ISSN No:-2456-2165

A Deep Neuro-Adaptive Synthetic Model for the Detection of E-Commerce Fraud Transactions

[1]Abubakar Babayo Munkaila
Department of Mathematical Sciences
Abubakar Tafawa Balewa University
Bauchi, Nigeria

[2]Abdulsalam Ya'u Gital
Department of Mathematical Sciences
Abubakar Tafawa Balewa University
Bauchi, Nigeria

[3]A. M. Kwami
Department of Mathematical Sciences
Abubakar Tafawa Balewa University
Bauchi, Nigeria

[4]Ramson Emmanuel Nannim
Department of Mathematical Sciences
Abubakar Tafawa Balewa University
Bauchi, Nigeria

[5]Mustapha Abdulrahman Lawal
Department of Mathematical Sciences
Abubakar Tafawa Balewa University
Bauchi, Nigeria

[6]Ismail Zahraddeen Yakubu
Department of Computing Technologies
SRM Institute of Science and Technology
Kattankulathur, Chennai, India

Abstract:- Fraud detection is a critical aspect of safeguarding financial systems and online transactions. Traditional methods often face challenges in handling imbalanced datasets, where fraudulent instances are significantly outnumbered by legitimate transactions. This research explores the effectiveness of combining deep learning methods with Adaptive Synthetic Sampling (ADASYN) to improve the performance of fraud detection models. Experimentation on python shows that the proposed DNN with ADASYN model achieved the best and highest classification accuracy of 97.8% as against the existing algorithm including DT with SMOTE which achieved 91%, NB with SMOTE which achieved 95% and RF with SMOTE which achieved 95% respectively. thus, from the experiment, it is noticed that addressing data class imbalance using techniques like ADASYN and SMOTE can positively impact fraud detection accuracy by mitigating the challenges posed by imbalanced datasets. The successful development of the proposed method has extended the detection accuracy, precision, recall and F-score of the methods compared to other classical machine learning methods. Thus, this enhances the effective fraud detection system for e-commerce security and trustworthiness of the platform protect users from fraudulent activities, reduce financial losses, and preserve the platform's reputation.

Keywords:- *Deep Neural Network; Feature Extraction; Machine Learning; Fraud Detection, ADASYN.*

I. INTRODUCTION

Overly aggressive fraud detection can lead to false positives, user frustration, and lost revenue [1]. The fraud detection dataset typically contains a high volume of legitimate transactions and a relatively small number of fraudulent ones, leading to class imbalance. Therefore, ensuring the model can effectively detect rare fraudulent events while not overwhelming the system with false alarms is a challenge [2]. Additionally, fraudsters continuously adapt and employ new techniques, necessitating a system that can learn and adapt to emerging threats in real time. However, the traditional machine-learning algorithm (Decision Tree, Naïve Bayes, Random Forest, and Neural Network) used in the existing study [3] do not offer gain particularly when dealing with complex and high-dimensional data. Whereas, deep learning models, especially deep neural networks, are capable of automatically learning and extracting intricate patterns and features from raw data [4]. This can be particularly beneficial in fraud detection, where fraudsters often employ sophisticated and non-linear strategies that are challenging to capture using handcrafted features. Therefore, balancing fraud detection accuracy with the need to provide a frictionless and enjoyable shopping experience for legitimate users with deep neural networks is a critical task that is explored in this research.

While SMOTE (Synthetic Minority Over-sampling Technique) as used in the existing study [3] is an effective method for addressing the class imbalance in machine learning [5], it does have some drawbacks and limitations such as sensitivity to noise, overfitting, information loss, Inability to Address Intra-Class Imbalance, Difficulty Handling Class Proximity, Lack of Adaptation and Computational cost [6]. To address these drawbacks, ADASYN is an extension of SMOTE that adaptively generates synthetic samples by focusing on the instances that

are more challenging to classify correctly [7]. It assigns higher weights to minority class instances that are difficult to learn, potentially addressing the issue of over-sampling in safe regions.

As suggested by the baseline author [3], it is expected to be able to use other algorithms or deep learning for fraud detection in e-commerce and other future study to improve neural network accuracy when using advance Sampling Technique.

The aim of this research is to develop and implement a deep neural network model that can effectively identify fraudulent transactions and activities on the E-commerce platform using ADASYN (Adaptive Synthetic Sampling) and Deep Neural Network (DNN) for fraud detection that can respond swiftly to emerging threats. The system's performance is evaluated against existing machine learning methods using appropriate metrics, such as accuracy, precision, recall, and F1-score.

