Journal of International Financial Trends
Vol. 1 (2025), No. 1, pp. 61-89
DOI: https://doi.org/10.55578/jift.2506.005

ARTICLE

A Boosted Deep ConVNet embedding Long Short Term Memory with Synthetic Minority Oversampling Techniques as Foiling Model for Payment Card Fraud

Lateef Gbolahan Salaudeen[1,2,*], Danlami Gabia[1], Muhammad Garbaa[1], Hassan Umar Surua[1]

[1] *Kebbi State University of Science and Technology, Aliero, P.M.B 1144, Aliero, Kebbi State, Nigeria*

[2] *Department of Computer Science, College of Natural and Applied Sciences*

Chrisland University, Abeokuta, PMB 2135 Owode-Ajebo Road, Abeokuta, Nigeria

[*]Corresponding author. Email: lsalaudeen@chrislanduniversity.edu.ng

Received: 20 April 2025, Accepted: 30 May 2025, Published: 13 June 2025

Abstract

Payment card fraud with contemporaries have persisted as strain challenges bedeviling the financial institutions. With hi-tech thieves exploiting flaws in the digital fraud prevention and detection system to prompts derogatory effects of unquantifiable financial losses, cash back, and customer frictions. An ideal Fraud Detection System (FDS) and countermeasure is require for mitigating these concerns. As a result, several scholars anticipated statistical methods, rule-based approaches with many others for detection. But, majority of these approaches suffers from imbalance data distribution, high dimensionality with sparsity challenges, and real-time detection. This study recommended enhanced Deep ConVNet embedding Long Short-Term Memory and resampling method of SMOTE (DCNN-LSTM+SMOTE) as potential solution. The model is design and implemented on Google Colab platform with GPU; where Tensorflow is used for the DL and Scikit learn for ML models respectively, and Python as the modelled language. Firstly, baseline experiment is steered on two orthodox ML models of Random Forest (RF), Logistics Regression (LR) for feature selection and engineering. While probing kaggle dataset obtained; comprising 284,807 records with 31 field's features. This dataset is very imbalance with data distribution sort of 0.17% deceitful and 99.8% non-deceitful. Second trialing is conduct; using SMOTE techniques to balance the dataset sort distribution and improved on used LR, RF, with other models such as Isolation forest, Artificial Neural Network (ANN), Multiple Layer Perceptron's (MLP), Light Gradient Boosting Machine (LGBM), Deep ConVNet and Long Short-Time Memory. In testing efficacy of these models, confusion matrix performance evaluation metrics is delved. This revealed the outcome of the balancing model trial; that described the proposed DCNN-LSTM+SMOTE superclass performance against other models. Where, its accuracy score and prevalence result is 99.8% distinctly. The model offered the second least Error Rate of 0.2%. With 99.9% of recall, True Negative Rate (TNR), Precision and F1-Scores outcomes respectively. Cohen Kappa result is 99.6% and the false positive rate of 0.00%. This result validates the developed model as remarkable in performance, when compared with benchmark studies; and it is promising in the classification of fraudulent credit card transaction in financial institution.

Keywords: Fraud Detection System; Imbalance Dataset; Deep Learning; Financial Institutions

1. INTRODUCTION

For decades, financial institutions have been rendering noble financial arbitrator services to all business organizations; keeping money and other valuable assets for individuals and institutions and possibly borrow money from them in order to provide loans or make other investment [1,2]. Besides, this institution is classified into two groups of banking and non-banking sectors; that are further portioned into three sub-units of depository, non-depository and investment bodies. With

https://doi.org/10.55578/jift.2506.005

institutionsstatuesque deliberated in [3,4]. For goals of profit expansion; engrains in refining client patronage trust through satisfactory service delivery which gears the sustenance with acquisition of new clients [5]. Congenially, financial institutions purpose is distressed by demystifying scheme of frauds [3,5,6]; transfused by fraudsters for hostile socio-economic trepidations; to achieve self-interested course [3].

For this cause, the world and the financial institutions had been reforming to endure the sophistication of digitalized community [7,8], where daily financial transactions are compelling via an e-commerce channel, gadgets, and mobile apps relishing binding credit cards for both online and offline transactions [9]. In ensuring global cashless policy is inexorable as economic enabler [10-12]. Besides, this is prone to fraud; due to nature for credit cards usage and affinities of fraudsters to exploits cards details via dark web links using either phishing or social engineering fraud tactics for tricky purposes [13]. Recently, statistic reveals that over 51% of the world populations (e.g. American, Asian and African) uses credit cards and online payment platform for transactions [14,3]; because of the imperious of Point of Sales (POS) system for transactions, advances in communication networks and Information Technology (IT). That was hosting for seamless services coated in encrypted end-to-end secure transactions for efficient procurement of merchandise required by individual and organization, via managing resources (e.g. time and efforts) with growth in productivity and profitability [15]. Contrarily, very few individuals felt secured and confident in using the cards for regular transactions [13]. As it considered, that the monetized daises can be usurped for deceitful purposes to incite shocking fraudulent transaction on individual (e.g. cardholders), merchant, financial institutions (e.g. card issuer or acquirer) and government [9]; thus leaving an imprint of derogatory implications of revenue losses, charge back, and customer frictions infiltrating customer reneging tantamount to reputation and/or infrastructure damage which perhaps leads to organization bankruptcy and individual psychological defects [5].

To regulate this imprecision of fraud; credit card issuers with their financial institutions and fraud experts came up with an idea of engaging diverse forms of fraud detection models, software's, processes, preventive and countermeasures approaches such as Card Validation Codes (CVC), Address Verification System (AVS), Multi-facet Authentication (MFA), Magnetic strips, Three dimensional holograms (3Ds), advance tracking and monitoring system, Biometrics and One-time password (OTP) with tokenization as new ways of mitigating the fraud [3,5]. In addition, the institutions consider the replacement of credit cards with astute cards. But, based on their evaluation, it is learnt to be costly. Due to widespread of POS gadget, and the vast amount of payment cards in circulation across the world [6]. Instead, the payment fraud is suggested for detection via rule-base scheme or abnormalities check in transaction [16]; this can be achieved via Internet Protocol (IP) address which identifies suspicious geo-location. This device with innovative technologies can raise red flags for resistance against dishonest financial transactions [17]. Although, the aforesaid tactics presented positive results. And, certainly not capable for the fraud abatement; due to improvement in modern technology and global system of communication, and fraudster out-smartness scheme in bypassing the prevention schemes [18]. This hindrances constituted to unceasing fraudulent scheme sparingly led to extreme loss [19]. So, there is need for more cogent proactive and predictive technological-driven fraud detection system (FDS) and counter-measures solutions in curbing the financial transactions menace. However, data analysis and modeling approaches comprising statistical method, data mining, machine, deep learning models with hybrids tactics are suggested as proxies in mitigating the fraudulent schemes [20,3,5,21].

Today, machine with deep learning models and their hybridized approaches have gained recognition across different and related fields due to their applicability and efficacy in combating myriad form of frauds [22,9,23-25]; by exploiting and analyzing datasets stemming from varied sources. Besides, Artificial Intelligence (AI) is portrayed as paternal fields of both machine and deep learning approaches. Deep learning (DL) dwell beneath ML and soft computing methods [26]; with numbers of DL models application presenting to scientific communities; these are suitable in countless aspects which includes safety, security, energy, hydrological systems modeling, economic, bioinformatics, health informatics, urban informatics, computational mechanics and many others [26]. On the other side, ML technique embraces immense set of computational actions (models) striving to mine data patterns and utilize the outcomes to drive scientific simulations notions for predictions [27].

While, DL is presented with the objective of moving ML closer to one of its original goals of AI [28]; that entails learning multiple levels of representation and abstraction to gain insights from dataset su4ch as images, text and sound [29]. Besides, [30] in a study distinguish between AI, ML and DL models. While, [31] study provides an elucidation on their range of learning approaches partitioned into three major groups (supervised, unsupervised and semi-supervised) with many others. In [32,33] distinct studies insight on top ten ML and DL models and their areas of applications were enunciated.

These, prospective scholar's explore their real world usefulness in aspects of Marketing research, Analysis of data, Image processing and Pattern recognition [34]; by linking matched study field dataset for analysis and towards fraud detection. For instance, the distinct studies of [19,35] applied the approach for Insurance fraud detection in financial institution. [36] Deploys for metastatic cancer detection, [37] in prediction of Parkinson's diseases. [38] Applied DL model for prediction of COVID-19 both in health sector. [39] Uses it for crop yield prediction in Agricultural sector. It is also deploying for computer vision and fault diagnosis [40,41]. While, the distinct studies of [42,43] and many others relishes it on SIMBox Bypass fraud detection in a Telecom industry. [44-46], applied both ML and DL models for intrusion detection system to identified unusual conduct in a network system. More so, [20,11,15] and many other researchers hires the methods for payment card fraud detection in banking sector. Where it's discovered that those approaches demonstrated promising results. But, the existing methods betrothed for the classification of credit cards transaction is hindered with challenges of scarcity of real-world dataset during experimentation, while the open source data available for experiments suffers from imbalance data dissemination that entails adjustments via resampling techniques with other approaches for data balancing [47,48]. Another problem is high dimensionality with sparsity in dataset features, amidst immediate discovery, and complexities inferiority of a genuine payment fraud curtailment. The aforementioned drawback initiates research in this field to be thought-provoking and difficult [11,49].

To this regard, several scholars' (e.g. [50-52,10,13,15]) have suggested tactics involving machine with deep learning models as well as their hybrid approaches towards classification of fraudulent credit card transaction. Apparently, some of these approach are disappointing in curbing the eroding acts of fraud. This necessitate the request for more proactive and radical regulatory mechanism for the fraud abatement [53]. This study aimed to leverage on the distinct contributions in [3,5] studies. While, refining to propose a hybridized models which serves has an improvement over the predated studies. In this research, a boosted Deep ConVNet embedding Long short time memory with Synthetic minority oversampling techniques (DCNN-LSTM+SMOTE) is proposed potential resolution to mitigate the inferences of fraudulent payment card transaction in financial institutions. With goals of comparison with benchmark studies for exploits during the classification of fraudulent credit card transaction; based on the appeal made in previously reviewed studies [11,15,38]; establishing the best performance model that could deter the consequences of payments fraud [5]; and to as well answers the raised under listed questions:

Q1. What is the best tactic to implement in taming the unceasing act of payment fraud?
Q2. How effective and efficient can the proposed enhanced hybrid DCNN-LSTM+SMOTE model be in classifying fraudulent credit card transaction?

This research is partitioned into five (5) sections, and deliberated thus, Section 2: presented assessment on the prevailing studies and models utilized towards payment fraud abatement. Section 3: presented discuss about materials and methods with dataset absorbed for this study. Section 4: Clarified about experimental data analysis with finding discussion Section 5: offers the research conclusion with suggested recommendation for future work.

2. Literature Review

Credit card fraud is literary known as payment card fraud [6,7]. In distinct studies of [54,3,5,49, 24,55]; concepts of fraudulent payment card transaction with their implication are discoursed [56,57]. Payment card fraud act is uprising and has shone as potential socio-economic threats instigating on public and private organization with individual globally for despicable reasons [5,58,54]. This criminal activity is obliging on influencing factor such as Data breaches, Skimming, Merchant conspiracy,

Triangulation, Inappropriate verification of credentials, Technological growth, Wrong card controlling tactics, Poor system security with integration [6,3,5]. However, pre-existing studies deploys ML, DL, statistical methods, rule based system, and data mining approaches and many others for controls [59,60]; with graph showing numbers of fraudulent credit card transaction cases and cost implications forecasts between 2010 up-to 2027 [61,21]. These are explored to affirm their implication on the knowledge field with drawback identified for considerable ways for model improvement towards abatement of the unceasing act of credit card fraud.

[11] Study proposes a vigorous DL method covering recurrent neural network and gated recurrent unit as base wits in assembling ensemble classifier, with a multilayer perceptron (MLP) as the meta-learner. The scholar offered conjoint balancing models approach of SMOTE-ENN to address the challenges of imbalance data distribution. The experiment outcomes of the proposed model displayed t sensitivity and specificity of 100% and 99.7% distinctly, which is higher to what other ML classified presented in the pre-existing work.

[61] Study explore ML models of XGBoost via the application of data augmentation methods addressing the encounters of imbalance data distribution to improve fraud detection rate. The study imbibes the evaluation metrics of precision and recall and leverage on historic datasets; using hybrid balancing model approach of SMOTE-ENN. The result of these ML model is profound in offering potential solution which can strengthen financial reliability, allot resources efficiently and reinforce customer trust in the face of the rising fraudulent schemes.

[13] Study proposes notions for fraudulent transaction detection using a Decision Tree Algorithm (DCA); where questionnaire were prepared and analyzed to explore students' awareness towards the fraudulent occurrences. 102 student's details across varied universities and countries were acquired for exploration. The outcomes exhibited an approximate 96% despondence recognition of how payment fraud ensues. While, 4.1% does not. Conversely, 82% despondence conveyed disposition on exercising tool built approaches for projected model to curtailment occurrences of payment card fraud.

[62] In this study, the scholar deploy novel unsupervised learning method for payment fraud detection. Auto-encoders (AE) with feature attention and Generative Adversarial Network (GAN) are betrothed to efficiently distinguish between transaction data. Two dataset of kaggle repository are involved for the study; while the proposed approach outdoes prevailing fraud detection models. The experimental result performances was compared with conventional ML tactics like Random forest (RF), Xtreme Gradient Boosting (XGB), K-Nearest Neighbor (KNN), Support Vector Machine (SVM), Decision Tree (DT), and pre-existing deep learning approach of LSTM, ConVNet, Multiple layer perceptron's (MLP), and AE. The proposed model has stronger generality, which efficiently evade the difficult of data inequity for better performance result. In real life situations, the scholar's technique can defense the interests of financial users.

