure is entrenching following the steps below:

1. Data Cleaning: where missing values and outliers are handles.
2. Encoding the categorical data: the task of converting to numerical variables
3. Feature Scaling: feature standardization is exhibited. Here, comparison is done between values of Table 1 and 2, for class distribution classification.
4. Feature correlation and selection: This is done at the stage to generate the scatter and density plot likewise generate the negative correlation matrix [16].
5. Splitting of the dataset into training (80) and testing sets (20) with validations (50:50)
6. Application of selected models (e.g. LR, RF, iforest, MLP, and others) for performance evaluation and comparison of the models to determine the one with outclass performance.
7. Data Resampling Methods: Oversampling Techniques of SMOTE is explored later to balance the irregularity in imbalance dataset distribution as the study addresses the overfitting and under-fitting challenges presented when baseline model experiment is performed [16, 25, 38].
8. Finally, establishes the best performance model suitable for regulating the fraudulent credit card transactions.

3.3. Baseline methods employed for this study

Machine learning just like statistical learning denotes "a set of tools for modeling and understanding complex datasets". The ML is a subset of Artificial Intelligence (AI) while the deep learning is well rooted beneath ML [16]. These, Jovel *et al.* [30] and Adeleke [39] elusively described in their studies. Brownlee [31] clarified on ranges of their learning method majorly classified into three forms of supervised, unsupervised, semi-supervised or Reinforcement learning algorithm with many others. In this study, both ML and DL of LR, RF, iforest, MLP, ANN, LightGBM and the proposed Deep Convolutional Neural Network (DCNN) were absorbed and ably deliberated beneath.

3.3.1. Logistics Regression (LR)

Logistic regression is a statistical and ML technique; that can be used for both regression and binary classification problems towards credit card fraud detection [40]. It can as well be used to predict definite variables by means of dependent variables. However, Fayommi *et al.* [8] in their literature survey provided clarification about the LR concept.

3.3.2. Random Forest (RF)

The RF algorithm is one of the most prevalent ensembles ML learning model, which has proven effective in various categorization tasks, with application on credit card fraud detection [31, 37, 40]. Fayyomi *et al.* [8] study presented an elusive

Table 6. Balancing model validation result.

Models	ACC (%)	Error Rate (%)	Recall (%)	FPR (%)	TNR (%)	Prec. (%)	Prevalence (%)	NER	Cohen Kappa (%)	F1-score (%)	MCC (%)
LR	0.92	0.08	0.93	0.09	0.91	0.90	0.45	0.52	0.4	0.92	0.84
RF	0.94	0.06	0.97	0.09	0.91	0.90	0.45	0.54	0.4	0.93	0.88
Isolation Forest	0.51	0.49	0.00	0.5	0.51	0.00	0.00	1.00	-0.5	0.00	0.00
MLP	0.95	0.05	0.98	0.07	0.93	0.93	0.46	0.53	0.42	0.95	0.91
LGBM	0.96	0.04	0.98	0.05	0.95	0.95	0.47	0.52	0.44	0.96	0.66
ANN	0.88	0.12	1.00	0.19	0.81	0.76	0.38	0.62	0.26	0.86	0.79
Proposed DCNN+SMOTE	1.00	0.00	1.00	0.001	1.00	0.50	0.001	1.00	0.00	0.67	0.00

Table 7. Epoch distribution for model accuracy training and validation results of the proposed DCNN+SMOTE.

Epoch	0	2	4	6	8
Prediction Model Accuracy Training	0.999	1.000	1.000	1.000	1.000
Prediction Model Accuracy Validation	0.995	0.999	0.999	0.999	0.999

Table 8. Epoch distribution for model loss training and validation results of the proposed DCNN+SMOTE.

Epoch	0	2	4	6	8
Prediction Model Loss Training	0.05	0.007	0.005	0.003	0.003
Prediction Model Loss Validation	0.02	0.027	0.029	0.035	0.034