II. RELATED WORK

For the purpose of detecting fraud, a variety of supervised and semi-supervised machine learning approaches are employed. Novel approaches to fraud detection, focusing on neural networks, data mining, and distributed data mining, along with a multitude of research methodologies and fraud detection techniques. Many other techniques are used to detect such fraud. For example, in 2020, (Sadineni, 2020) Detect fraudulent transactions using principal component analysis to perform dimensionality reduction to separate irrelevant attributes from relevant and thus, extracted only the desired attributes such as time of transaction, amount and transaction class etc. Decision tree provides better result than the compare algorithm. However, better results can be obtain using deep learning multi layers of abstraction

Similarly, (Khatri, Arora, & Agrawal, 2020) compared some established supervised learning algorithms to differentiate between genuine and fraudulent transactions. imbalanced dataset to check the suitability of different supervised machine learning models to predict the chances of occurrence of a fraudulent transaction. Decision Tree perform better than other compare models. however, the stuy failed to apply the resampling techniques to the respective datasets being used

Furthermore, (Dornadula & Geetha, 2019) design and develop a novel fraud detection method for streaming transaction data, with an objective, to analyze the past transaction details of the customers and extract the behavioral patterns using several machine learning algorithms observed that Logistic regression, decision tree and random forest are the algorithms that gave better results. However, a better result can be obtain using deep learning multi layers of abstraction

In 2021, (Gomes, Jin, & Yang, 2021) proposed Insurance Fraud Detection with Unsupervised Deep Learning a new variable importance methodology incorporated with two prominent unsupervised deep learning models, namely, the autoencoder and the variational autoencoder. The proposed unsupervised deep learning variable importance methodology, relative to supervised variable importance, offers pragmatic insights into the data while also providing exceptional performance in the absence of training output labels. However, the study ignored data balancing techniques which may degrade the accuracy.

Recently (Singh, Jain, & Biable, 2022) proposed financial fraud detection approach based on firefly optimization algorithm and support vector machine. A new methodology has been proposed for detecting credit card fraud (financial fraud) that is a hybridization of the firefly bio-inspired optimization algorithm and a support vector machine (called FFSVM), which comprises two sequential levels. The proposed approach has achieved an accuracy of 85.65% and successfully classified 591 transactions, which is far better than the existing techniques Low. However, the study attains a low classification accuracy and high experimental time. Moreover, (Aslam, Hunjra, Ftiti, Louhichi, & Shams, 2022) proposed an insurance fraud detection: evidence from artificial intelligence and machine learning. Three predictive models (logistic regression, support vector machine, and naïve Bayes) are applied for developing the fraud detection mechanism. The results reveal that the support vector machine outperforms in terms of accuracy, and the logistic regression achieves the highest f-measure score. However, the study is limited solely on the data of auto insurance from United States

Additionally, (Rukhsar, Bangyal, Nisar, & Nisar, 2022) predict insurance fraud detection using machine learning algorithms. A comparative analysis on various classification algorithms, namely Support Vector Machine (SVM), Random-Forest (RF), Decision-Tree (DT), Adaboost, K-Nearest Neighbor (KNN), Linear Regression (LR), Naïve Bayes (NB), and Multi-Layer Perceptron (MLP) to detect the insurance fraud. The comparative results of classification algorithms conclude that DT gives the highest accuracy of 79% as compared to the other techniques. However, the study aachieved low classification accuracy due to high dimension of the datasets.

More recently, (Mohammed, Boujelben, & Abid, 2023) proposed a novel approach for fraud detection in blockchain-based healthcare networks using machine learning base on a system architecture for detecting fraudulent transactions and attacks in the BC network based on Machine Learning (ML). The results demonstrate that the Random Forest algorithm outperformed others by achieving the highest accuracy, execution time, and scalability. However, the study ignored data balancing techniques which may degrade the accuracy.

ISSN No:-2456-2165

Similarly, (Yu et al., 2023) proposed a multi-perspective fraud detection method for multi-participant e-commerce transactions using a novel fraud detection technique that integrates machine-learning and process mining models to monitor real-time user behaviors. Extensive experiments showed that the proposed method can effectively capture fraudulent transactions and behaviors. However, the study fails to incorporate more time features to the behavior patterns so as to make the risk identification more accurate.

III. METHODOLOGY

This work aims to investigate and extend the work achieved in (Saputra et. al 2019) by using the deep neural network (DNN) classifier. the proposed approach is described in detail in the preceding sections and can be simply divided into the data processing stage and modeling stage. We estimate the performance of classifiers depending on different types of metrics: Accuracy, Precision, Recall, and F1 score. It is calculated based on the confusion matrix which provides their presentation of the number of actual and predicted cases obtained from the classifier.

This research aims to classify e-commerce transactions that include fraud and non-fraud using Deep Neural Network (DNN). The research process is carried out as shown Figure 3.2. Detecting fraud using the ADASYN (Adaptive Synthetic Sampling) technique in combination with a Deep Neural Network involves several key steps. ADASYN is used to address class imbalance by generating synthetic samples for the minority class (fraudulent transactions), and a Deep Neural Network is employed as the classifier for fraud detection. The combination of ADASYN for handling class imbalance and a Deep Neural Network for learning complex patterns in the data can be effective in fraud detection tasks and be adapt to changing fraud patterns and maintain high accuracy in detecting fraudulent activities.

A. Data Preparation and Feature Engineering

This stage involves preparing the dataset, which include both legitimate and fraudulent transactions. This stage will ensure the data is cleaned and properly formatted. Perform feature selection and engineering by identifying and selecting relevant features for the model using feature scaling, dimensionality reduction, and transformation with PCA. We split the dataset into training and testing sets: in this research, we used 80% of the data for training and 20 for the testing. The training set is used to train the model and the testing set is used for final evaluation.