[63] Tried addressing the encounters of missing values and imbalanced class dissemination in payment dataset. The scholar develop models to detect monetary statement fraud. Foremost, the scholar deploy list-wise and pairwise removal to tame missing value glitches. Therefore, suggested integration of three attributes selection approaches and applies a nonlinear distance association to choose noteworthy attribute with best outcome at four recital assessment metrics. More so, the scholar engaged under-sampling and oversampling techniques to curtail the imbalance class dissemination in dataset. Lastly, rule-based approach that is not sufficient for fraud detection is imbibed to produce beneficial rule, while exploring several companies dataset. Ensemble learning model of RF is offered in this study and avails financiers, experts and auditing personnel as references.

[64] Suggested an ensemble model based on sequential modeling of data imbibing deep recurrent neural networks and a novel voting tool based on artificial neural network for payment fraud detection. This study trial was delved with distinct two real-life dataset that show the superclass assessment of the suggested model against their benchmark studies. The time analysis of the intellectual advocated model portrays its efficacy in terms of immediate assessment likened with existing model in fraud detection foray.

[59] Deliberated about the challenges related with each approach of models deployed, which inclusive of LR, DT, RF, and Naïve Bayes with ANN imbibed for payment card fraud detection. The study carried out a literary survey that compares different author's model performances by embracing outdated rule-based approach, where ML models, with DL approach are explore. It's concluded that

both ML and DL models, in precisely, presented capable outcomes in identifying credit card fraud, as it learn from enormous datasets and identify patterns that are problematic for human analysts to detect. DL methods, such as neural networks, have great potential for fraudulent transactions detection. Conversely, payment card fraudsters linger to develop new and sophisticated methods to evade detection, and fraud detection systems must remain to advance and adjust to these varying threats

[65] Delved two experiment, first on baseline models where five supervised ML models of LR, DT, RF, NN and XGB were explored. In this study comparative analysis entrenched. XGB ordering models is considered appropriate for the fraud detection based evaluation metrics such as recall and f1-scores that provided 70% and 81% outcomes respectively; better than LR, DT, RF and NN. The second experiments, explore five resampling approaches to balance the original dataset. This reveals the activeness of an ensemble approach when dealing with imbalanced class sorting hitches. The resampling approaches are observed as operative method that advances the performance of imbalance dataset. However, the enriched VAEGAN model attained an admirable precision and F1-scores, but the advance recall and AUC at certain expansion ratios were not significant compared to GAN and VAE models.

[66] Built innovative model with a hybrid approach of DL with ML. where, Bi-LSTM-Auto-encoder and Isolation Forest are conjoined to detected payment fraud. Kaggle dataset explored in this study. There anticipated model presented 87% detection rate of payment fraud. Compared to Isolation Forest with 79%, Local Outlier 3%, and LSTM-Auto-encoder 82% of detection rates respectively. The proposed model achieved utmost detection rate.

[52] Study suggested hidden Markov model (HMM) combining Deep Neural Network (DNN), which poised efficiently result toward payment fraud detection. It recorded highest accuracy score, diminished errors, which is timely for fraud abatement. The outcome of the experiment displays the proposed model efficiency in classifying payment transactions with precision rate of 97%.

[67] Study absorbed the practice of LR and Isolation Forest to shape the incidence of fraud. The dataset engaged was obtained from Kaggle repository, these battle with challenges of from imbalance class dissemination. The researchers failed to balance before instituting their discoveries. In appraising their model recital: Precision, Recall, F1-score and AUC-ROC are used. It discovered that LR produced 99.91% accuracy score for training and 78% testing data. 95% disclosed for precision, 56% recall and 70% F1-scores respectively. Isolation forest offered 99.82% accuracy score for training data and 74% for testing data. While, it precision, recall and F1-score were 49% consistently. From the outcome, it surmised that LR is the model with excellence demonstration against iforest model.

[68] Study applied ML models of CNN on dataset obtained from kaggle repository to identify and classified fraudulent credit card transaction into genuine and fraudulent classes to lessened the number of false alerts. The assessment metrics absorbed includes Accuracy score, Misclassification, Precision, Recalls and F1-score. Comparative analysis is performed between proposed model of ConVNet model, RF and LR. It is recognized that ConVNet model is the finest in terms of performances without starting result percent.

[69] The researcher emphasis on improving model parameters, refining recital actions, while incorporating DL to fix errors and diminish false negative rate. DT, XGBoost, LR, RF, and SVM were absorbed. The study likens thee models across multiple assessment metric and learnt DT achieves preeminent with recall of 100%, followed by XGB 85%, LR 74.5%, RF 76%, and SVM 69% respectively. By joining multiple classifier ensembles and rigorously assessing the routine. This study, remarkably advances credit card fraud detection system. But, the assessment parameters expose weaknesses of these model.

[70] Designed a fraud system that learnt user's attributes and transaction attributes. The study anticipated hybrid neural network with a clustering-based under-sampling approach on identity and transaction attributes (HNN-CUHIT). For addressing imbalance data dissemination and fraud detection challenge. As real-life dataset acquired from a city bank during SARS-CoVd, 2020 is explored for experiment. In tackling the imbalance data dissemination problem, the proposed model trials depicts outcome of data dissemination ratio in magnitude of honest and dishonest set of 1:1; for which the model assessment is finest. With F1-scores of 0.0572 in HNN-CUHIT and 0.0454 in CNN model via ROS. On fraud detection trials, the F1-scores is 0.0416 in HNN-CUHIT, achieving the greatest outcome. While, it is 0.0284, 0.0360 and 0.0396 distinctly for RF, LR, and CNN models. Base on this

trials results; it was deduced that HNN-CUHIT excel in performances against the orthodox ML model imbibed for the imbalance trials and fraud detection.

[71] Betrothed ML model of CNN with Artificial Intelligence for payment card fraud detection. As kaggle dataset was explored. The outcomes of the proposed model is overwhelming as it presented 99.8% accuracy score, that is greater likened to preceding models of LR, RF and SVM results in benchmark study. The exertion cultivates a webapp software possessing great accuracy rate with precision in prediction and detection fraud. The software if incorporated and extended for commercial use may lessen fraudulent transaction rate.

[20] Study involved collaborative model of KNN, RF, SVM, Bagging and Boosting within a voting structure. SMOTE under-sampling and ensemble approach are as well utilized to address imbalance data distribution challenges. The practical framework involves exploratory data (EDA) and evaluation. Google Colab is utilized as implementation platform; these have capability of easing model training and testing. Relative analysis study was delved among the suggested ensemble model, traditional ML models, and individual classifiers. The outcome discloses the greater recital of the ensemble methods over other models in justifying encounters linked to payment card fraud detection.

[50] Study measured the efficacy of ML models such as XGB, LGBM, LR, RF, extra tree and CatBoost; while publicly available dataset of payment transaction consisting of 550,000 records was imbibed. The dataset absorb in assessing the ML models evaluation metrics of accuracy, recall and F1-scores with confusion matrix. The ML model used achieve high accuracy and precision results of 100% across board.

[3] Betrothed models ANN, MLP, CNN, RF, LR and proposed hybrid LGBM+SMOTE model. While, comparative study is delved using eleven assessment metrics are imbibed to validate models with the best results against others. It was discovered that the LGBM+SMOTE model presented surpasses results across seven categories out assessing metrics. The LGBM+SMOTE have 96% accuracy score, 0.4% misclassification, 95% recall, 47% prevalence, 45% Cohen kappa, 96% F1-score and 93% of Matthew's correlation co-efficiency (MCC). LGBM+SMOTE model excellent performance is hamper on the few kaggle dataset engaged.

[5] Advances on [3] study involving larger dataset. In this study, the scholar offered hybridized DCNN+SMOTE based models. The procedural approach uses is synonymous with predated work. Where, baseline model trial is conducted, examining models like LR, RF, Isolation forest and MLP. The bid for inapt assessment metric like accuracy to create findings on disparity in data distribution suffers with over-fitting and under-fitting trials; that led to poor impression outcomes. That tends to only predict the bulk or smaller classes. The second experiment conducted explored data augmentation approach of SMOTE which balance distribution of dataset used. The models performance outcome was justified based on seven performance evaluation metrics out of the eleven arrayed. DCNN+SMOTE model showed a superclass performance results across board of evaluation, showing 1.00% accuracy score, recall, true negative rate with F1-scores distinctly. While, 0.001% results is observed for both false positive rate and prevalence separately. In contrast, to what RF, LR, Iforest, MLP, ANN and LGBM presented even when SMOTE is applied to them all for upgrading.

[21] Applied deep learning models of LSTM, 2DCNN, 1DCNN, ANN and two other ML models of SVM and RF. While three distinct kaggle datasets from European dataset (ECD), small card dataset (SCD) and Tall card dataset (TCD) are engaged for payment card fraud detection. In addressing the challenges of unequal dataset distribution involving most credit card; random under sampling, near miss sampling and SMOTE are used. The experimental outcome over dataset utilized for model showed that the deep learning model of DCNN and LSTM yielded better performances than old-style models. While all the model in the study performs side-by-side, LSTM with 50 block was singled as the one model with greater F1-score results of 84.85%.

[60] Study involves ML models like CNN, RF, SVM, LR, NB, and KNN with a suggested hybrid model of CNN+RF for fraudulent transaction detection. The hybrid model presented an accuracy score of 99.98% against other delved model that presented 99.94%. This research does not only depict that the hybrid model work on specific dataset. Besides, it confirm the research gaps as problem statement, which proposed approach regulates. The dataset betrothed for this study can always be used to solve classification and regression model task. Weka software is the development and implementation

platform utilized. Thus, the hybrid CNN+RF model is proven as the best recital model for payment card fraud detection.

From the literary survey done, it was deduced that most researcher that solve the challenges of payment fraud delves, do so in relationship with challenges highlighted in [3,5] studies; which revolves around disparity in data class distribution; with high dimensionality and sparsity challenges [20]; fondled within the open source kaggle dataset available. Due to lack of real-world dataset for research. This imbalance data distribution with other challenges presented suboptimal fraud detection capabilities. These pre-existing works [20,21,53,61] advised over the deployment of balancing model approaches like data augmentation, resampling methods, and many others for the utilization to manage imbalanced credit card fraud data for more springing results that can curtail fraudulent credit card inferences. Besides, a broad study concerning the approaches effectiveness is enunciated in subsection 3.1.2. However, there is no effective approach which could be implemented to tame the unceasing act of fraudulent credit card transaction based on literature review [20]. As fraudsters often time advances the fraud knowledge to bypass any fraud prevention and scheme [18]. This answered the raised question in (Q1).

2.1. Machine Learning Models Engage in This Study

This research aspect imbibes four ML models of Random forest, iforest, LGBM, with linear regression model of LR adopted for the study experiments [3,5]. For which first experiment was performed on baseline models delving only LR and RF based due to their antecedent in classification and regression tasks precisely on credit card fraud transactions [14]. The second experiment relish adopts both the ML and DL models for comparative study along with proposed improved DCNN-LSTM+SMOTE model.

2.1.1. Logistics Regression

Logistic regression is an arithmetical model; often engaged to salvage binary classification and regression challenges task. It is applicable to payment card fraud [3,5,50]. It can as well be deploy to predict and detection tumors, spam in e-mails and many others [7]. Besides, [14,7] in their respective work provided elucidation about the LR concept. LR is often use to estimate the probability that an instance belongs to a particular class. In a Logistic Regression, model computes a weighted sum of input features plus a bias term but instead of outputting the result directly like Linear Regression model its output is obtained by applying the logistic function (also known as sigmoid function), representing the estimated probability of the instance belonging to the positive class.

2.1.2. Random Forest

This is a trendily used ML model initiated by Leo Breiman and Adele Cutler. It is termed RF because is a subsets of data and features which ended up in building a forest of decision tree. Details about this model formulation is considered in [14,72]. RF associates the outcome of multiple decision trees to reach single outcome. The model ease of usage and flexibility prowess have fueled its adoption for handling both classification and regression task [14,72].

2.1.3. Solation Forest

Fei Tony Liu in 2008 initiated the concept of Isolation forest, which is as well known as iForest. It is an unsupervised ML model often deploy for anomaly detection in tabular data; which involves the splitting of sub-samples of the data in relation to some attributes at random [51]. The advantages and variations of this models that includes density iforest, fair-cut iforest is enunciated [14].

2.1.4. Light Gradient Boosting Machine (LGBM):

LBGM is prevailing engaged ML models; that's well-known for its competence and correctness in handling many data types and complexity problem [62,3,5]. It cascades beneath the gradient boosting structures that were ensemble learning approaches; combining the analytical power of various models to create a stronger overall prediction [3].

2.2. Deep Learning Model Absorb for This Study

This encompasses ANN, LSTM, MLP and deep ConVNet. DL models are carefully chosen has they can be used for tabular data classification and not only for image sorting [3]. More so, it can assist to address the challenges of high dimensionality and sparsity in dataset [3,5,37].

2.2.1. Multiple Layer Perceptron's (MLP)

It is a type of artificial neural network that fall under the broader category of deep learning models. MLPs are commonly used for classification tasks, where the goals is to predict the class labels of input data based on its features; as depicted in Figure 1. The MLP design consist of input, hidden layer and output layer, which are measured via objective function, activation with optimization function and threshold [73].