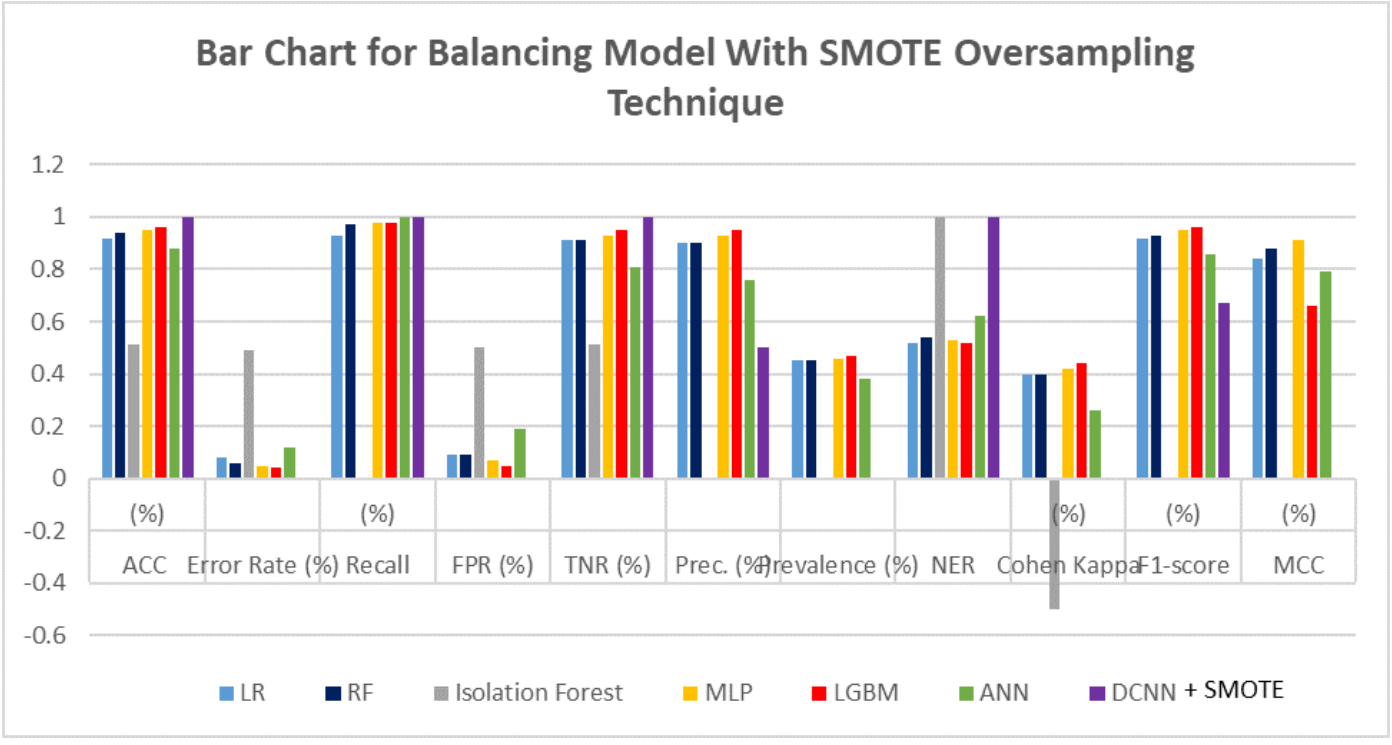

Figure 4. Bar chart for balance model using SMOTE oversampling techniques.

description of RF model with the aid of illustration diagram depicting its general working structure.

3.3.3. *Isolation Forest (iforest)*

This is otherwise known as iForest; the model is often used in anomalous classification and detection problem. Isolation means 'separating an occurrence from the rest of the occurrences'. Since anomalies are 'few and different', thus they are more susceptible to isolation. It builds an ensemble of iTrees for a given data set, then anomalies are those instances which have short average path lengths on the iTrees. There are only two variables in this method; the number of trees to build and