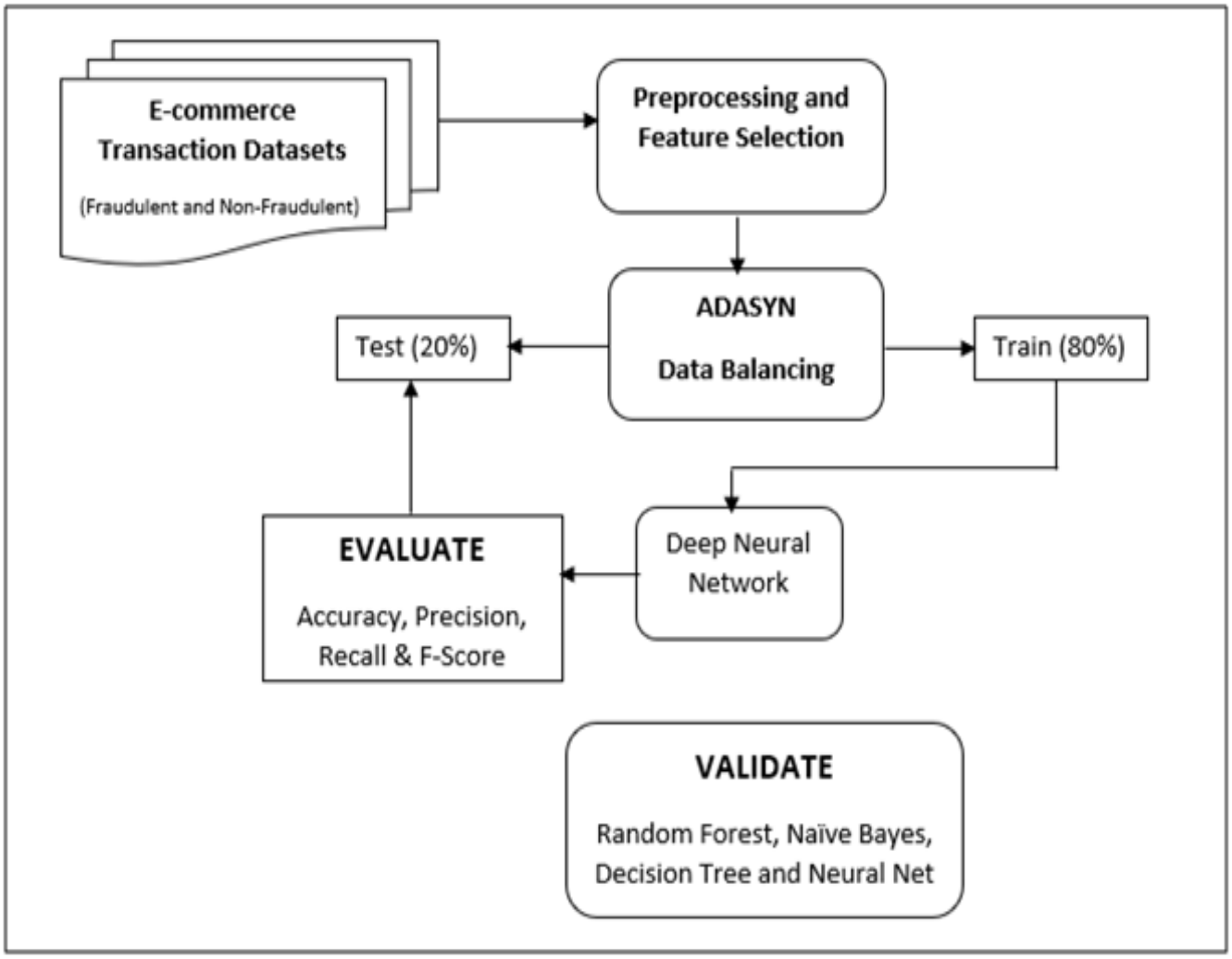

Fig 1 Framework for the Proposed Method

ISSN No:-2456-2165

B. Data Balancing using ADASYN

DASYN (Adaptive Synthetic Sampling) is a data balancing technique used to address class imbalance in machine learning datasets. It focuses on generating synthetic samples for the minority class, particularly those instances that are more challenging to classify correctly. We apply ADASYN to address class imbalance. This helps balance the class distribution. The steps used to create the balance datasets are outline below:

- Calculate the number of samples in each class (majority and minority) to understand the level of class imbalance.
- Set parameters such as the desired number of synthetic samples to generate (usually based on a desired balance ratio) and a distance metric for measuring the difficulty of classification.
- Calculate the imbalance ratio (IR): The IR is defined as the number of majority class samples divided by the number of minority class samples. This ratio helps determine how much over-sampling is needed.
- **Compute K-Nearest Neighbors**
- For each minority class sample:
- Calculate the k-nearest neighbors (KNN) of that sample from both the minority and majority classes.
- Compute the minimum number of KNN belonging to the majority class (min_maj).
- **Calculate the Imbalance Ratio for Each Sample**
- Calculate the imbalance ratio for each minority class sample using the formula:
- IR_i = min_maj / k, where k is the number of neighbors.
- **Calculate the Amount of Synthetic Samples**
- Calculate the number of synthetic samples to generate for each minority class sample based on its IR_i value.
- **Generate Synthetic Samples**
- For each minority class sample:
- Select k-nearest neighbors from the majority class.
- Randomly choose one of the neighbors.
- Generate synthetic samples along the line connecting the selected neighbor and the original sample, based on the previously calculated number of synthetic samples.
- **Combine Original and Synthetic Data**
- Combine the original dataset with the newly generated synthetic samples to create the balanced dataset.