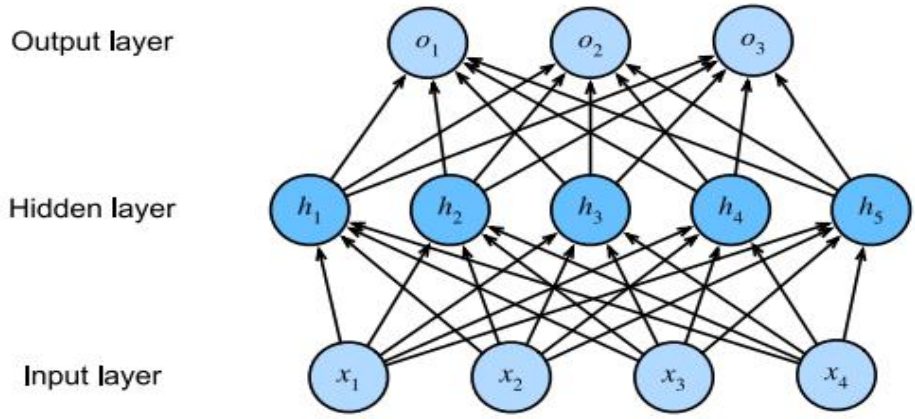

Figure 1. Multiple layer Perceptron Structure with hidden layer of 5 hidden units

2.2.2. Deep Convolutional Neural Network (DCNN) Model

This is otherwise shortened as ConVNet, DCNN is protracted form of ANN that are predominantly engaged for feature extraction from the grind like matrix dataset [74]. The DCNN approach is of great significance in the study field of both ML and DL with some bounding limitations [75]. Besides, its applicability is domicile in aspect of computer vision, Natural language processing, and recommendation system [75-77]. DCNN is usually use for spatial data (e.g., images) however, in the study it was delve for relational kaggle dataset.

2.2.3. Long Short Time Memory (LSTM)

This is the prominent approach for addressing vanishing gradients challenges [21,76,37,78]. LSTMs is a standard recurrent neural networks (RNN) model. The detail constructive explanation of this models is expounded in [21,78,79]. LSTM used for sequential data, Figure 2 below represented the LSTM structure model.

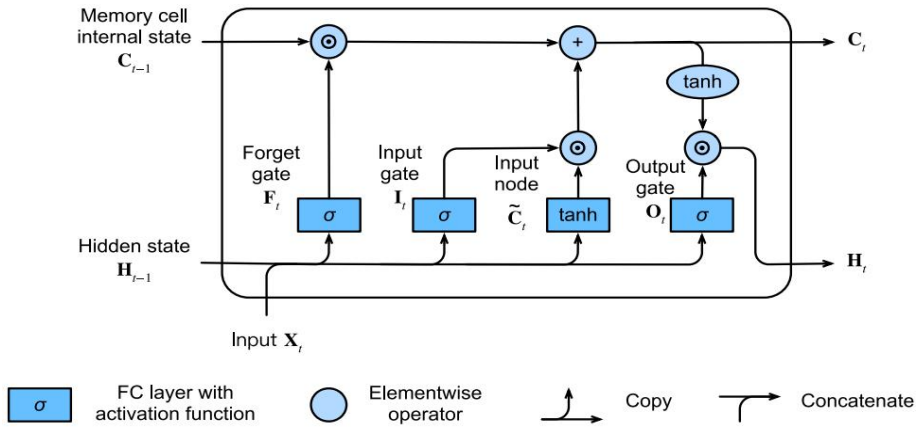

Figure 2. LSTM Structure Model

2.2.4. Proposed Boosted DCNN-LSTM+SMOTE Approach

This model is explicitly describe in [21]. While SMOTE techniques was embed to balance the imbalance, distribution in the dataset as described in subsection 4.1.2 [3,5]. This serves as refining method. This model is engraining as it support time series dataset for data analysis [41,61]. Table 1 below depicts areas hybrid deep learning models of DCNN-LSTM was previous imbibed in the aspects of natural language processing, health sector, text analytics, fault classification and many others. This study was the first to apply the approach in the aspect of payment fraud. The approaches for fraudulent scheme detection have similar scenarios, so this research scope is not an exception [18].

Table 1. Field where Hybrid DCNN-LSTM are utilized

S/N.	Author	Field of application	Specialization/area
1.	Zonyfar et al., [76]; Wang et al., [80]	Web Prediction, Natural Language Processing (NLP)	Web Technology/ Engineering Sentiment Analysis with Speech recognition
2.	Lilhore et al., [37]	Health Sector	Prediction of Parkinson's diseases
3.	Zhang et al., [73]	Actual Time Prediction	Human Energy Feasting and Air Pollution prediction
4.	Shang et al., [81]	Fault Ultrasonic Signal Classification	Signal handling of Ultrasonic guided Lamb waves for impairment detection in metallic pipelines
5.	Yang et al., [40]	Computer Vision-based vibration dimension method that can regulate the natural frequency of diverse beam	Complexity embroil in BSS computation and Modal frequency extraction
6.	He et al., [41]	Fault Diagnosis	Rod Pumping System

3. MATERIALS AND METHODS

3.1. Datasets

This study exploit dataset collected from Kaggle repository via the link https://www.kaggle.com/mlg-ulb/Creditcardfraud to studied ML and DL models along with the proposed DCNN-LSTM+SMOTE for fraudulent transaction detection. The dataset sample format as shown in Table 2 entails 284,000 transaction records. In which 99% are group as non-fraudulent (0) and 0.2% as fraudulent class (1) as depicted in Figure 4. Besides, the dataset have 31 column features classified as V1-V28, Amount, Class and Time. This dataset is imbalanced as there are more non-fraudulent group, which served as the majority class and the fraudulent as minority class. To address challenge of imbalance in data distribution, Synthetic Minority Oversampling Technique (SMOTE) was divulge and introduced [3,5] in section 4.1.2. While data pre-processing with feature extraction process was inherently, explored.

Table 2. Sample format of Dataset utilized for this study

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

(a) Cleaning dataset:

Data cleaning is the first stage of pre-processing stage. In this stage, dataset undertakes cleaning, to address duplicity and missing values in the dataset. To use the cleanse dataset, the models is further trained. Besides, this steps entails erasing the rows of missing or inappropriate values is inevitable by preprocessing procedure: OneHotEncoder, MinmaxScaler, StandardScaler, RobustScaler, and Command in the Google Colab Platform exploring the python commands of:

 # Checking if there is any missing data remaining in the dataset
Dataset.isna ( ).sum( )

(b) Balancing the dataset:

The dataset for absorb is extremely imbalanced [6,3,5]. The sign of its skew feature depicts few fraud records presented in Figure 4. The usefulness of data preparation and model testing is important dataset distribution during exploration [6]. In addressing this contest, two methods were hired in [20] study which include under sampling and oversampling approach. These is extenuated in [3,5] studies.

(c) Data analysis:

To better comprehend the dataset imbibed for this study, data pre-processing is delved; where open source collections like Pandas, Matplotlib, NumPy, Seaborn using PyCharm community are imbibed. Matplotlib, NumPy, Seaborn were exceptional collections for notion in Python [3,69] and are as well explored. Certain visualization on histogram, bar graphs, density plots and box plots are obtained. While, Google Colab Platform are explored to gain insight on the dataset. For a familiarity with the dataset, scatter and density plots and imbalance data distribution illustration is displayed in Figure 3 and Figure 4 below.

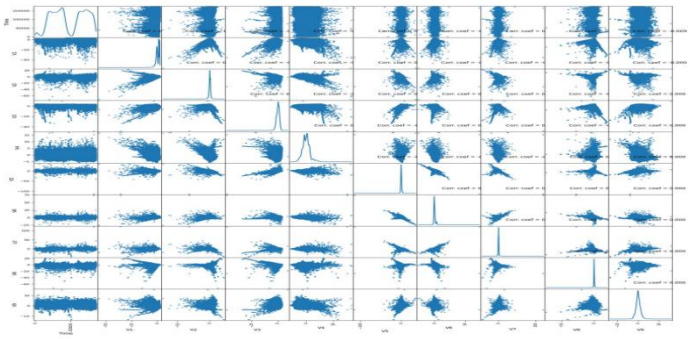

Figure 3. Scatter and Density Plot of the Dataset

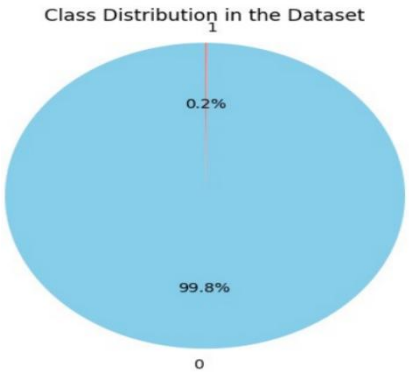

Figure 4. Imbalance Dataset distribution

Figure 5. Transactions Amount Frequency

From Figure 4, it is depict that the dataset is imbalance and it is much skew, in this regard. However, Logistics Regression, Random Forest, Isolation Forest, MLP with the proposed DCNN+LSTM+SMOTE is considered. Figure 5, depicted the transaction amount frequency, it's deduced that most of all payment transaction matters' quantities are below $2,500 with average of $88.35. However, one can trust on this attribute united with other attributes to discover fraud [6]. While, the negative class correlation in the features of V17, V14, V12 and V10 were visually compared in Figure 6.

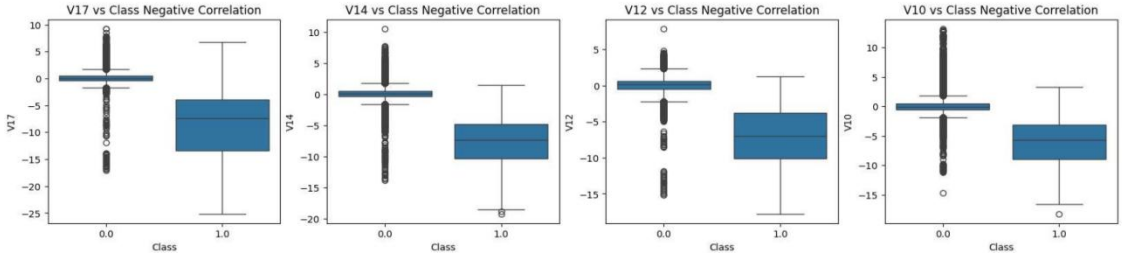

Figure 6. Negative Class Correlation from the Dataset

(d) Features' correlation:

The dataset 28 features are altered based on Principal Components Analysis (PCA) traits. However, Figure 7 below displays the correlation matrix heat map of variables involving in the dataset:

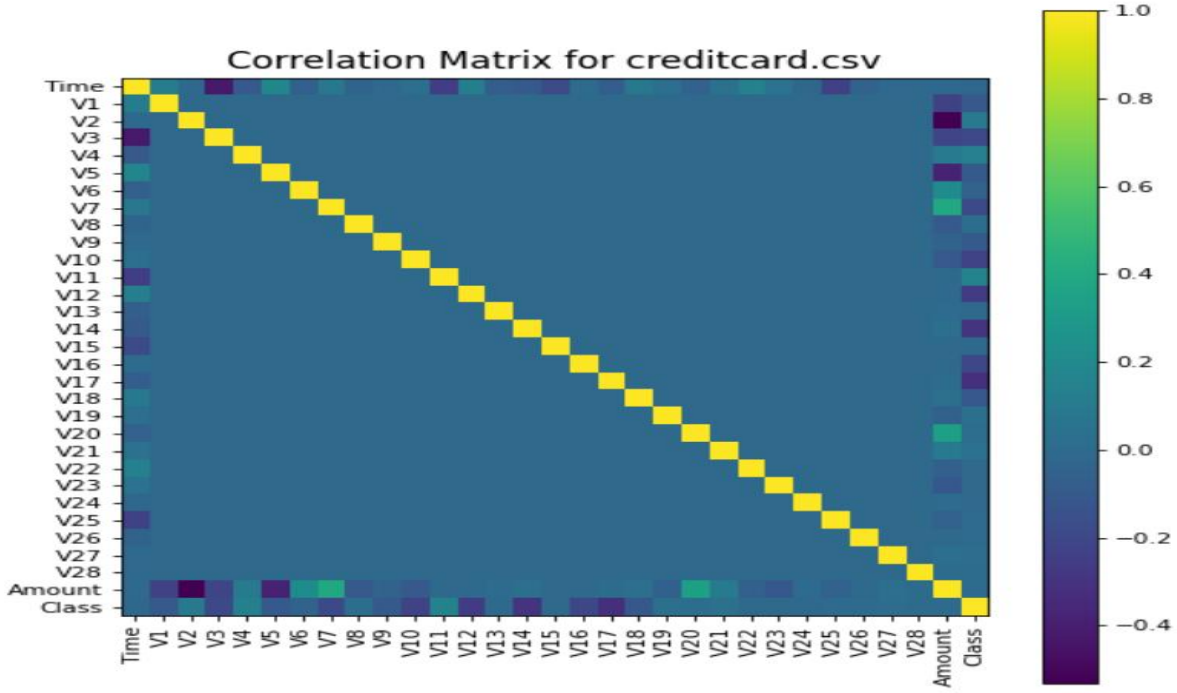

Figure 7. Correlation Matrix heap-map for the dataset

It was deduced that certain variables has no impression on the outcome while identifying payment transactions recorded low correlation ratio. Besides, variables like V4, V8, V13, V15, V22, V23, V24, V25, and V26 have no intense association and were excepted [6].

3.1.1. Handling Imbalance Class Distribution

To address the problem of imbalance class distribution six (6) distinct approaches of random sampling methods, weighted methods, evaluation metrics, ensembles methods, data augmentation methods and domain knowledge can be applied [47,82]. Some of these [20,82] deliberated in their study. Obviously, most scholar's module up this distinct method without given proper creditability to its usage; which is the reason for this elucidations as resampling approach of SMOTE was imbibed in this study, it approaches mimics others.