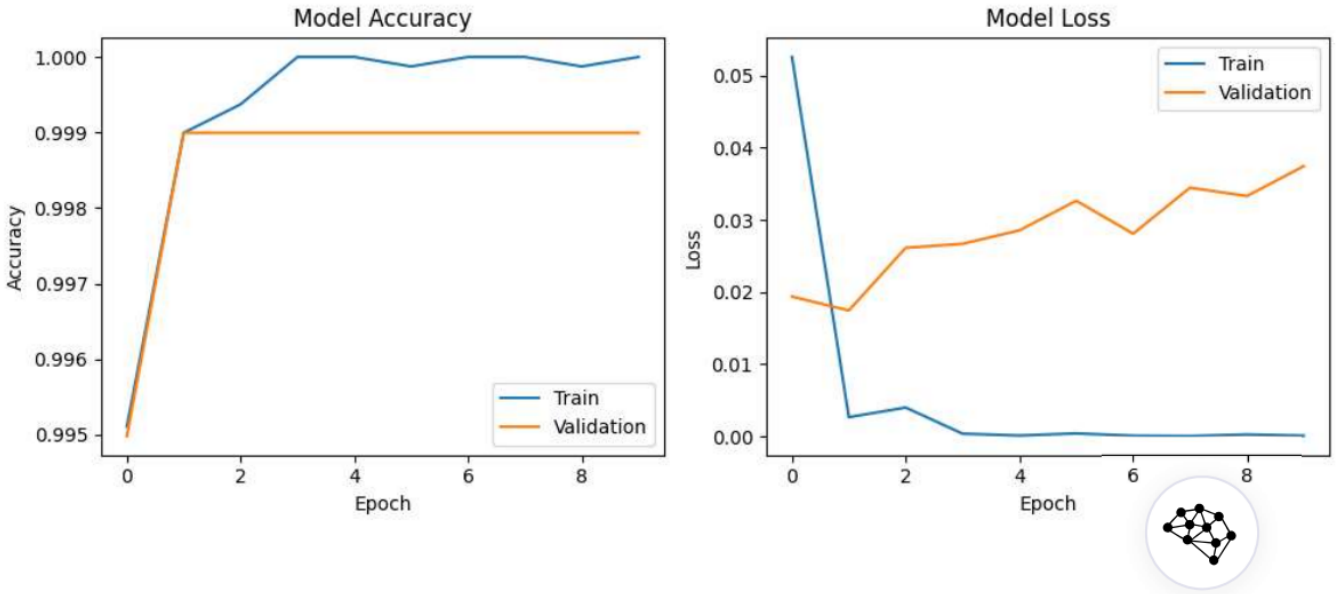

Figure 5. Plot for model accuracy and model loss of the proposed DCNN+SMOTE.

the sub-sampling size. It was display in the study of Vaishnavi Nath Dornadula [41] that 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.

3.3.4. Multiple Layer Perceptron's (MLP)

The simplest and most common type of feed- forward deep neural network. It consists of multiple layers of neurons each fully connected to each other. It made up of three components of input, hidden layer and output layer and its often used for binary classification. This are controlled via the objective function, activation with optimization function and the threshold [42].

3.3.5. Artificial Neural Network (ANN)

It is a very common method that simulate the apparatus of learning in biological organisms [43]. The grand vision of neural networks is to create artificial intelligence by building machines whose architecture simulates the computations in the human nervous system. This is obviously not a simple task because the computational power of the fastest computer today is a minuscule fraction of the computational power of a human brain [43].

3.3.6. Light Gradient Boosting (LGBM)

It is an advanced gradient boosting architecture signifying excellent credit card fraud detection performance [40]. LightGBM can be utilized in credit card fraud detection to examine transaction data, about attributes like transaction time, location, amount, and historical data [16]. The model constructs a collection of DT to advance their configuration to detect fraudulent transactions accurately.

3.4. Proposed Deep Convolutional Neural Network (DCNN) based Synthetic Minority Oversampling Techniques (SMOTE)

The DCNN is a popular deep learning model. Its purpose is to process diverse dimensions of dataset such as image, text and audio [43]. DCNN has recently become a focus for many scholars [42, 43] in studying image classification and credit card fraud detection task, due to its efficiency on learning more meaningful and useful representations that yielded optimal results, outperforming other traditional ML algorithm. Using this model in the analysis of credit card detection in financial institution is worth investigating further. However, just similar to other machine learning and deep learning methods, the conventional DCNN also suffers from imbalance class distribution, high dimensionality, and sparsity problem. From Table 1 and 2 above, it is wright established that the dataset engaged is unbalanced [16, 17, 38]. However, a model is required to address challenges of over-fitting and under-fitting [25]. These necessitated the need for improvement. In this research, the effectiveness of DCNN is combined with SMOTE to uncover more insights on credit card fraud detection. The resampling techniques of the SMOTE techniques classifies dataset into equal balance distribution of non-fraudulent and the fraudulent transitions considered as the best fit. The SMOTE techniques tried to replicate the form of the class having less number of values and tries to remove the problem of the oversampling and when the sample is picked then the number probability for the two classes to be picked will be the same [44]. LinkedIn [20] and Noviandy [38] present comprehensive studies on the application of data augmentation technique in addressing the binary classification problem inbound in credit card fraud dataset. When this is applied appropriately, Figure 2 is achieved.

3.5. Experimental environment

This research has been implemented on a personal laptop with Intel i7-5600U CPU, 2.6GHz speed, 16 GB RAM, and an SSD hard disk. The memory consumption rate is 25%, at most, and hard disk utilized is almost 0%. Thus, the laptop is adequate for this study [16]. In this study, Scikit learn package is used for ML classification while Tensorflow is deployed for the DL. The PPL utilized in this study engaged pre-processing library like Numpy, Pandas, Scikit-Learn, Matplotlib, Seaborn and many others; that were ably described in Akinola *et al.* [19]. Besides, Google Colab integrated with Jupyter notebook and Google drive cloud infrastructure platforms were the utilized environments software; and these were extensively described in Saluadeen *et al.* [16] and Sharma *et al.* [45].

3.6. Evaluation and performance metrics

A Confusion Matrix Table (CMT) is a table that is often use to described the performance of classification model (or "classifier") on a set of data for which the true values are known [16, 39]. It as well permits the visualization of the performance of an algorithm or models [16, 46]. The CMT reviews each tuples traits of (TN, FP, FN, TP) and performance evaluation of any models employ during experimentation either on binary classification problem task or Multi-class.