C. Deep Neural Network Model Architecture Design

An artificial neural network (ANN) having several layers between the input and output layers is called a deep neural network (DNN). Whether the relationship is non-linear or linear, the DNN determines the appropriate mathematical operation to convert the input into the output. As it progresses through the layers, the network determines the likelihood of every output. For instance, a DNN trained to identify dog breeds will examine the provided image and determine the likelihood that the dog belongs to a particular breed. After reviewing the findings, the user can decide which probabilities the network should show (above a particular threshold, for example) and provide the suggested label. Since each mathematical operation is regarded as a layer in and of itself, complex DNNs have several layers, earning them the moniker "deep" networks.

Complex non-linear relationships can be modeled by DNNs. Compositional models are produced using DNN architectures, in which the object is represented as a layered assembly of primitives. In comparison to a shallow network that performs comparably, the additional layers allow for the composition of characteristics from lower layers, potentially representing complicated data with fewer units. Numerous variations on a few fundamental strategies make up deep structures. Every architecture has achieved success in particular fields. Comparing the effectiveness of different architectures isn't always feasible unless the data sets used for evaluation are the same.

Typically, DNNs are feedforward networks, meaning that information moves straight from the input layer to the output layer without going through a loop. Initially, the DNN builds a map of virtual neurons and gives connections between them random integer values, or "weights". After multiplying the inputs and weights, an output between 0 and 1 is produced. An algorithm would modify the weights if a specific pattern was not correctly recognized by the network. In this manner, the algorithm can increase the weight of some factors while figuring out the best mathematical operation to process the data in its whole. The proposed DNN architecture employed in this work is depicted in Figure 2.

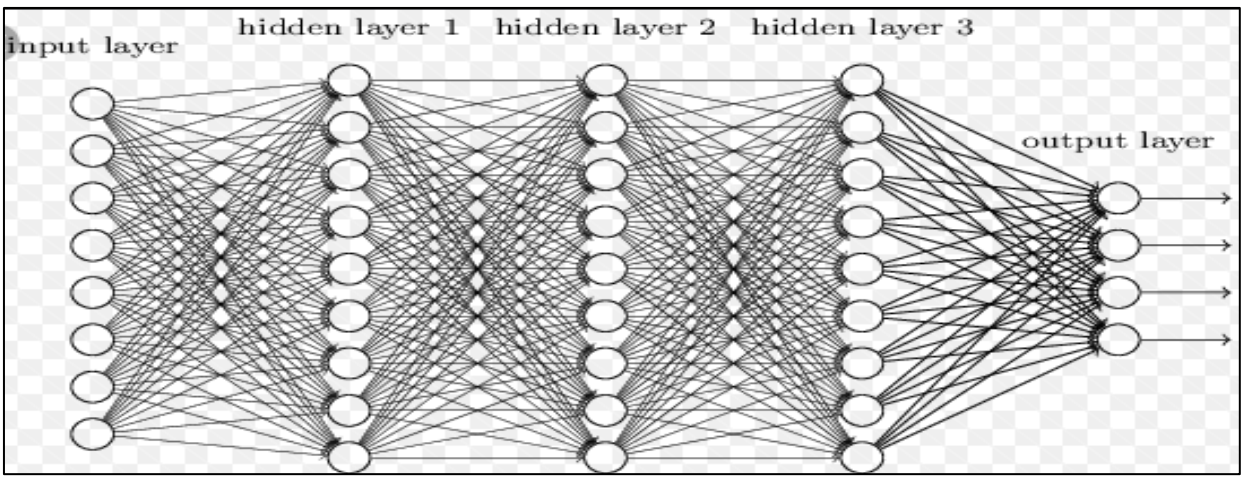

Fig 2 Structure of a Deep Neural Network (DNN)

A standard DNN with an input layer, three hidden layers, and an output layer is depicted in the above diagram. Information is sent to the buried layers via input neurons found in the input layer. Each neuron has one output, one activation function (which determines the output of a given input), and weighted inputs (synapses). The changeable parameters called synapses are what turn a neural network into a parameterized system. The activation signal, which is sent to the activation function to acquire a single output from the neuron, is created by the weighted sum of the inputs. The linear, step, sigmoid, tanh, and ReLU functions are the most often utilized activation functions. We employed a sigmoid activation function in this study.

In this research, we will design the Deep Neural Network architecture by define the architecture of the neural network such as the number of layers, the number of neurons in each layer, activation functions, and the regularization techniques.

D. Model Training

This stage involves training the Deep Neural Network. We use the training dataset (including the synthetic samples) to train the model. Monitor the model's performance on the validation set during training and optimize hyperparameters such as learning rate, batch size, and the number of epochs using the validation set to improve the model's performance. We made used of the python toolkit, due to the fact that it is easier and it is more user friendly when compared to other machine learning applications.

E. Model Evaluation

This stage involves evaluating the model on the testing set. We will assess the model's performance on unseen data using appropriate evaluation metrics for fraud detection, such as precision, recall, F1-score, and accuracy. this can be achieved by adjust the decision threshold to balance between false positives and false negatives.