(a) Resampling Method:

This is dominance technique integrates for solving imbalance class distribution. It entails resampling the data, either by inflating the quantity of samples from the smaller class (oversampling) or lessening the quantity of samples from the bulk class (under-sampling). This is insinuated to balance the class distribution in credit card dataset and as well reduce the biased in the model formulate. However, resampling methods are entraps with over-fitting, information loss or computational cost drawback challenges. Conversely, [47] surmised that one should choose resolutely among the resampling methods, when rooting data analysis task.

(b) Weighted methods:

This is another approach that could be deploy to solve imbalance class distribution in dataset. In this, different weights are assigned to the classes, so that the model pays more attention to the smaller class and less to the bulk class. This can be achieving via modifying the loss function or the algorithm parameters to penalize the errors on the minority class more than the error on the majority class. Weighted method help improves the model sensitivity and specificity; without altering the data distribution. However, weighted method can introduce some compromises, such as complexity, instability, or calibration problems [47]. This approach is applied in the formulation of deep learning model of DCNN

(c) Evaluation Metrics:

This deals with the use of a suitable evaluation metrics that can capture the models performance on both classes, rather than relying on the overall accuracy. Some common metrics that can handle class imbalance are Precision, Recall, F1-Score, ROC curves, and AUC [47]. These metrics can assist in appraisal of varied models and identify the optimal balance between true positive (TP) and false positive (FP), or between false negative (FN) and true negative (TN). However, evaluation metrics can also depend on the context and objective of the classification task, so one should think resolutely in selecting the precise metric to tackle problem [47].

(d) Ensemble Methods:

This deals with the usage of ensemble approaches that trusts multiple models in producing final prediction. Ensemble approaches assist in reducing the variance and biasness in models. And escalate the diversity and robustness over prediction. Ensemble approach instances include bagging, boosting, and stacking. These approach can incorporate resampling or weighing techniques to handle class imbalance challenges. However, ensemble technique can have some drawbacks such as complexities, interpretability or scalability [47].

(e) Data Augmentation:

This method uses augmentation which generates new samples from the existing data by applying some alterations and adjustments. Data augmentation can support the increase in size and diversity of data, and reduce the over-fitting and underrepresentation of the minority class. Some instance of data augmentation is cropping, flipping, rotating, scaling, or adding noise. This model can also be domain-specific, such as using synthetic minority oversampling techniques (SMOTE) for numerical data, or

using natural language generation (NLP) for textual data. Data augmentation has restraint of quality relevance, and validity of the generated data. Different data augmentation methods are hire in the [61] study.

(f) Domain Knowledge:

This involves using some prior information or expert knowledge about the data and the problem. Domain knowledge can assist in understanding the causes and consequences of class imbalance, and design more effective and effective solutions. Some instances of domain knowledge include feature engineering, feature selection, anomaly detection or cost sensitivity learning. This approach can also be deploying to enhance the data quality, the model performance and the business value [47]. The challenges of domain knowledge are that it may require some assumption, validations and collaborations.

3.2. Second Dataset

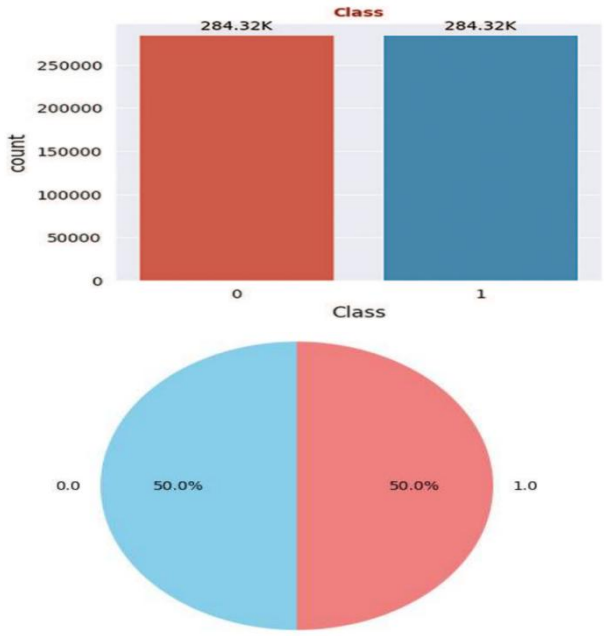

Figure 8. Distribution of Training and Test Set

3.3 Framework for model Design

The study simulate framework for model design and evaluation metrics performances as depicted in [3,5]. In this research, operation processes covering the EDA while separating of dataset into training and testing class [20]. The training dataset successively input into the chosen models for both the training and testing phases. Following this, the evaluation outcomes are steered on the trained model to judge its performance.

3.3. Experimental Platform

This study was carried out on private computer with specification of Intel i7-5600U CPU, 2.7GHz speed, 256 GB RAM, and SSD hard disk, with memory feasting rate of 26%. Hard disk operated virtually 0%. Besides, supercomputer is found appropriate [3,5]. This research indoctrinate Scikit learn suite for ML sorting while Tensorflow is arranged for the DL. Python encoding language was betrothed for EDA. While, library like Panda, Numpy, Scikit-Learn, Matplotlib, Seaborn and many others; discussed in [5,67]. Besides, Google Colab integrated with Jupyter notebook and Google drive cloud infrastructure platforms were the implementation software; and extensively discoursed [3,5,67].

3.4. Evaluation Metrics

The confusion matrix and its performance evaluation metrics encompassing accuracy score, misclassification or error rate, recall, precision, prevalence, F1-score, Null Error Rate (NER), True positive rate, false negative rate, Cohen kappa, and Matthew's correlation co-efficient are imbibed for this study, which is previous deliberated in [3,5,21] distinct studies.

4. RESULTS ANALYSIS AND DISCUSSION

4.1. Model Performances

The model betrothed for study are discussed in section 2.1 and 2.2 above with an evolving tactics for addressing binary classification problems [3,5]. These methods deliberated yield accurate results than orthodox regression-based modeling. It has been reported that deep learning models of LSTM, Deep ConVNet, MLP, and proposed boosted DCNN-LSTM+SMOTE model are superior in performance compared to Isolation forest and both Logistics Regression (LR) and Random Forest (RF) even when SMOTE techniques is integrated with each one of them.

4.1.1. For the First Experiment

Table 3 offered the confusion matrix table generated for baseline trials; where two machine learning models of RF and LR are studied on inequality dataset.

Table 3. Confusion Matrix Table for the Baseline Model on Imbalanced Class Distribution

Models	True negative (TN)	False negative (FN)	False positive (FP)	True positive (TP)
LR	17794	8	17	25
RF	17799	3	11	31

The Figure 10 below provides the bar chart conception with justification table's results for the baseline models. Here, color representation is used to discern between the LR and RF. Blue color is used to attribute LR and RF by orange color. From the Figure 10, it is deduced that the performance evaluation metrics of accuracy, and TNR/specificity of both models are proliferated with the same outcomes of (99.9%) distinctly. Besides, the Error Rate (ER) results of the LR and RF is uniform by (0.1%). However, the recall, precision and F1-Score outcomes distinguished between the two baseline models. Where, the recall result of LR is registered with (75.8%) a bit greater than that of RF (70.5%). The LR precision result is (59.5%), this is less to the RF (73.8%). Lastly, the F1-score of LR (66.7%) while that of RF is (72.1%). Based on this results, it is inferred that RF is the baseline model with best performance evaluation during the classification task on imbalance dataset.

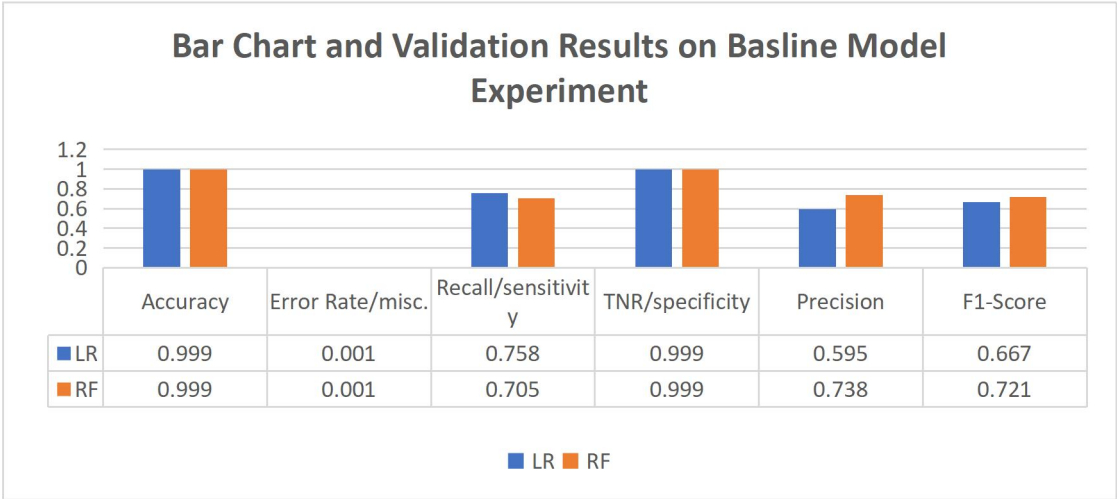

Figure 10. Bar Chart for the Baseline Model

4.1.2. Second Experiment

Table 4 below depict the confusion matrix table for balance dataset. Table 5, presented the balancing model experiment and validated results after the application of SMOTE Techniques applied on training data to avoid leakage. Here, a balance dataset was produce to ensure the model is not biased towards the majority class. The SMOTE technique can be expressed as:

$$X_{new} = x_j + \alpha * (x_m - x_j)$$

Where

- α is a random number between 0 and 1
- x_j is the original minority class instance
- x_m is one of the k-nearest neighbor of x_j

In addition, feature engineering and data preprocessing on the dataset is conducted as early described under section 3.1 to extract significant traits from the data. With proposed DCNN-LSTM+SMOTE presenting overshadowing results against the previous studies where LGBM+SMOTE [3] is deployed and DCNN+SMOTE of [5] study. Table 6 depicts the balancing models hyper-parameter sceneries. Dataset for models was splits into training (80%) and validation/testing (20%) with performance measured by accuracy, precision, recall, F1-score, Matthews Correlation Coefficient (MCC) and many others.

Table 4. Confusion Matrix Table for the Balancing Model Experiments with SMOTE Techniques

Models	**TN**	**FN**	**FP**	**TP**
LR+ SMOTE	40	3	4	38
RF+SMOTE	42	1	4	38
ISOLATION FOREST +SMOTE	43	0	42	0
MLP+SMOTE	42	1	3	39
LGBM+SMOTE	42	1	2	40
ANN+SMOTE	43	0	10	32
DCNN+SMOTE	995	0	1	1
LSTM+SMOTE	22	1	1	18
PROPOSED DCNN-LSTM+SMOTE	2	0	0	995

Table 5. Balancing Model with SMOTE Oversampling Techniques Validation Results

Models	Acc (%)	Mis (%)	Sen (%)	Fpr (%)	Spe. (%)	Prec (%)	Prev. (%)	Ner (%)	Ck (%)	F1s (%)	Mcc
LR+SMOTE	0.918	0.082	0.905	0.091	0.930	0.927	0.45	0.52	0.398	0.916	0.84
RF+SMOTE	0.941	0.059	0.905	0.087	0.977	0.974	0.45	0.541	0.40	0.938	0.88
ISOLATION FOREST + SMOTE	0.506	0.494	0.00	0.494	1.000	0.000	0	1.00	-0.494	0.000	0.00
MLP+SMOTE	0.953	0.047	0.929	0.067	0.977	0.975	0.46	0.530	0.423	0.952	0.91
LGBM+SMOTE	0.965	0.035	0.976	0.045	0.977	0.976	0.471	0.518	0.447	0.976	0.93
ANN+SMOTE	0.882	0.118	0.762	0.189	1.000	1.000	0.38	0.624	0.258	0.865	0.79
DCNN+SMOTE	0.999	0.001	0.50	0.001	1.000	1.000	0.001	0.999	0.00	0.667	0.71
LSTM+SMOTE	0.930	0.07	0.900	0.043	0.957	0.947	0.429	0.548	0.382	0.923	0.90
PROPOSED DCNN-LSTM+SMOTE	0.998	0.002	1.000	0.00	1.000	1.000	0.998	0.002	0.996	1.000	1.00

Table 6. Balancing Model Hyper-Parameter Sceneries

Models	Epochs	Batch size	Optimizer	Learning rate	Layers configurations
LR +SMOTE	10		Adam	0.001	GridSearchCV(log_model,param_grid = param_grid, cv = 3, verbose=True,n_jobs=-1)
RF+SMOTE	10		Adam	0.001	Randomforestclassifier(n_estimators =100, random_state =2
IFOREST+SMOTE	10		Adam	0.001	Isolationforest(contamination =0.01, random state =2)
MLP+SMOTE	10	32	Adam	0.001	Dense(128,64,relu) → Dense(32,relu) →Dense (1, sigmoid)
LGBM+SMOTE					
ANN+SMOTE	10	64	Adam	0.001	ANN(64,relu) →Dense (1, sigmoid)
DCNN+SMOTE	20	64	Adam	0.001	Conv1 D (64) → Maxpool (2,1) →Conv1D (32) →Maxpool (2,1) →Flatten→Dense(64) →Dense(1,sigmoid)
LSTM+SMOTE	10	64	Adam	0.001	LSTM(64,relu)→ Dense (1, sigmoid)
PROP. DCNN-LSTM+SMOTE	20	64	Adam		Conv2 D (32, (3,1) → Conv2 D (64,(3,1) →Maxpooling2D (2,1) →Conv1D (32) →Maxpooling 2 D(2,1) →Flatten→Dense(64) →Dense(1,sigmoid) →Dropout (0.5)