- True negative (TN)/m- is the number of correct predictions that an instance is negative. Here, we predicted "No", and they are not fraudulent
- False positive (FP)/o- is the number of incorrect predictions that an instance is positive. Here, predicted "Yes", but they are not actually fraudulent (TYPE 1 ERROR)
- False negative (FN)/l- are the number of incorrect of predictions that an instance negative. We predicted "No" but they are actually fraudulent (TYPE 11 ERROR)
- True positive (TP)/e- are the number of correct predictions that an instance is positive (i.e. fraudulent).

1. Accuracy: The accuracy (ACC) is the proportion of the total number of predictions that were correctly classified. In same vein, it is the overall, how often is the classifier correct? It is determine using the syntax:

$$ACC = \frac{(TP + TN)}{TP + TN + FP + FN}. \quad (1)$$

2. Misclassification/ error rate: This is the overall of how often the classifier is wrong.

$$MIST = \frac{(FP + FN)}{TP + TN + FP + FN}. \quad (2)$$

This is also equivalent to 1 Minus Accuracy (i.e. MIST = 1- ACC). And it is otherwise known as "Error rate".

3. Recall/ true positive rate/ sensitivity: When it's actually "Yes", how often does it predict yes?

$$\text{REC} = \frac{\text{TP}}{(\text{TP+FN})}. \quad (3)$$

4. False positive rate: When it's actually "No", how often does it predict yes?

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

5. True negative rate/ specificity: When it is actually no, how often does it predict no?

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

This is also known as Specificity. Equivalent to 1 minus false positive rate (i.e. 1- FPR).

6. Precision: When it predicts yes, how often is it correct?

$$\text{PREC.} = \frac{TP}{(TP + FP)}. \quad (6)$$

7. Prevalence: How often does the yes condition actually occur in our sample?

$$\text{PREV.} = \frac{\text{Actual Fraud (Yes or Positive)}}{\text{Total no. of actual and predicted classifiers}}. \quad (7)$$

8. Null error rate: This is how often you would be wrong if you always predicted the majority class.

$$\text{NER} = \frac{\text{TN + FP}}{\text{TP + TN + FN + FP}}. \quad (8)$$

9. F1 Score: This is a weighted average of the true positive rate (Recall) and precision.

$$\text{F1-Score} = \frac{2 \times (\text{Precision} \times \text{Recall})}{(\text{Precision+Recall})} \times 100. \quad (9)$$

10. Matthews Correlation Coefficient.

$$MCC = \frac{(TP \times TN) - (FP \times FN)}{\sqrt{(TP+FP) \times (TP+FN) \times (TN+FP) \times (TN+FN)}}. \quad (10)$$

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

4. Results and discussion

This section presents results analysis for the two successive experiments conducted in this study.

4.1. Results and discussion on the baseline models

Table 3 below presented the confusion matrix values bred during the baseline experiments where three ML Models of LR, RF and Isolation forest and single DL model of MLP are delved on imbalance dataset. Matthews correlation Coefficient (MCC) introduced by Comotto [47] as part of evaluation metrics in their study is not engaged during this result presentation of the baseline models due to lack of suitability performance to imbalance class distribution. Table 4 offered the baseline validation results in tandem with Figure 3 displaying the bar chart for visualization of the baseline model validation results respectively.

From the Table 4 analysis report; its deduced that the accuracy score, recall with precision rate and F1-score of all the baseline models are abounds with (1.00%) classifier as superclass outcomes respectively. This makes it difficult to establishes the best outperforming models amidst them based on

those metrics results. Another metrics considered were, the Null error rate (NER) of (0.002%), Prevalence and Cohen's Kappa (0.998%) that also presented a uniformly synonymous results distinctly.

This constraint the baseline experiment finding establishment to FPR and TNR evaluation metrics that is also an unfitting yardstick for presenting results on binary classification problem. Here, RF was discovered to generate the least FPR result of (0.194%), followed by LR (0.357%), MLP (0.442%) and isolation forest of (0.510%). Under the specificity, RF exhibited the highest results of (0.806%), followed by LR (0.643%), MLP (0.560%) and isolation forest that presented the least close range specificity results of (0.490%). Based on this finding, its glaring that the RF is the best baseline model displaying surpassing result of performances. Since the dataset for this experiment is highly skewed, its recommended to delved the models with balance dataset to established cogent and more alluring results; that can assist financial institution in regulating the menace of credit card fraud.

4.2. Results and discussion on DCNN based SMOTE oversampling method

This section, provides classification report for the confusion matrix values generated and displayed in Table 5 during the balancing model experiments. Table 6 presented the validation results of the balancing models. While, Figure 4 presented the bar chart for visualization of the balancing model results in comparison with other models, after the application of data augmentation techniques of SMOTE Oversampling method.