F. Datasets Description

This research makes use of a Kaggle dataset on e-commerce fraud. The dataset has 151,112 records total; 14,151 records are categorized as fraudulent; the ratio of fraud data is 0.093. By creating synthesis data, ADASYN (Adaptive Synthetic Sampling) corrects the class imbalance in the fraud transaction dataset. As a result, the overall data set is 151,112 records, of which 14,151 are identified as fraudulent, and the fraud data ratio is 0.093. The procedure of ADASYN (Adaptive Synthetic Sampling) creates synthesis data in order to achieve data balance.

G. Evaluation Metric

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

$$\text{Precision} = \frac{TP}{TP+FP} \quad (2)$$

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

$$\text{F1} = 2* \frac{Precision*Recall}{Precision+Recall} \quad (4)$$

IV. RESULTS

This subsection presents the results achieved by the proposed model. We evaluate the performance of the proposed model against other related machine learning techniques. Table 1 depicts the overall performance of the proposed against other baseline algorithms in terms of accuracy, precision, recall and F-score.

Table 1 Overall Results for Binary Classifications of Ecommerce Fraud Across Baseline Algorithms

Algorithm	Sampling Technique	Accuracy	Precision	Recall	F-score
Proposed DNN	ADASYN	97.8	97.2	89.4	96.2
Proposed DNN	NIL	96.5	95.9	80.5	95.8
Decision Tree (DT)	SMOTE	91.0	91.6	60.4	91.2
Decision Tree (DT)	NIL	91.0	54.1	59.8	56.8
Naïve Bayes (NB)	SMOTE	95.0	94.9	54.2	94.5
Naïve Bayes (NB)	NIL	95.0	91.1	54.1	67.9
Random Forest (RF)	SMOTE	95.0	80.5	58.1	94.3
Random Forest (RF)	NIL	95.0	95.5	55.0	69.8

From table 4, the proposed system with ADASYN achieved the best performance in terms of accuracy, precision, recall and F-Measure. This demonstrates the superiority of the proposed model against the other existing algorithm. In the next subsections, we provide the detail discussion on the results analysis and evaluation based on the standard evaluation metric use in this study. They include; accuracy, precision, recall and f-measure as analyze in the next subsections.

A. Classification Accuracy

This performance metric deals with the correct prediction made by the model. Evaluating the classification accuracy of an ecommerce fraud detection model using a Deep Neural Network (DNN) combined with the ADASYN (Adaptive Synthetic Sampling) technique involves assessing how well the model can correctly classify instances of fraud and non-fraud transactions. Figure 2 depict the performance achieved by the proposed model against state-of-the-art approaches. The result are numerical values ranging between 1 and 0. Values close to 1 indicates better classification

ISSN No:-2456-2165

accuracy while values close to 0 indicates poor classification accuracy.

From Figure 3 above, the proposed DNN with ADASYN model achieved the best and highest classification accuracy of 97.8% as against the existing algorithm including DT with SMOTE which achieved 91%, NB with SMOTE which achieved 95% and RF with SMOTE which achieved 95% respectively. This suggest that, for all the base line models used in this study, the data sampling techniques was very detrimental to accuracy. thus, from the experiment, it is noticed that addressing data class imbalance using techniques like ADASYN and SMOTE can positively impact fraud detection accuracy by mitigating the challenges posed by imbalanced datasets. These techniques contribute to better model generalization, reduced overfitting, and improved sensitivity in capturing fraud instances.