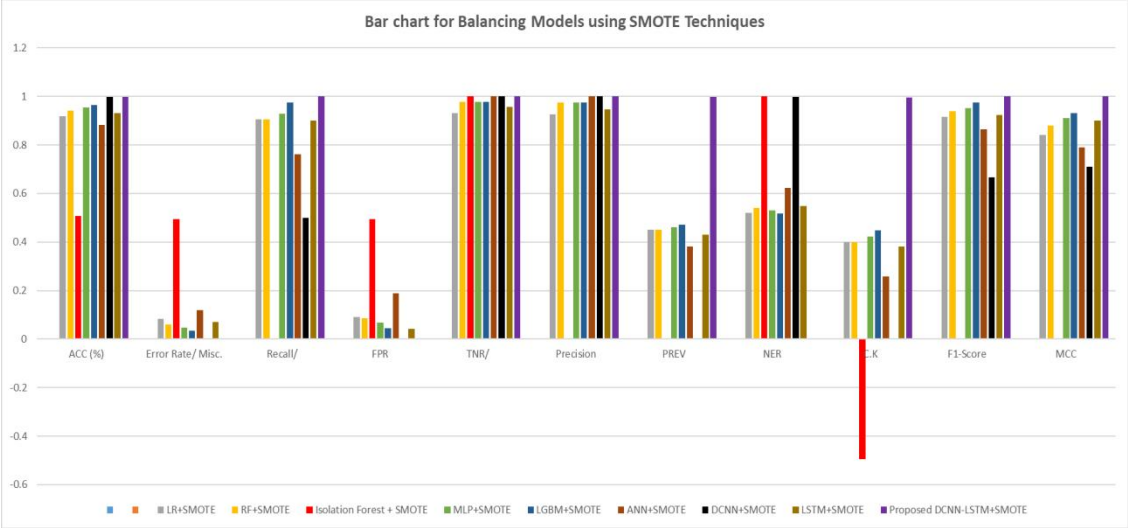

Figure 11. Bar Chat for balancing model with Validation Result Table using SMOTE Oversampling Techniques

In Figure 11 above, the models used were clearly distinguished with color separation to present details about their performances. LR+SMOTE is represented with Grey color, RF+SMOTE yellow color, Isolation Forest +SMOTE is denoted by red color, MLP+SMOTE green color, LGBM+ SMOTE blue color, ANN+SMOTE dark red color, DCNN+SMOTE black color, LSTM+SMOTE denoted with gold accent color, and propose DCNN-LSTM+SMOTE model with purple color

4.1.2.1. Accuracy Score

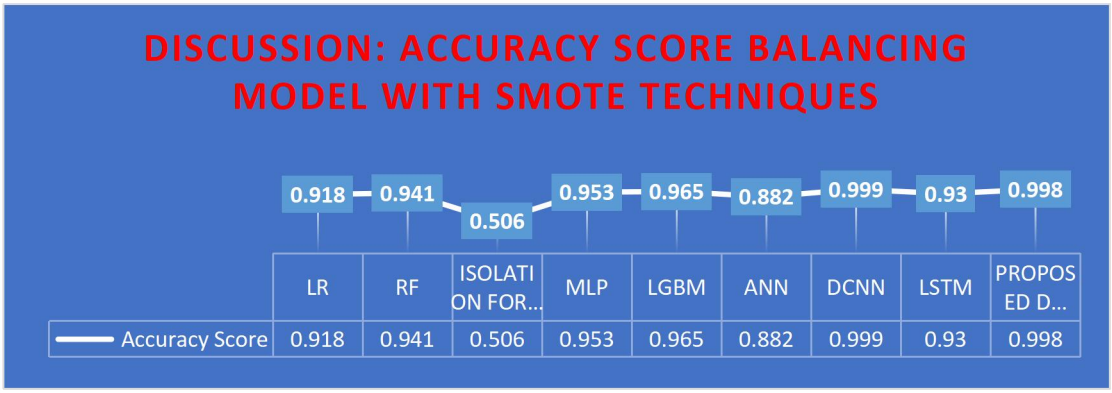

Figure 12. Accuracy Score for Balancing Model using SMOTE Techniques

From the Figure 12 and Figure 15; presented the accuracy score validation results and the Cluster Bar for Accuracy Score result with SMOTE oversampling techniques for the proposed DCNN-LSTM+SMOTE and DCNN+SMOTE model respectively; which presented an outclass recital of 99.8% and 99.9% accuracy result respectively better than the rest of the models of LGBM+SMOTE (96.5%), MLP+SMOTE (95.3%), RF+SMOTE (94.1%), LR+SMOTE (91.8%), ANN+SMOTE (88.2%). Isolation Forest+SMOTE exhibited poorest accuracy recital of (50.6%) respectively. The DCNN+SMOTE and DCNN-LSTM+SMOTE proposed presents confusion matrix and Classification reports displayed in Figure 13, while Figure 14 portrayed accuracy model and loss model plot for the DCNN-LSTM+SMOTE Model proposed. While, Figure 15 depicted for the cluster bar accuracy respectively below.

```
Confusion Matrix:
 [[995   0]
 [  1   1]]

Classification Report:
              precision    recall  f1-score   support

         0.0       1.00      1.00      1.00       995
         1.0       1.00      0.50      0.67         2

    accuracy                           1.00       997
   macro avg       1.00      0.75      0.83       997
weighted avg       1.00      1.00      1.00       997
```

Figure 13. DCNN+SMOTE Confusion Matrix and Classification Report

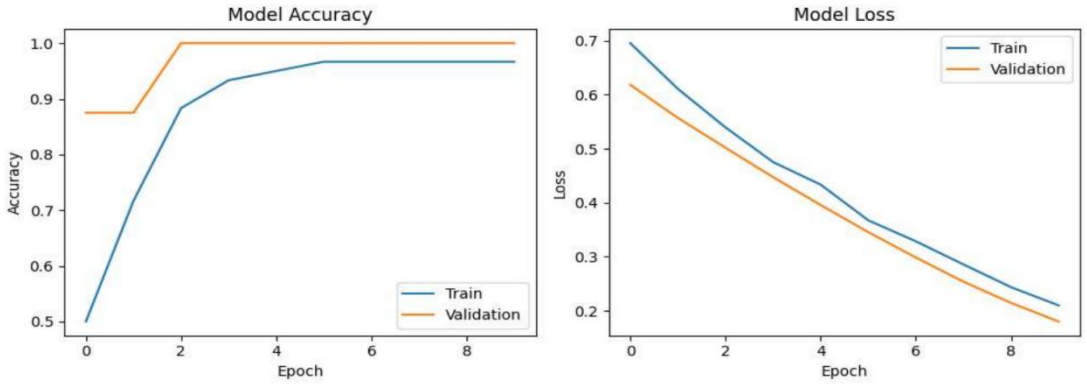

Figure 14. Accuracy Model Plot and Loss Model Plot of DCNN-LSTM+SMOTE Model

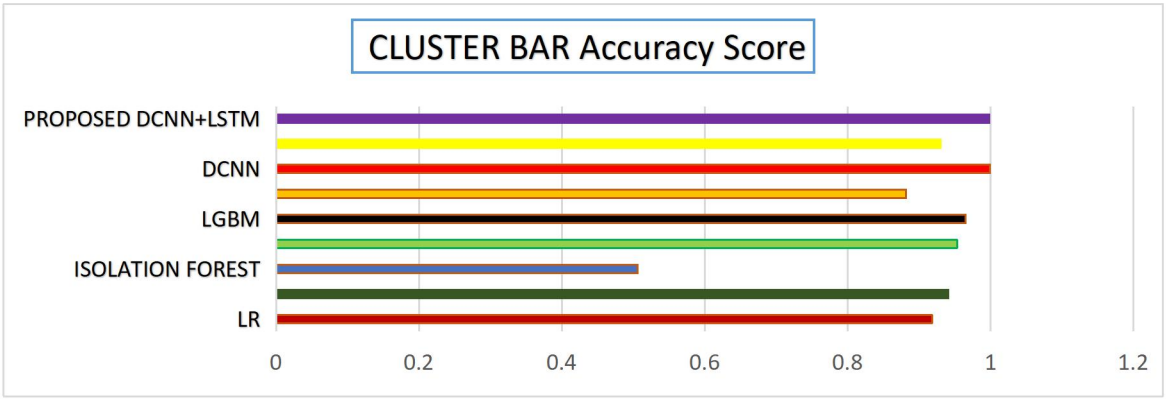

Figure 15. Cluster Bar Accuracy Score Validation Result with SMOTE oversampling Techniques

4.1.2.2. Error Rate/Misclassification

The Figure 16 presented the validation result of the proposed DCNN-LSTM+SMOTE model that presented the second best least ER of (0.2%) preceded by DCNN+SMOTE that displayed (0.1%). Isolation Forest+SMOTE offered the worst misclassification of (0.49%), with other models presenting results in preceding order ANN+SMOTE (0.12%), LR+SMOTE (0.08%), RF+SMOTE (0.06%), MLP+SMOTE (0.05%), and LGBM+SMOTE (0.04%) respectively.

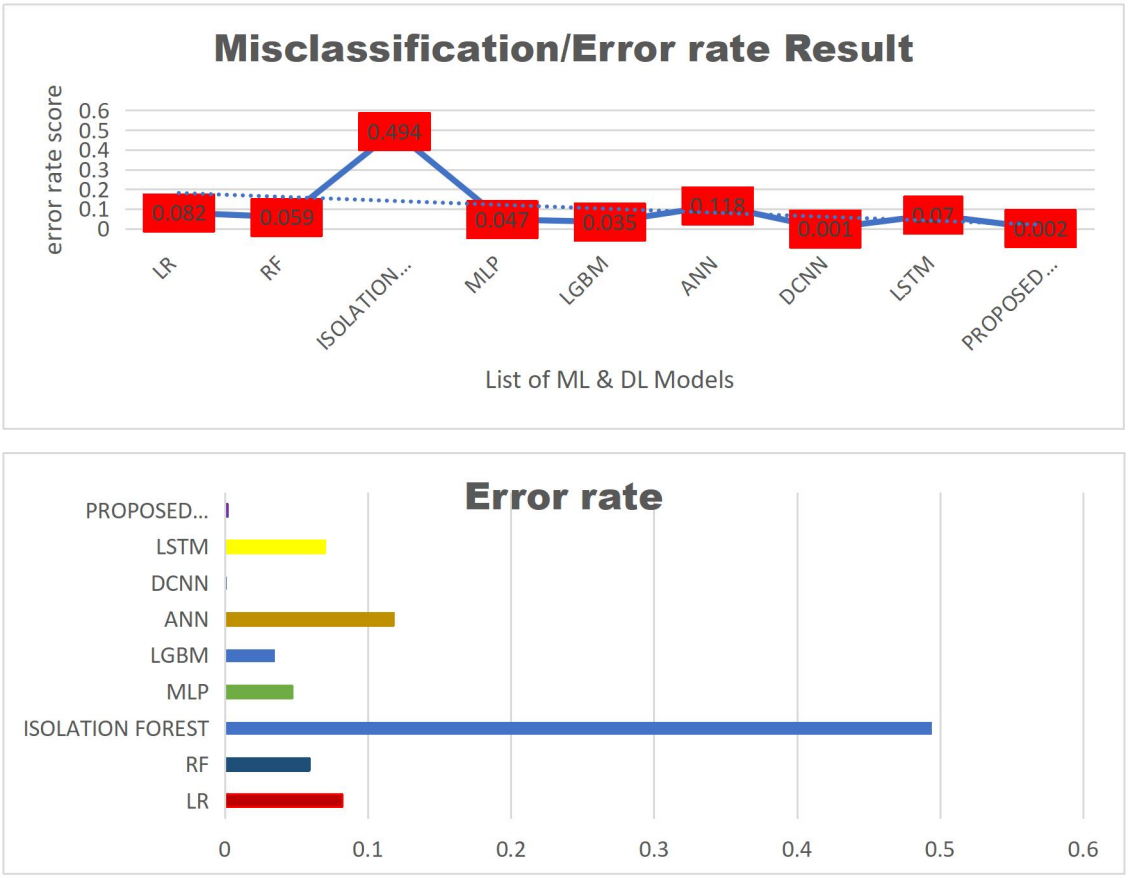

Figure 16. Misclassification or Error Rate

4.1.2.3. Recall/ Sensitivity

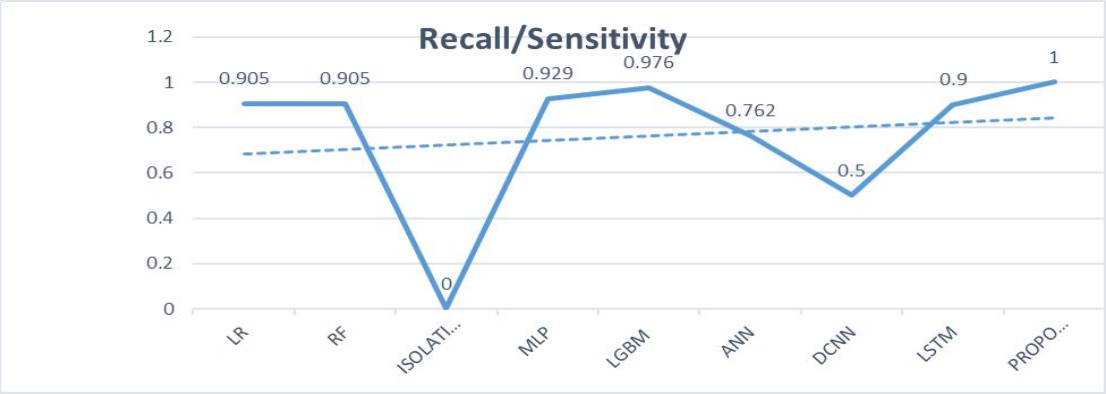

Figure 17. Recall Validation Result with SMOTE Oversampling Techniques

The proposed DCNN-LSTM+SMOTE presented the best recall performance result with (99.9%), followed by LGBM+SMOTE (97.6%), MLP+SMOTE (92.9%), and both LR+SMOTE and RF+SMOTE that presented (90.5%) distinct results. While, LSTM+SMOTE displayed (90.0%), ANN+SMOTE (76.2%), DCNN+SMOTE presented (50.0%) recall result as isolation forest presented the worst of (0.0%). The Figure 18 below displays the confusion matrix with validation results of the ANN+SMOTE model.

```
Confusion Matrix:
 [[43  0]
 [10 32]]

Classification Report:
              precision    recall  f1-score   support

         0.0       0.81      1.00      0.90        43
         1.0       1.00      0.76      0.86        42

    accuracy                           0.88        85
   macro avg       0.91      0.88      0.88        85
weighted avg       0.90      0.88      0.88        85
```

Figure 18. Confusion Matrix and validation Result of Balancing Model ANN+SMOTE Screenshot

4.1.2.4. False Positive Rate (FPR)

DCNN-LSTM+SMOTE model proposed, unveiled null (0.00%) result. While, DCNN+SMOTE generated (0.1%) in an ascending orders with rest of the model where LSTM+SMOTE displayed (4.3%), LGBM+SMOTE (4.5%), MLP+SMOTE (6.7%), RF+SMOTE (8.7%), LR+SMOTE (9.1%), and ANN+SMOTE (18.9%). Isolation forest +SMOTE was identified as model with greatest FPR result of (49.4%), and proclaimed as the worst model.