Based on the value of accuracy achieved, the proposed DCNN+SMOTE presented a remarkable performance of 1.00% accuracy result (Figure 4) against the other models of LGBM (0.96%), MLP (0.95%), RF (0.94%), LR (0.92%), ANN (0.88%) and Isolation Forest that displayed the worst accuracy performance of (0.51%) respectively. Table 7 and 8 which is derived from Figure 5 describes the model accuracy training with validation result and Model loss training with validation results for the proposed DCNN+SMOTE respectively.

In term of Error Rate/Misclassification, the proposed DCNN+SMOTE model displayed the least misclassification record of (0.00%), while Isolation forest presented the worst misclassification or error rate of (0.49%), these the other models ensues in the preceding orders ANN (0.12%), LR (0.08%), RF (0.06%), MLP (0.05%), and LGBM (0.04%) respectively. In another development, the proposed DCCN+SMOTE and ANN in terms of Recall/ Sensitivity presented a remarkable performance of (1.00%) recall; which was followed by both LGBM and MLP with recall rate of (0.98%) distinctly. A closer result of (0.97%) was displayed by RF as the third on the roll and LR (0.93%) to be the fourth; while isolation forest remains the worst with (0.00%) of sensitivity result. To further show performance of the proposed DCNN+SMOTE in terms of False Positive Rate (FPR), the proposed DCNN+SMOTE model presented the least false positive rate of (0.001%), followed by LGBM (0.05%), MLP (0.07%), with both LR and RF presented (0.09%) results to be the fourth on the troll, isolation forest is the fifth with (0.5%), and ANN was visible with (0.19%) record of FPR classification to be the one with the worst False positive rate.

In another remarkable performance in terms of specificity/True Negative Rate (TNR), the proposed DCNN+SMOTE presented the superclass performance of specificity results of (1.00%), followed by LGBM (0.95%), MLP (0.93%), both LR and RF displayed (0.91%) result each, ANN (0.81%) and isolation forest with the least result of (0.51%) respectively. This also reflect remarkable performance in term of precision where, LGBM was discovered to displayed superclass performance of (0.95%) against the rest of the models. MLP presented close range results of (0.93%). Both LR and RF offers (0.90%) each, ANN (0.76%), the proposed DCNN+SMOTE (0.50%) and Isolation forest (0.00%) offering the worst precision result. This can also be seen in the results achieved based on prevalence where DCNN+SMOTE presented the second worst prevalence result of (0.001%), isolation forest (0.00%), ANN (0.38%) both LR and RF (0.45%) each, MLP (0.46%) and LGBM (0.47%). In terms of the Null Error Rate (NER), it can be seen that the DCNN+SMOTE and Isolation forest gave the highest impression of (1.00%) each as wrong classifier of predicting majority class. Followed by ANN (0.62%), RF (0.54%), MLP (0.53%) and both LR and LGBM (0.52%) each respectively while in term of Cohen's Kappa, the LGBM presented a superclass performance of (0.44%), MLP (0.42%), ANN (0.26%), both LR and RF (0.4%) each, the proposed DCNN+SMOTE (0.00%) and worst impression result displayed by isolation forest in an out of range presenting (-0.5%) result.

Further remarkable performance can be seen when the F1-scores is used in the measurement where the LGBM presented an outclass performance with (0.96%), closely followed by MLP (0.95%), RF (0.93%), LR (0.92%), ANN (0.86%), the proposed DCNN (0.67%), and Isolation forest (0.00%) respectively. Finally, the Matthews Correlation Coefficient (MCC) was used to measure performance of the proposed DCNN+SMOTE technique along the baseline approaches. It can be concluded that, MLP displayed a superclass perfect positive prediction performance of (0.91%), followed by strong positive result of RF (0.88%), LR (0.84%), ANN (0.79%), LGBM (0.66%) while the proposed DCNN+SMOTE and Isolation Forest presented a no better than random prediction for the MCC. In can be concluded that, the reason for the performance of the proposed DCNN+SMOTE is based on the incorporation of the SMOTE that enable it to addressed challenges of over-fitting and under-fitting.