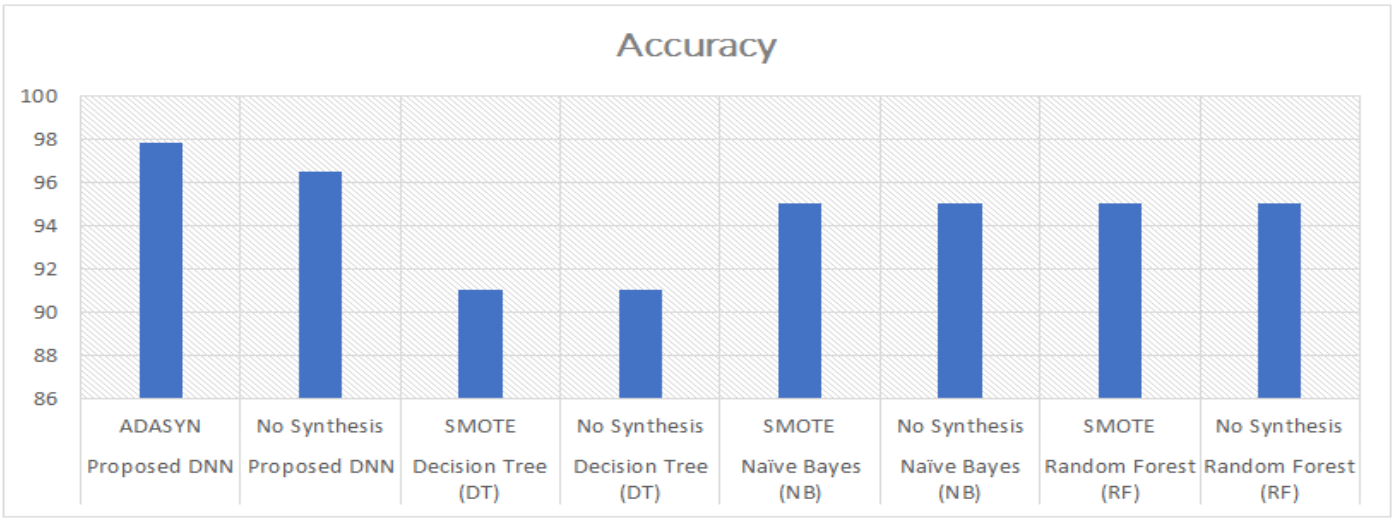

Fig 3 Performance Comparison with Existing Method for Classification Accuracy

However, accuracy is a simple and intuitive metric, but it may not always be the best choice for evaluating a model's performance, especially in cases where the classes are imbalanced. In situations where one class dominates the dataset, a model that predicts the majority class for every instance might achieve a high accuracy, even though it's not really performing well. In such cases, other metrics like precision, recall and F1-score are often used to provide a more comprehensive understanding of a model's performance, particularly when dealing with imbalanced datasets. These metrics consider factors such as false positives, false negatives, and true positives to provide a more nuanced evaluation of a model's abilities. Therefore, the precision was elaborated in the next subsection.

B. Precision

The accuracy can be misleading in some cases. precision and recall help us further understand how strong the accuracy shown holds true for a particular problem. Figure 4 depict the performance achieved by the proposed method against the existing method for the precision. The result are numerical values ranging between 1 and 0. Values close to 1 indicates better classification precision while values close to 0 indicates poor precision.

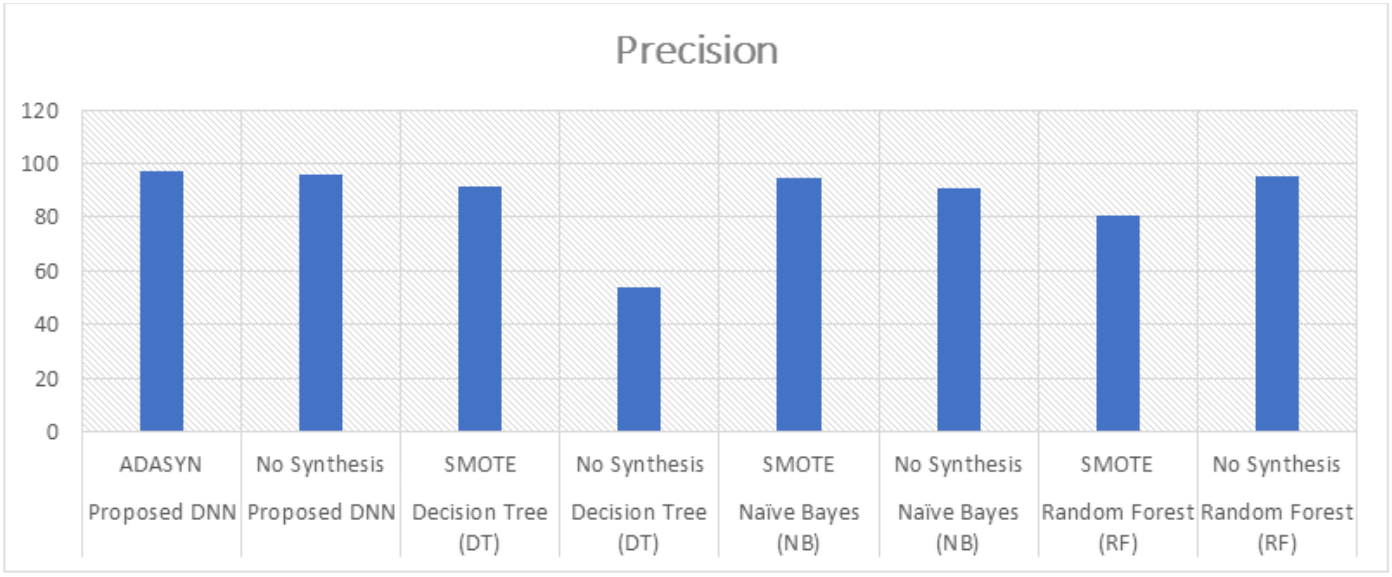

Fig 4 Performance comparison with existing method for precision

ISSN No:-2456-2165

From Figure 4 above, the proposed DNN with ADASYN model achieved the best and highest precision of 97.2% as against the existing algorithm including DT with SMOTE which achieved 91.6%, NB with SMOTE which achieved 94.9% and RF with SMOTE which achieved 80.5% respectively. This suggest that, for all the base line models used in this study, the data sampling techniques was very detrimental to precision. Thus, from the experiment, it is noticed that addressing data class imbalance using techniques like ADASYN and SMOTE can positively impact precision by mitigating the challenges posed by imbalanced datasets. These techniques contribute to better model generalization, reduced overfitting, and improved sensitivity in capturing fraud instances. precision doesn't take into account the cases where the model missed positive instances (false negatives), which is where recall comes into play. In situations where both false positives and false negatives have different implications, precision and recall need to be balanced to find an optimal model performance. Therefore, the recall score is analyzed in the next subsection.