4.1.2.5 Specificity/ True Negative Rate (TNR)

It is discovered that the proposed DCNN-LSTM+SMOTE, DCNN+SMOTE, ANN+SMOTE, and Isolation forest +SMOTE models presented superclass performance of specificity results of (99.9%) respectively, closely followed by both LGBM+SMOTE and RF presenting (97.7%) distinct result. While, LSTM+SMOTE displayed (95.7%), and LR+SMOTE (93.0%) as the specificity results.

4.1.2.6 Precision

Deduced that the deep learning models of proposed DCNN-LSTM+SMOTE, DCNN+SMOTE, and ANN+SMOTE showed superclass performance of (99.9%) against other models. LGBM presented a close range result of (97.6%), MLP+SMOTE (97.5%), RF+SMOTE offers (97.4%), LSTM+SMOTE

(94.7%) each. LR+SMOTE presented (92.7%) precision result whereas Isolation forest +SMOTE displayed (0.00%) to be the worst precision result.

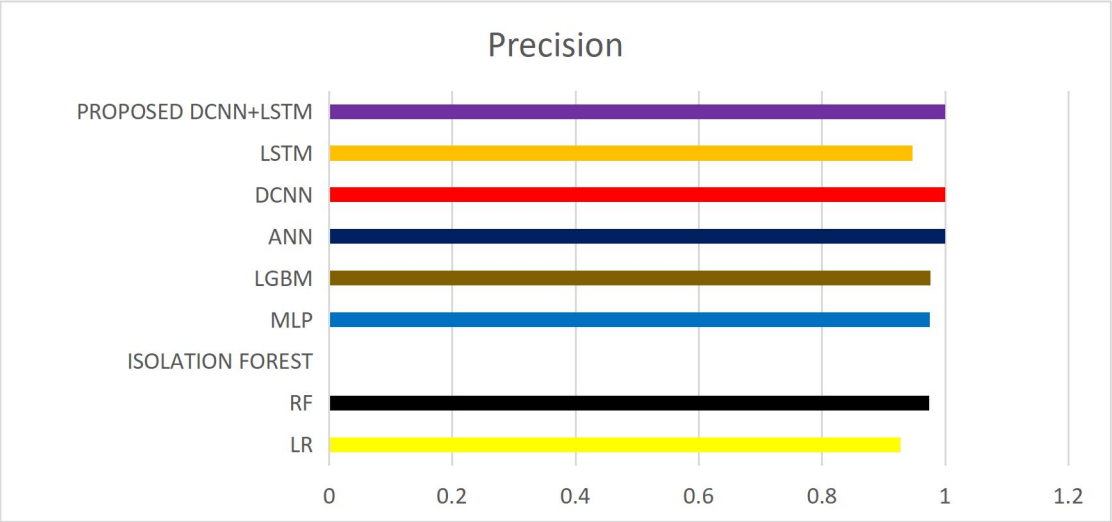

Figure 19. Precision Validation Result with SMOTE Oversampling Techniques

```
Accuracy: 0.9647058823529412
Confusion Matrix:
 [[42  1]
 [ 2 40]]
Classification Report:
              precision    recall  f1-score   support
```

olab.research.google.com/drive/1KHVYux2AIND6kLHz-fsTKtXjS

, 5:08 AM

0.0	0.95	0.98	0.97	43
1.0	0.98	0.95	0.96	42
accuracy			0.96	85
macro avg	0.97	0.96	0.96	85
weighted avg	0.96	0.96	0.96	85

Figure 20. Confusion Matrix with validation Result Balancing Model of LGBM+SMOTE

4.1.2.7. Prevalence

Isolation forest +SMOTE model presented the least prevalence result of (0.00%), followed by deep learning models of DCNN+SMOTE with (0.1%) and ANN+SMOTE (38.0%). The distinct models of LSTM+SMOTE shown (42.9%), while both LR+SMOTE and RF+SMOTE distinctly insinuates (45.0%) prevalence result; closely followed by MLP+SMOTE with (46%), LGBM+SMOTE (47.1%). The proposed DCNN-LSTM+SMOTE model offered the highest prevalence result of (99.8%) which is a surpassing outcome against other models.

4.1.2.8 Null Error Rate (NER)

The DCNN-LSTM+SMOTE model anticipated offered minimum NER outcome of (0.2%). While, Isolation Forest+SMOTE displayed the highest with (100%). The rest of the models thereof, displayed a decreasing result with DCNN+SMOTE posing (99.9%), ANN+SMOTE (62.4%), LSTM+SMOTE

(54.8%), RF+SMOTE (54.1%), MLP+SMOTE (53.0%), LR+SMOTE (52.0%) and LGBM+SMOTE (51.8%) respectively. Figure 21 shown the NER results of all the model performances.

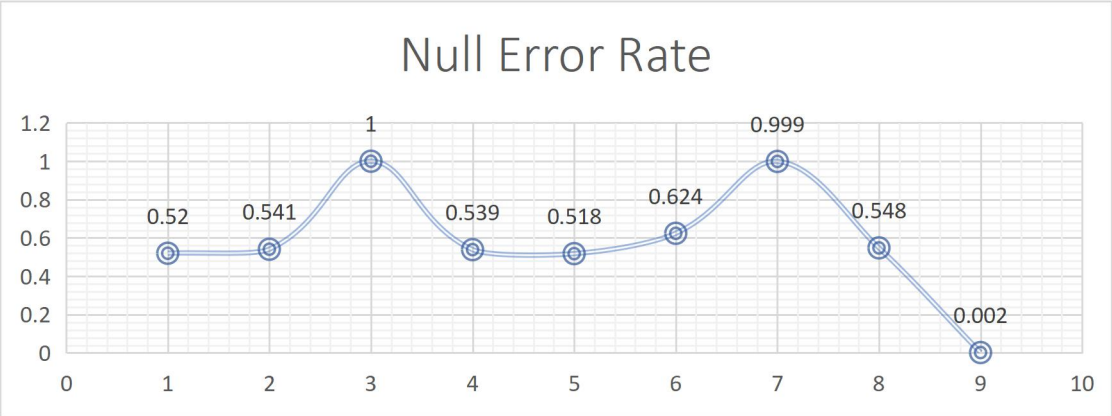

Figure 21. Null Error Rate Validation Rate with SMOTE Oversampling Techniques

```
Confusion Matrix:
 [[43  0]
 [42  0]]
Classification Report:
              precision    recall  f1-score   support

         0.0       0.51      1.00      0.67        43
         1.0       0.00      0.00      0.00        42

    accuracy                           0.51        85
   macro avg       0.25      0.50      0.34        85
weighted avg       0.26      0.51      0.34        85
```

Figure 22. Confusion Matrix with Training and Testing Balancing Model Result of Isolation Forest +SMOTE

4.1.2.9. Cohen's Kappa

Isolation forest+SMOTE offered negatively earmarks outcome of (-49.4%); that denotes a worst performance amidst all other models. The suggested DCNN-LSTM+SMOTE model demonstrated superclass performance result of (99.6%) against other models. In which, LGBM+SMOTE followed suite with distance (44.7%) in descending of MLP+SMOTE (42.3%), RF+SMOTE (40.0%), LR+SMOTE (39.8%), LSTM+SMOTE (38.3%), ANN+SMOTE (25.8%). DCNN+SMOTE model presented slightest Cohen Kappa outcome of (0.00%). The confusion matrix, and classification report and model accuracy and loss screenshot of LSTM+SMOTE is presented in Figure23 and Figure 24 below.

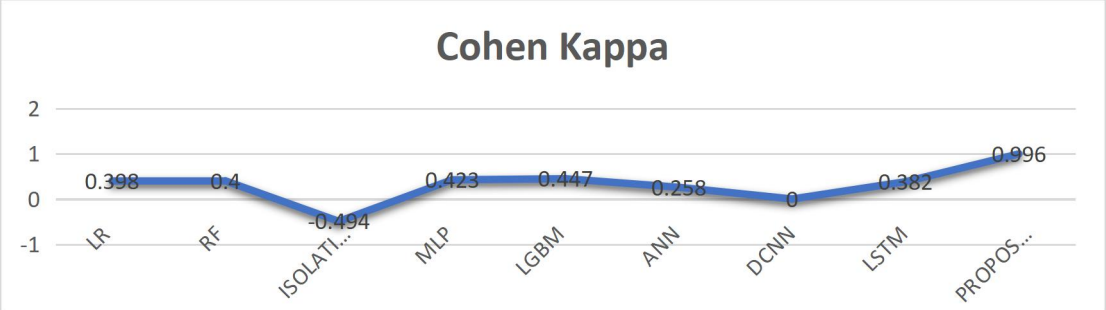

Figure 23. Cohen Kappa Validation Results with SMOTE Oversampling Techniques

```
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
```

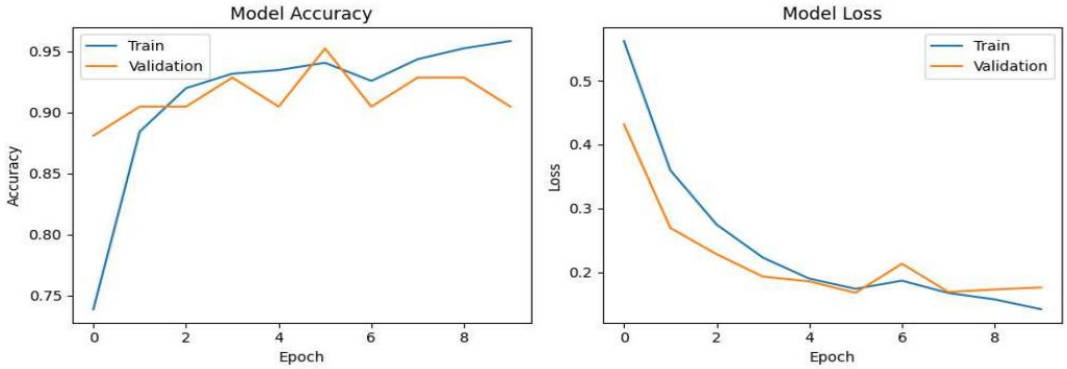

Figure 24. Confusion Matrix, Classification Report and Model Accuracy and Loss of LSTM+SMOTE

4.1.2.10. F1-Scores

Here, the DCNN-LSTM+SMOTE model generated the utmost performance evaluation outcome of (99.9%), closely followed by LGBM+SMOTE (97.6%), MLP+SMOTE (95.2%), RF+SMOTE (93.8%), LSTM+SMOTE (92.3%), LR+SMOTE (91.8%), ANN+SMOTE (86.5%), DCNN+SMOTE (66.7%), and Isolation Forest+SMOTE (0.00%) respectively. Here, Isolation Forest +SMOTE is denounced as the worst performance models. This is presented in Figure 25 below.

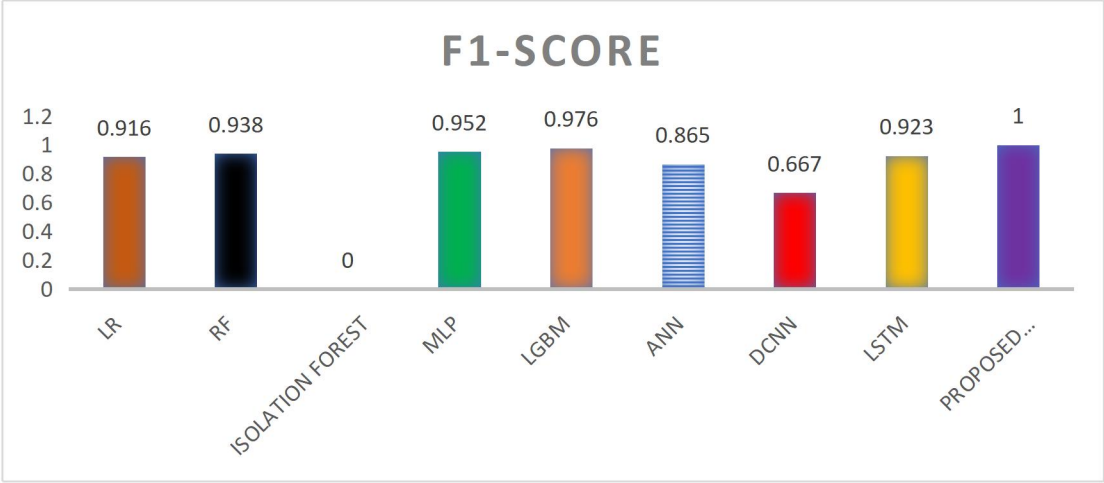

Figure 25. F1-SCORE validation Result with SMOTE Oversampling Techniques

4.1.2.11. Mathews Correlation Coefficient (MCC)

Using the MCC evaluation metric as introduced in [83] study. It is deduced that the recommend DCNN-LSTM+SMOTE model offered perfect forecasting results; with outshine performance of 100%, followed in close range with LGBM+SMOTE (0.93%), MLP+SMOTE (0.91%), LSTM+SMOTE (0.90%), RF+SMOTE (0.88%), LR+SMOTE (0.84%), ANN+SMOTE (0.79%), DCNN+SMOTE (0.71%) that indicates relative good predictions and Isolation Forest+SMOTE (0.00%) ascribed worst

performing models offering random prediction (no better than flipping a coin). The diagrammatic representation in shown in Figure 26 below.