5. Conclusion and recommendation

In conclusion, the analysis and classification of fraudulent credit card transactions were performed in this study using a dataset publicly available on Kaggle; both machine learning and deep learning models such as LR, RF, Isolation Forest (iForest), MLP, ANN, and the proposed DCNN+SMOTE were utilized respectively. A baseline model experiment was first performed, probing three ML models (LR, RF, iForest) and a single DL model (MLP). The application of an inappropriate

performance evaluation metric like accuracy to establish findings on imbalanced class distribution at this phase is absurd, as it suffers from overfitting and underfitting and leads to poor generalization of the outcomes. The classifier tends to predict only the majority class (i.e., the negative and non-fraudulent class). The second experiment was then performed after which a data augmentation method engaging SMOTE oversampling techniques was imbued. The research results for the best performance model are justified based on the seven performance evaluation metrics of Accuracy, Misclassification or Error Rate, Recall, FPR, TNR, and NER out of a total of eleven deployed. The proposed DCNN+SMOTE overwhelmingly displayed superclass performance across the board evaluation, showing 1.00% results for accuracy, recall, TNR, and F1-score and 0.001% distinct results for both FPR and Prevalence respectively. This contrasts with what other models like LR, RF, Isolation Forest, MLP, ANN, and LGBM presented. This research serves as an improvement over the work of Salaudeen *et al.* [16], Akinola *et al.* [19], Khalid *et al.* [25], Nalayini *et al.* [48] and Shang *et al.* [49] work with the best results. The results of all our oversampling models are good enough to compete with benchmark studies in the field of credit card fraud detection

Finally, it is suggested that financial institutions should embrace the application of proactive and improved countermeasures for the protection of their customers against fraudulent credit card transactions; because fraudsters keep developing diverse techniques to outsmart or break security measures set in place by financial institutions. In future work, an enhanced hybrid deep learning method is suggested to have a more lucid approach toward credit card fraud detection. Subsequent work in this field should try exploiting the use of the MCC evaluation metric in binary classification tasks, because it enhances the performance of the model and is good for imbalanced datasets based on characteristics efficiency.

References

[1] T. P. Bhatla, V. Prabhu, & A. Dua, "Understanding credit card frauds", Cards business review **1** (2003) 1. https://popcenter.asu.edu/sites/default/files/problems/credit_card_fraud/PDFs/Bhatla.pdf.

[2] Guide to understanding the total impact of fraud, by International Public Sector Fraud Forum (IPSFF) Cabinet Office and Commonwealth Fraud Prevention Centre. (2020, february). https://assets.publishing.service.gov.uk/media/5e4bedb986650c10e5a91d89/2377_The_Impact_of_Fraud_AW_4_pdf.

[3] E. Btoush, X. Zhou, R. Gururaian, K. C. Chan and X. Tao, *A Survey on credit card fraud detection technique in banking industry for cyber security*, 8th International Conference on Behavioral and Social Computing (BESC), Doha, Qatar, 2021, pp. 29–31. https://ieeexplore.ieee.org/abstract/document/9635559.

[4] J. P. Morgan, "2022 AFP payments fraud and control report", (2022) pp. 1–69. https://www.jpmorgan.com/content/dam/jpm/commercial-banking/insights/cybersecurity/highlights-afp-2022-payments-fraud-and-control-report.pdf

[5] A. A. El Naby, E. E. Hemdan & A. El-Sayed, *Deep learning approach for credit card fraud detection*, 2nd IEEE International Conference on Electronic Engineering (ICEEM), Menoufia University, Egypt, 2021. https://www.researchgate.net/publication/354112779_Deep_Learning_Approach_for_Credit_Card_Fraud_Detection.

[6] A. M. Nancy, G. S. Kumar, S. Veena, N. A. Vinoth, & M. Bandyopadhyay, "Fraud detection in credit card transaction using hybrid model". AIP Conference Proceedings, AIP Publishing LLC **2277** 2020 130010. https://pubs.aip.org/aip/acp/article/2277/1/130010/1026833/Fraud-detection-in-credit-card-transaction-using.

[7] A. Shah, and Y. J. Makwana, "Credit card fraud detection", ResearchGate 2023. https://www.researchgate.net/publication/369857378_Credit_Card_Fraud_Detection#fullTextFileContent.

[8] A. M. Fayyomi, D. Eleyan, A. Eleyan, "A survey paper on credit card fraud detection techniques" International Journal of Scientific & Technology Research (IJSTR) **10** (2021) pp. 72–179. https://www.ijstr.org/final-print/sep2021/A-Survey-Paper-On-Credit-Card-Fraud-Detection-Techniques.pdf.

[9] The World Bank, "Credit card ownership (%age 15+)", World Bank Gender Data Portal (2023). https://genderdata.worldbank.org/indicators/fin7-t-a/.

[10] K. J. Barker, J. D'amato, & P. Sheridon, "Credit card fraud: awareness and prevention", Journal of financial crime **15** (2008) 398. https://www.emerald.com/insight/content/doi/10.1108/13590790810907236/full/html.

[11] Here's how credit card fraud happens and tips to protect yourself, by A. White. (2023, June 6). https://www.cnbc.com/select/credit-card-fraud/.