C. Recall

As stated earlier, the precision and recall help us further understand how strong the accuracy shown holds true for a particular problem. Figure 5 depict the performance achieved by the proposed method against the existing method for the recall. The result are numerical values ranging between 1 and 0. Values close to 1 indicates better classification recall while values close to 0 indicates poor recall.

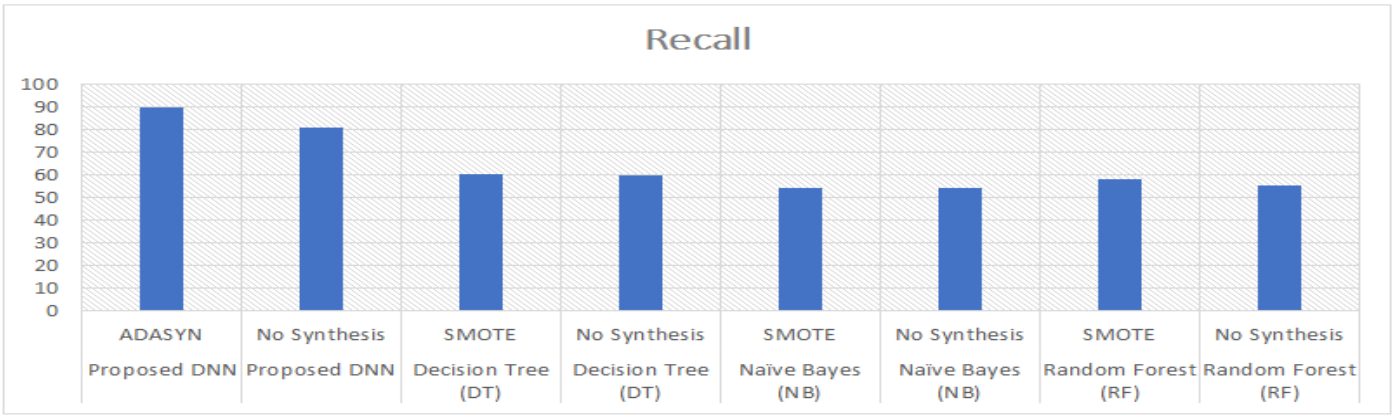

Fig 5 Performance Comparison with Existing Method for Recall

From Figure 5 above, the proposed DNN with ADASYN model achieved the best and highest recall of 89.4 % as against the existing algorithm including DT with SMOTE which achieved 60.4 %, NB with SMOTE which achieved 54.2 % and RF with SMOTE which achieved 58.1 % respectively. Thus, from the experiment, it is noticed that addressing data class imbalance using techniques like ADASYN and SMOTE can positively impact recall by mitigating the challenges posed by imbalanced datasets contributing to better model generalization, reduced overfitting, and improved sensitivity in capturing fraud instances.

D. F-Measure

The precision and recall problems are combined into a single score using the F-Measure. The accuracy of a test is measured by the F1 score, commonly known as the F-score or F-measure, in statistical analysis of binary classification. It is determined by dividing the number of correctly identified positive results by the total number of positive results—including those that were incorrectly identified—and by dividing the number of correctly identified positive results by the total number of samples that should have been identified as positive. This calculation is based on the test's precision and recall. A greater number in each instance indicates the degree of confidence that may be placed in the performance or classification accuracy.

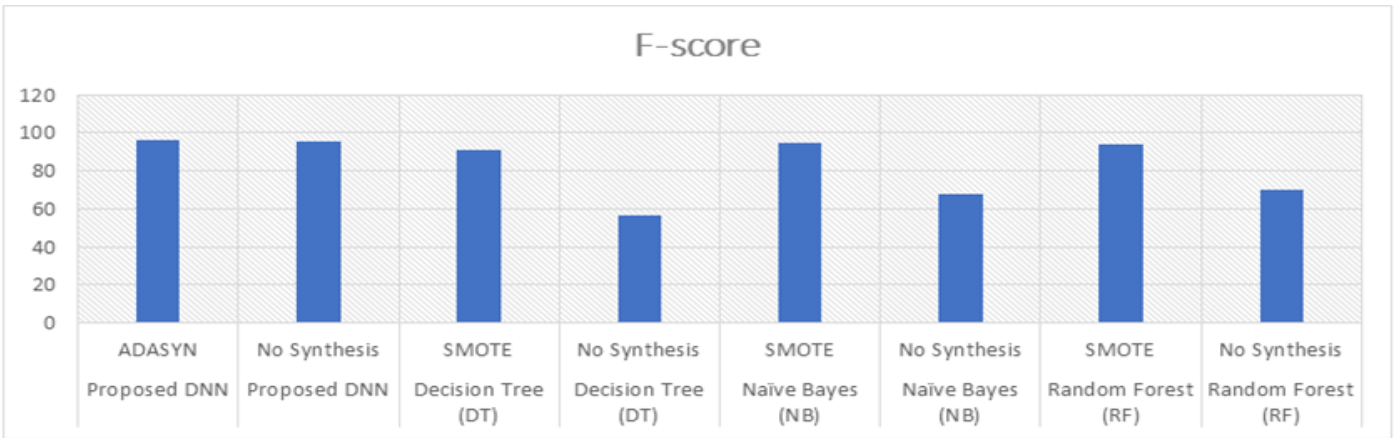

Fig 6 Performance Comparison with Existing Method for F-Measure

ISSN No:-2456-2165

From Figure 6 above, the proposed DNN with ADASYN model achieved the best and highest F-1 of 96.2 % as against the existing algorithm including DT with SMOTE which achieved 91.2 %, NB with SMOTE which achieved 95.5 % and RF with SMOTE which achieved 94.3 % respectively. Thus, from the experiment, it is noticed that addressing data class imbalance using techniques like ADASYN and SMOTE can positively impact recall by mitigating the challenges posed by imbalanced datasets contributing to better model generalization, reduced overfitting, and improved sensitivity in capturing fraud instances. The overall summary of the result presented earlier is depicted in Figure 7.