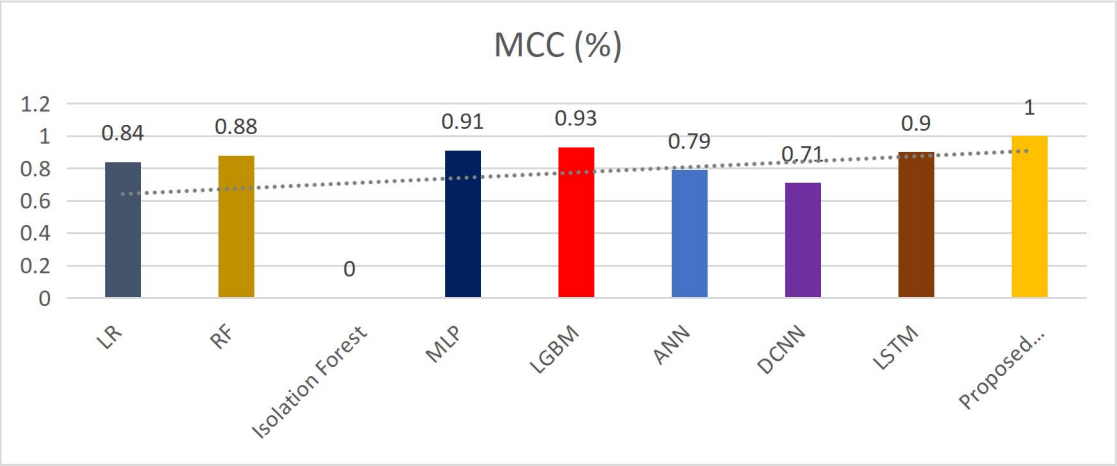

Figure 26. Bar chart for validation result of MCC using SMOTE

4.1.3. Comparisons with Benchmark Study

This research results are used in comparison with the study of [67,3,5,50], that fails to explore any resampling or data augmentation techniques to balance the dataset employed in their study. Their result suffers from over-fitting and under-fitting challenges. This [20] proposed to address using an ensemble approach for superseding result while delving SMOTE oversampling and under-sampling techniques using only ML models.

Besides, [20] follows suites and deploys more ML models with better results. This study approach is novel in its application to credit card fraud detection and could competes with other bench mark study as the result is optimal and serves as a potential solution to the challenges of credit card fraud.

Table 7. Benchmark Comparison of Proposed DCNN-LSTM+SMOTE with existing studies

Author	Models utilized/ proposed	Per. Evaluation metrics	Results
[67]	2 ML models of LR and Isolation Forest LR was proposed	Accuracy Score, Precision, Recall, F1-Scores, AUC-ROC Logistics Regression Training Results: ACC, Score = 99.91%, Logistics Regression Testing Results: ACC Score =78%, Precision = 0.95, Recall = 0.56 and F1-Score = 0.70 respectively. Isolation Forest Training Results: ACC Score =99.82% Isolation Forest Testing Results: ACC Score =74%, Precision = 0.49, Recall = 0.49 and F1-Score = 0.49 respectively	Logistic Regression algorithm out-performed isolation forest algorithm.
[20]	Ensemble model (PM) that integrates a SVM , KNN, RF, Bagging, and	Accuracy Score = 99.95%, Precision = 99.95%, Recall = 99.95%, and F1-	The PM (SMOTE) technique demonstrated superior performance, exhibiting the greatest levels of accuracy, precision, and F1 score.

	Boosting classifiers (PM1, PM2). Algorithms were used.	Score =99.95%. Computational Time Efficiency is consider in this study.	
[50]	6ML models of Logistic regression, Extra trees, Random forest, XGB, LGBM and CatBoost Different Dataset is used in this study.	Accuracy Score = 100%, Recall =100%, F1-score= 100% All the models perform excellently. However, Training time comparison Models is used to established their findings. Logistic regression 4.1302; Extra trees 58.0004; Random forest 456.0544; XGB 328.2394; LGBM 7.9552; and CatBoost 75.5760	Both LR and LightGBM provide amazing efficiency, as their training times are on the scale of seconds.
[5]	LR, RF, Iforst, MLP, LGBM, ANN. DCNN+SMOTE proposed	Eleven parameters of accuracy, ER, recall, FPR,TNR, Prev., NER, F1-score, MCC were adopted	DCNN+SMOTE presented overwhelming superclass performance across board, 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.
PROPOSED DCNN-LSTM+SMOTE	4ML Models of RF, LR, Isolation forest, LGBM and 4 DL Models of ANN, MLP, DCNN, LSTM and proposed hybrid DCNN-LSTM+ SMOTE	Accuracy Score = 99.8%, Error rate = 0.2 %, Recall = 99.9%, Precision =99.9%, NER= 0.2% , Cohen Kappa = 99.6% and F1-score =99.9%	DCNN-LSTM+SMOTE was the best model with superclass performances across other evaluation metrics delved for this study. and can contend fraudulent payment card transaction.

In Table 7, most of the scholars performs comparative analysis study either using machine or deep learning models and ensemble or hybrid methods to classified credit card transactions in financial institutions. The study of [50]; is helpful for novice researchers to understand the performance of the ML models for fraudulent transaction detections using a public dataset. While their future work sues for the evaluation of these ML models using multiple datasets for more resounding results. Also, the scholar advises for the application of deep learning models for credit card fraud detection using the same dataset, along with other datasets, to compare the performance of machine learning and deep learning models; these this thesis work accomplished with the propose enhance hybrid deep learning models of DCNN-LSTM+SMOTE. However, this study, does not considered training time efficiency in establishing the results unlike [20,50] distinct studies.

The performance differences between models (e.g., DCNN-LSTM+SMOTE vs. DCNN+SMOTE in Table 7) are not statistically validated. Statistical tests (e.g., t-test, ANOVA) is not consider to ratify significance, as predated studies does not applied it.

5. CONCLUSION AND RECOMMENDATION

In today's digitalized financial transaction compelling world, credit card fraud as become a bone of contention distressing the financial dealings of both organization and individuals; rendering huge financial losses with many other implication. This is forcing financial institutions, Card issuers and fraud experts to invest time and finances in developing more sophisticated fraud prevention and detection models with policies for abatement proceedings that could revels, repels and moderate inferences of the payment fraud. This study aimed for improvement on influence-predated study's findings. That identifies major gaps, hampering the abatement of the unceasing act of payment frauds. These was center on the understated:

i. Inaccessibility of complete and real life credit card dataset; as they are private properties and neither financial institutions nor card users (individuals) wishes to divulge and releases such records, leading to unfitting and under trained system.
ii. Lack of single and potent fraud prevention models which can execute unfailingly in all settings while outperforming all other models.
iii. Nonexistence of good and efficient evaluation metrics that cannot only describe the accuracy of the system and as well gives a better comparative outcome amidst dissimilar methods.
iv. Lack of competence on system to adjust itself efficiently to changing setting of fraudulent scheme and honest changes in procurement habit of a customer.
v. High dimensionality and sparsity challenge rate in datasets available on open sources repository; due to large numbers of features column.

This study proposed DCNN-LSTM+SMOTE as a solution to mitigate the inferences of credit card fraud. Emphatically, this model performed well across seven model out of eleven-performance evaluation metrics exploit. These affirms the model as an ideal approach for the detection of fraudulent transactions in financial institution. This answered the model effectiveness raised question in Q2 under section 1. It is advise that financial institution should adopt a more upbeat and not reactive counter measures approach in shielding their customer against frauds; as fraudster indulges in diverse overthrow measure for circumventing fraud abatement methods. For imminent study, more improved crossbreed approach of either ML or DL approaches is advocated towards detection of payment card fraud in financial institutions as they tend to present good predictive results than conventional machine learning models.

Funding Statement: The authors confirm that no external funding was received for the conduct of this research or the preparation of this manuscript.

Contribution: The authors have read and agreed to the published version of the manuscript.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data supporting the findings of this study are available upon reasonable request from the first and corresponding author.

Conflict of Interest Statement: In this study, no conflicts of interest is pronounced; as all authors agreed to its submission

REFERENCES

1. Hayes, A., Anderson, S., & Kvilhaug, S. C. (2023). *What is a financial institution?* Investopedia. https://www.investopedia.com/terms/f/financialinstitution.asp
2. Horton, M. (2023, September 19). *Different types of financial institutions*. Investopedia. https://www.investopedia.com/ask/answer/061615/what-are-major-categories-financial-institutions-and-what-are-their-primary-role.asp
3. Salaudeen, L. G., Gabi, D., Muhammad, G., & Suru, H. U. (2024a). Light gradient boosting machine (LGBM) for credit card fraud detection in financial institution. *Direct Research Journal*

of Engineering and Information Technology, 12(1), 19-34. https://doi.org/10.26765/DRJEIT17933661

4. Aggarwal, S. (2024, January). *Financial institution: Types, roles and advantages*. https://www.shiksha.com/online-course/articles/financial-institutions-types-roles-and-advantages
5. Salaudeen, L. G., Gabi, D., Muhammad, G., & Suru, H. U. (2024b). Deep convolutional neural network (DCNN) based synthetic minority oversampling techniques: A forfending model for fraudulent credit card transactions in financial institution. *Journal of Nigerian Society of Physical Sciences (NSPS)*. https://doi.org/10.46481/jnsps.2024.2037
6. Al-Smadi, B. (2021). *Credit card security system and fraud detection algorithm* [Doctoral dissertation, Louisiana Tech University]. https://digitalcommons.latech.edu/dissertations/1947
7. Ayorinde, K. (2021). *A methodology for detecting credit card fraud* [Master's thesis, Minnesota State University]. Cornerstone.
8. Zaman, S. I., Khan, A. S., & Gupta, H. (2023). How digitalization in banking improves service supply chain resilience of e-commerce sector? A technological adoption model approach. *Operations Management Research, 16*, 904-930. https://doi.org/10.1007/s12063-023-00378-9
9. Kewei, X., Peng, B., Jiang, Y., & Lu, T. (2021). A hybrid deep learning model for online fraud detection. *2021 IEEE International Conference on Consumer Electronics and Computer Engineering* (pp. 431-434). IEEE. https://doi.org/10.1109/ICCECE51280.2021.9342401
10. Emejo, J. (2023, March 20). *Cashless policy as economic enabler*. This Day. https://www.thisdaylive.com/index.php/2023/03/20/cashless-policy-economic-enabler
11. Mienye, I. D., & Sun, Y. (2023). A deep learning ensemble with data resampling for credit card fraud detection. *IEEE Access, 11*, 30628-30638. https://doi.org/10.1109/ACCESS.2023.3262020
12. Kolawole, O. (2022, December 9). *What Sweden and India can teach Nigeria about cashless economy?* Techpoint Africa. https://techpoint.africa/2022/12/09/lesson-sweden-indian-nigeria-cashless/
13. Alraddadi, A. (2023). A survey and a credit card fraud detection and prevention model using the decision tree algorithm. *Engineering, Technology & Applied Science Research, 13*(4), 11505-11510. http://www.etasr.com/
14. Fayyomi, A. M., Eleniyan, D., & Eleniyan, A. (2021). A survey paper on credit card fraud detection techniques. *International Journal of Scientific & Technology Research, 10*(9), 72-79. http://www.ijstr.org/
15. Malik, E. F., Khaw, K. W., Belaton, B., Wong, W. P., & Chew, X. (2022). Credit card fraud detection using a new hybrid machine learning architecture. *Mathematics, 10*(9), 1480. https://doi.org/10.3390/math10091480
16. Sarwade, S. (2023, May 12). *Anomaly detection in credit card fraud*. Analytics Vidhya. https://www.analyticsvidhya.com/blog/2023/05/anomaly-detection-in-credit-card-fraud/
17. Jendruszak, B. (2023, July 14). *Credit card fraud detection: The guide*. SEON. https://seon.io/resources/credit-card-fraud-detection/
18. Hagos, K. (2018). *SIMBox fraud detection using data mining techniques: The case of Ethio Telecom* [Master's thesis, Addis Ababa University].
19. Naik, J., & Laxminarayana, J. (2017). Designing hybrid model for fraud detection in insurance. *IOSR Journal of Computer Engineering, 19*(3), 24-30. https://www.iosrjournals.org
20. Khalid, A. R., Owoh, N., Uthmani, O., Ashawa, M., Osamor, J., & Adejoh, J. (2024). Enhancing credit card fraud detection: An ensemble machine learning approach. *Big Data and Cognitive Computing, 8*(1), 6. https://doi.org/10.3390/bdcc8010006
21. Nguyen, T. T., Tahir, H., Abdelrazek, M., & Babar, A. (2024). Deep learning method for credit card fraud detection. *arXiv*. https://arxiv.org/abs/2012.03754
22. Boesch, G. (2023). *The most popular deep learning software in 2023*. Viso.ai. https://viso.ai/deep-learning/deep-learning-software/
23. White, A. (2023, June 6). *Here's how credit card fraud happens and tips to protect yourself*. CNBC. https://www.cnbc.com/select/credit-card-fraud/
24. Shakya, R. (2018). *Application of machine learning techniques in credit card fraud detection* [Master's thesis, University of Nevada]. https://digitalscholarship.unlv.edu/thesesdissertations/3454