[12] K. Ayorinde, *A methodology for detecting credit card fraud*, M.S. thesis, Minnesota State University, Mankato, 2021. https://cornerstone.lib.mnsu.edu/etds/1168.

[13] B. Al-Smadi, *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.

[14] A. Maharjan, and P. Chudal, *Comparative analysis of algorithms for credit card fraud detection*, Proceedings of the KEC Conference, Kantipur Engineering College, Dhapakhel Lalitpur, 2019, pp. 199–204. https://kec.edu.np/wp-content/uploads/2020/01/Paper_36.pdf.

[15] S. Dhameja, K. Jacob & D. P Richard, "Clarifying liability for twenty-first-century payment fraud", Economic Perspectives, **37** (2013) 107. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2386037.

[16] L. G. Salaudeen, D. Gabi, G. Muhammad & H. U. Suru, "Light gradient boosting machine (lgbm) for credit card fraud detection in financial institution", Direct Res. J. Eng. Inform. Tech. **12** (2024) 19. https://www.researchgate.net/publication/379939944_Light_Gradient_Boosting_Machine_LGBM_for_Credit_Card_Fraud_Detection_in_Financial_Institution.

[17] K. Chaudhary, J. Yadav & B. Mallick, "A review of fraud detection techniques: credit card", International Journal of Computer Applications **45** (2012) 39. https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=c77f3459fbbc036def7e77962958d64d4ada7291.

[18] A. S. Alraddadi, "A survey and a credit card fraud detection and prevention model using the decision tree algorithm", Engineering, Technology & Applied Science Research **13** (2023) 11505. https://www.etasr.com/index.php/ETASR/article/view/6128.

[19] K. E. Akinola, D. A. Aina, O. Oyedele, and J. A. Braimoah, "Credit card fraud detection using logistics regression and isolation forest algorithm", UNIZIK Journal of Engineering and Applied Sciences **2** (2023) 187. https://journals.unizik.edu.ng/ujeas/article/view/2203.

[20] LinkedIn, "How you can address class imbalance in binary classification task? "(2023, November 6). https://www.linkedin.com/advice/3/how-can-you-address-class-imbalance-binary-classification.

[21] J. Gao, *Data argumentation in solving data imbalance problems*, Degree Project, Department of Computer Science and Engineering, Second Cycle, 30, credits Stockholm, Sweden, 2020. https://www.diva-portal.org/smash/get/diva2:1521110/FULLTEXT01.pdf.

[22] 5 techniques to handle imbalanced data for a classification problem by S. Mazumder. (2021, June 21). https://www.analyticsvidhya.com/blog/2021/06/5-techniques-to-handle-imbalanced-data-for-a-classification-problem/.

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

[24] Credit card detection by Great Learning Team (GLT). (2023). https://www.mygreatlearning.com/blog/credit-card-fraud-detection.

[25] A. R. Khalid, N. Owoh, O. Uthmani, M. Ashawa, J. Osamor, and J. Adejoh, "Enhancing credit card fraud detection: an ensemble machine learning approach", Big Data Cogn. Comput. **8** (2024) 6. https://www.mdpi.com/2504-2289/8/1/6.

[26] Anomaly detection in credit card fraud, by S. Sarwade. (2023, May 12). Analytic vidhya. https://www.analyticsvidhya.com/blog/2023/05/anomaly-detection-in-credit-card-fraud/.

[27] Credit card fraud detection: The Guide, by B. Jendruszak. (2023, July 14). https://seon.io/resources/credit-card-fraud-detection.

[28] E. F. Malik, K. W. Khaw, B. Belaton, W. P. Wong & X. Chew, "Credit card fraud detection using a new hybrid machine learning architecture", Mathematics **10** (2022) 1480. https://doi.org/10.3390/math10091480.

[29] A. Mosavi, S. Ardabili, & A. R. Várkonyi-Kóczy, "List of deep learning models", Inter-academia 2019 lnns **101** (2020) 202. https://doi.org/10.1007/978-3-030-36841-8_20.

[30] J. Jovel, and R. Greiner, "An introduction to machine learning approach for biomedical research", Front Med (Lausanne) **8** (2021) 771607. https://pubmed.ncbi.nlm.nih.gov/34977072/.

[31] 14 different types of learning in machine learning, by J. Brownlee. Blog, (2019, November 11). https://machinelearningmastery.com/types-of-learning-in-machine-learning.

[32] V. V. Shakirov, K. P. Solovyeva, & W. L. Dunin-Barkowski, "Review of state-of-the-art in deep learning artificial intelligence", Optical memory and neural networks **27** (2018) 65. https://link.springer.com/article/10.3103/S1060992X18020066.

[33] J. Yashvi, T. Namrata, D. Shripriya & J. Sarika, "A comparative analysis of various credit card fraud detection techniques", International Journal of Recent Technology and Engineering **7** (2019) 402. https://www.researchgate.net/publication/332264296_A_comparative_analysis_of_various_credit_card_fraud_detection_techniques.

[34] D. Tanouz, R. R. Subramanian, D. Eswar, G. V. P. Reddy, A. R. Kumar, and C. H. V. N. M. Praneeth, *Credit card fraud detection using machine learning*, In Proceedings of the 5th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2021, pp. 967–972. https://www.researchgate.net/publication/369199151_Credit_Card_Fraud_Detection_Using_Enhanced_Random_Forest_Classifier_for_Imbalanced_Data.

[35] K. Ramani, I. Sunetha, N. Pushpalatha & P. Harsih, "Gradient boosting techniques for credit card fraud detection", Journal of Algebraic Statistics **13** (2022) 553. https://publishoa.com/index.php/journal/article/view/660.

[36] G. L. Sahithi, V. Roshmi, Y. V. Sameera and G. Pradeepini, *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, 2022, pp. 1237–1241. https://ieeexplore.ieee.org/abstract/document/9776955/.

[37] P. Y. Prasad, A. S. Chowdary, C. Bavitha, E. Mounisha & C. Reethika, *A comparison study of fraud detection in usage of credit cards using machine learning*, In Proceedings of the 7^{th} International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, 2023, pp. 1204–1209. https://ieeexplore.ieee.org/abstract/document/10125838.

[38] R. T. Noviandy, G. M. Idroes, A. Maulana, I. Hardi, E. S Ringga & R. Idroes, "Credit card fraud detection for contemporary financial management using xgboost-driven machine learning and data augmentation techniques", Indatu Journal of Management and Accounting **1** (2023) 1. https://www.researchgate.net/publication/374087884_Credit_Card_Fraud_Detection_for_Contemporary_Financial_Management_Using_XGBoost-Driven_Machine_Learning_and_Data_Augmentation_Techniques.

[39] A. J. Adeleke, *Development of an automated real-time credit card fraud detection system*, B. Sc. Project, Department of Computer Science and Mathematics, College of Basic and Applied Sciences, Mountain Top University, Ibafo Ogun State, Nigeria, 2022.

[40] A. Aslam & A. Hussain, *A performance analysis of machine learning techniques for credit card fraud detection*, Journal on Artificial Intelligence **6** (2024) 1. https://doi.org/10.32604/jai.2024.047226.

[41] V. N. Vaishnavi Nath Dornadula & S. Geetha, "Credit card fraud detection using machine learning algorithms" procedia computer science **165** (2019) 631. https://doi.org/10.1016/j.procs.2020.01.057.

[42] A. Zhang, Z. C. Lipton, M. Li & A. J. Smola, "Dive into deep learning", arXiv preprint arXiv:2106.11342 (2022). https://doi.org/10.48550/arXiv.2106.11342.

[43] A. Agarwal, M. Iqbal, B. Mitra, V. Kumar & N. Lal, "Hybrid CNN-BILSTM-attention based identification and prevention system for banking transactions", Nat. Volatiles & Essent. Oils **8** (2021) pp. 2552–2560. https://www.nveo.org/index.php/journal/article/view/809.

[44] K. Fu, D. Cheng, C. Dawei & L. Zhang, *Credit card fraud detection using CNN*, International Conference on Neural Information Processing, 2016, pp. 483-490. https://link.springer.com/chapter/10.1007/978-3-319-46675-0_53.

[45] A comprehensive guide to google colab: features, usage, and best practices, by A. Sharma. (2020). https://www.analyticsvidhya.com/blog/2020/03/google-colab-machine-learning-deep-learning.

[46] Y. Sun, Z. Li, X. Li, and J. Zhang, "Classifier selection and ensemble model for multi-class imbalance learning in education grants prediction" Applied Artificial Intelligence **35** (2021) 290. https://www.researchgate.net/publication/349083942_Classifier_Selection_and_Ensemble_Model_for_Multi-class_Imbalance_Learning_in_Education_Grants_Prediction.

[47] Evaluation metric: leave your comfort zone ant try MCC and brier scope, by F. Comotto. (2022, January 8).

[48] C. M. Nalayini, J. Katiravan, A. R. Sathyabama, P. V. Rajasuganya, and K. Abirami, "Identification and detection of credit card fraud using CNN", in *Application of Computational Intelligence in Management & Mathematics*, 2023,- pp 267—280. https://link.springer.com/chapter/10.1007/978-3-031-25194-8_22.

[49] L. Shang, Z. Zhang, F. Jang, Q. Cao., H. Pan, and Z. Lin, "CNN-LSTM Hybrid model to promote signal processing of ultrasonic guided lamlo waved for damage detection in metallic pipeline", MDPI **16** (2023) 7059. https://doi.org/10.3390/s23167059.