25. Alfaiz, N. S., & Fati, S. M. (2022). Enhanced model using machine learning. *Electronics, 11*(4), 662. https://doi.org/10.3390/electronics11040662
26. Mosavi, A., Ardabili, S., & Várkonyi-Kóczy, A. R. (2020). List of deep learning models. In *Inter-Academia 2019* (pp. 202-214). Springer. https://doi.org/10.1007/978-3-030-36841-8_20
27. Jovel, J., & Greiner, R. (2021). An introduction to machine learning approach for biomedical research. *Frontiers in Medicine*. https://doi.org/10.3389/fmed.2021.771607
28. Lisalab. (n.d.). *Deep learning tutorial*. https://github.com/lisalab/DeepLearningTutorials
29. Chouiekh, A., & El Haj, E. I. (2018). ConvNets for fraud detection analysis. *Procedia Computer Science, 127*, 133-138. https://doi.org/10.1016/j.procs.2018.01.113
30. Aggarwal, C. C. (2018). *Neural networks and deep learning*. Springer. https://doi.org/10.1007/978-3-319-94463-0
31. Brownlee, J. (2019, November 11). *14 different types of learning in machine learning*. Machine Learning Mastery. https://machinelearningmastery.com/types-of-learning-in-machine-learning/
32. Dugga, N. (2023, March 7). *Top 10 machine learning applications and examples in 2023*. Simplilearn. https://www.simplilearn.com/tutorials/machine-learning-tutorial/machine-learning-applications
33. Hassan, P. (2016, December 17). *Artificial learning, machine learning and deep learning: Know the difference*. Systweak Blogs. https://blogs.systweak.com/artificial-learning-machine-learning-and-deep-learning-know-the-difference/
34. Lu, S., & Li, R. (2021). DAC: Deep auto-encoder-based clustering, a general deep learning framework of representation learning. *arXiv*. https://arxiv.org/abs/2102.07472
35. Sheshasaayee, A., & Thomas, S. S. (2017). A study of hybrid learning methodologies in insurance fraud detection techniques. *International Journal of Engineering Research, 3*(8), 178-181.
36. Ahmad, I., et al. (2022). Metastatic cancer detection using hybrid deep learning model. *Journal of Medical Imaging*. https://www.metalisticcancerdetection
37. Lilhore, U. K., Dalal, S., Faujdar, N., et al. (2023). Hybrid CNN-LSTM model with efficient hyper-parameter tuning for prediction of Parkinson's disease. *Scientific Reports, 13*, 14605. https://doi.org/10.1038/s41598-023-41314-y
38. Chieregato, M., Frangiamore, F., Morassi, M., et al. (2022). A hybrid machine learning/deep learning COVID-19 severity predictive model from CT images and clinical data. *Scientific Reports, 12*(1), 4329. https://doi.org/10.1038/s41598-022-07890-1
39. Oikonomidis, A., Catal, C., & Kassahun, A. (2022). Hybrid deep learning-based models for crop yield prediction. *Applied Artificial Intelligence, 36*(1), 2031822. https://doi.org/10.1080/08839514.2022.2031823
40. Yang, R., Singh, S. K., Tavakkoli, M., et al. (2020). CNN-LSTM deep learning architecture for computer-vision based model frequency detection. *Mechanical Systems and Signal Processing, 136*, 106677. https://doi.org/10.1016/j.ymssp.2019.106677
41. He, Y., Liu, Y., Shao, S., et al. (2019). Application of CNN-LSTM in gradual changing fault diagnosis of rod pumping system. *Mathematical Problems in Engineering, 2019*, 4203821. https://doi.org/10.1155/2019/4203821
42. Deussom-Djomadji, E. M., Basile, K. I., Christian, T. T., et al. (2023). Machine learning-based approach for identification of SIM Box Bypass fraud in a Telecom Network based on CDR analysis. *Journal of Computer and Communications, 11*(2), 142-157. https://doi.org/10.4236/jcc.2023.112010
43. Deussom-Djomadji, E. M., Matemtsap Mbou, B., Tchagna Kouanou, A., et al. (2022). Machine learning-based approach for designing and implementing a collaborative fraud detection model through CDR and traffic analysis. *Transactions on Machine Learning and Artificial Intelligence, 10*, 46-58. https://doi.org/10.14738/tmlai.104.12854
44. Hassan, M. M., Gumaei, A., Alsanad, A., et al. (2020). A hybrid deep learning model for efficient intrusion detection in big data environment. *Information Sciences, 513*, 386-396. https://doi.org/10.1016/j.ins.2019.10.069
45. Vinayakumar, R., Alazab, M., Soman, K. P., et al. (2019). Deep learning approach for intelligent intrusion detection system. *IEEE Access, 7*, 41525-41550. https://doi.org/10.1109/ACCESS.2019.2895334

46. Kim, J., Kim, J., Kim, H., et al. (2020). CNN-based network intrusion detection against denial-of-service attacks. *Electronics, 9*(6), 916. https://doi.org/10.3390/electronics9060916
47. LinkedIn. (2023, November 6). *How you can address class imbalance in binary classification task?* https://www.linkedin.com/advice/0/how-can-you-address-class-imbalance-binary-classification-yxkve
48. Gao, J. (2020). *Data augmentation in solving data imbalance problems* [Master's thesis, KTH Royal Institute of Technology]. https://www.kth.se/polopoly_fs/1.968123!/DataAugmentation.pdf
49. Great Learning Team. (2023). *Credit card fraud detection*. https://www.mygreatlearning.com/blog/credit-card-fraud-detection/
50. Aslam, A., & Hussain, A. (2024). A performance analysis of machine learning techniques for credit card fraud detection. *Journal on Artificial Intelligence*. https://doi.org/10.32604/JAI.2024.047226
51. Cortes, D. (2019). *An introduction to isolation forest*. https://cran.r-project.org/web/packages/isotree/vignettes/An_introduction_to_isolation_forest.html
52. Aghware, F. O., Yoro, R. E., Ejeh, P. O., et al. (2023). DeLClustE: Protecting users from credit-card fraud transaction via the deep-learning cluster ensemble. *International Journal of Advanced Computer Science and Applications, 14*(6), 94-100. https://doi.org/10.14569/IJACSA.2023.0140611
53. Baker, M. R., Mahmood, Z. N., & Shaker, E. H. (2022). Ensemble learning with supervised machine learning models to predict credit card fraud transactions. *Revue d'Intelligence Artificielle, 36*(4), 509-518. https://doi.org/10.18280/ria.360410
54. Zoho Books Team. (2024, April 4). *Online payment fraud 101: What it is, types, and how to prevent it*. https://www.zoho.com/books/academy/banking-and-payments/payment-fraud.html
55. 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 & Technology, 8*(9), 110-115. www.ijert.org
56. White, A. (2023, June 6). *Here's how credit card fraud happens and tips to protect yourself*. CNBC. https://www.cnbc.com/select/credit-card-fraud/
57. Natasha, G. (2022, April 19). *Credit and debit card market share by network and issuer*. The Motley Fool. https://www.fool.com
58. International Public Sector Fraud Forum. (2020, February). *Guide to understanding the total impact of fraud*. UK Cabinet Office. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/778306/GuideToUnderstandingTheTotalImpactOfFraud.pdf
59. Shah, A., & Makwana, Y. (2023). *Credit card fraud detection*. ResearchGate. https://www.researchgate.net/publication/369857378_Credit_Card_Fraud_Detection
60. Singh, S., Ninje, H., Ajinkya, F., & Neware, R. (2024). Credit card fraud detection using a hybrid machine learning algorithm. *Preprints*. https://doi.org/10.20944/preprint2024021206.v1
61. Noviandy, R. T., Idroes, G. M., Maulana, A., et al. (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). https://heca-analitika.com/ijm
62. Ting, K. M., & Zhou, G.-T. (n.d.). *Isolation forest*. [Unpublished manuscript].
63. Cheng, C., Kao, Y., & Lin, H. (2021). A financial statement fraud model based on synthesized attribute selection and a dataset with missing values and imbalanced classes. *Applied Soft Computing, 108*, 107487. https://doi.org/10.1016/j.asoc.2021.107487
64. Forough, J., & Montazi, S. (2021). Ensemble of deep sequential models for credit card fraud detection. *Applied Soft Computing, 99*, 106883. https://doi.org/10.1016/j.asoc.2020.106883
65. Ding, Y., Kang, W., Feng, J., et al. (2023). Credit card fraud detection based on improved variational autoencoder generative adversarial network. *IEEE Access, 11*, 83680-83691. https://doi.org/10.1109/ACCESS.2023.3302339
66. Cheon, M. J., Lee, D. H., Joo, S. H., & Lee, O. (2021). Deep learning based hybrid approach of detecting fraudulent transactions. *Journal of Theoretical and Applied Information Technology, 99*(16), 4044-4054. http://www.jatit.org/

67. Akinola, K. E., Aina, D. A., Oyede, O., & Braimoh, J. A. (2023). Credit card fraud detection using logistics regression and isolation forest algorithm. *UNIZIK Journal of Engineering and Applied Sciences, 2*(1), 187-195. https://journals.unizik.edu.ng/index.php/ujeas
68. Madhavi, M., Reddy, K. R. V., Swetha, B., & Kumar, R. B. (2023). Credit card fraud detection using CNN. *International Journal of Research Trends and Innovation, 8*(4), 845-854. www.ijrti.org
69. Prasad, P. Y., Chowdary, A. S., Bavitha, C., et al. (2023). A comparison study of fraud detection in usage of credit cards using machine learning. *2023 7th International Conference on Trends in Electronics and Informatics* (pp. 1204-1209). IEEE. https://doi.org/10.1109/ICOEI56765.2023.10125710
70. Huang, H., Liu, B., Xue, X., et al. (2024). Imbalance credit card fraud detection data: A solution based on hybrid neural network and clustering-based under-sampling technique. *Applied Soft Computing, 154*, 111368. https://doi.org/10.1016/j.asoc.2024.111368
71. Devi, R. R., & Parthibranjanray. (2023). Credit card fraud detection using AI/ML/CNN. *Iconic Research and Engineering Journals, 6*(9), 242-249. https://doi.org/10.5281/zenodo.8225678
72. Vaishnave, J. (2019). Credit card fraud detection using random forest algorithm. *International Journal of Advance Research, Ideas and Innovations in Technology, 5*(2). www.ijariit.com
73. Zhang, A., Lipton, Z. C., Li, M., & Smola, A. J. (2022). *Dive into deep learning*. https://d2l.ai/
74. GeeksforGeeks. (2024, March 14). *Introduction to convolutional neural network*. https://www.geeksforgeeks.org/introduction-convolution-neural-network/
75. Gavrilova, Y. (2021, August 3). *Introduction to convolutional neural network*. Serokell. https://serokell.io/blog/introduction-to-convolutional-neural-network
76. Zonyfar, C., Lee, B., & Kim, J. (2023). HCNN-LSTM: Hybrid convolutional neural network with long short-term memory integrated for legitimate web prediction. *Journal of Web Engineering*. https://doi.org/10.13052/jwe1540-9589.2251
77. Carrasco, R., San, M., Urban, M., & Sicilia, A. (2020). Evaluation of deep neural networks for reduction of credit card fraud alerts. *IEEE Access, 8*, 186421-186432. https://doi.org/10.1109/ACCESS.2020.3026222
78. Choi, J. Y., & Lee, B. (2018). Combining LSTM network ensemble via adaptive weighting for improved time series forecasting. *Mathematical Problems in Engineering, 2018*, 2470171. https://doi.org/10.1155/2018/2470171
79. Siami-Namini, S., Tavakoli, N., & Siami Namin, A. (2019). The performance of LSTM and Bi-LSTM in forecasting time series. *2019 IEEE International Conference on Big Data* (pp. 3285-3292). IEEE. https://doi.org/10.1109/BigData47090.2019.9005997
80. Wang, G., Kang, W., Wu, Q., et al. (2018). Generative adversarial network (GAN) based data augmentation for palmprint recognition. *2018 Digital Image Computing: Techniques and Applications* (pp. 1-7). IEEE. https://doi.org/10.1109/DICTA.2018.8615798
81. Shang, L., Zhang, Z., Jang, F., et al. (2023). CNN-LSTM hybrid model to promote signal processing of ultrasonic guided Lamb waves for damage detection in metallic pipelines. *Sensors, 23*(16), 7059. https://doi.org/10.3390/s23167059
82. Warghade, S., Desai, S., & Patil, V. (2020). Credit card fraud detection from imbalanced dataset using machine learning algorithm. *International Journal of Computer Trends and Technology, 68*(3), 22-28. https://doi.org/10.14445/22312803/IJCTT-V68I3P105
83. Comotto, F. (2022, January 8). *Evaluation metric: Leave your comfort zone and try MCC and Brier score*. Towards Data Science. https://towardsdatascience.com/evaluation-metric-leave-your-comfort-zone-and-try-mcc-and-brier-score-4dbf6ce5f9e6