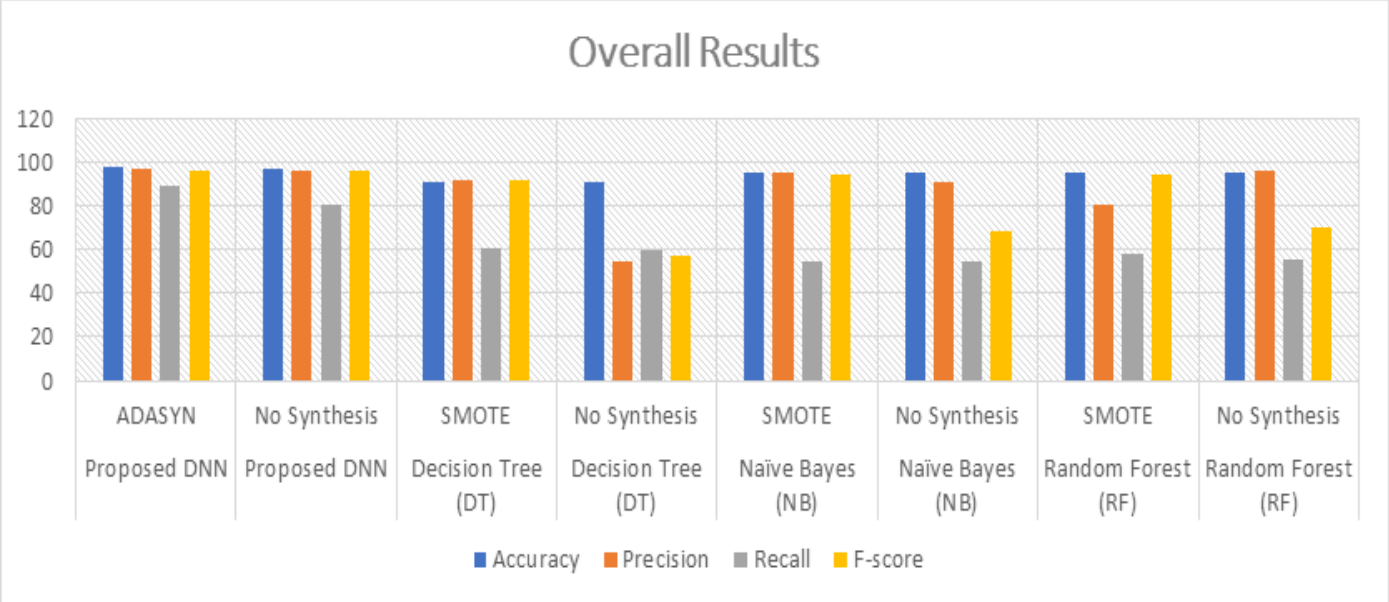

Fig 7 Overall performance comparison with baseline algorithms

From Figure 7, is observe that the proposed attain the first place in all cases of the metrics used for evaluation. Therefore, from the results presented and analyzed above, it may be noticed that the proposed deep learning attains the first place in all the cases and NB attains the second place and only inferior to RF and DT on the benchmark algorithm. Furthermore, it is also clear that the proposed deep learning attains the highest level of performance by obtaining value very close to 100% in accuracy, recall, precision and F-measure.

Therefore, from the experiment, we notice that the performance difference between a Deep Neural Network (DNN) with ADASYN (Adaptive Synthetic Sampling) and conventional machine learning with SMOTE (Synthetic Minority Over-sampling Technique) arises from the inherent capabilities of deep learning models and the complexity of the data distribution. Hence the success of the DNN with ADASYN over the conventional machine learning with SMOTE can be attributed to the fact that Deep neural networks can capture complex, non-linear relationships in the data through the learning of hierarchical features. They automatically learn relevant representations from the input data, potentially capturing intricate patterns that may be challenging for conventional machine learning models.

Additionally, conventional machine learning models, such as the DT, NB and RF, may struggle to capture non-linear relationships and high-dimensional feature interactions without explicitly engineered features. Also, DNNs are capable of end-to-end learning, meaning they can learn hierarchical representations directly from raw data without extensive feature engineering. This is particularly beneficial when dealing with complex data distributions where relevant features may not be easily identifiable. DNNs automatically learn data representations and embeddings during training, allowing them to adapt to the underlying structure of the data. This adaptability is advantageous in scenarios where the data distribution is complex and not well-defined.

While SMOTE generates synthetic samples, it may not inherently capture the complexity of the data distribution in terms of feature representations. Deep learning models can handle large-scale complexity, especially when the dataset is vast and exhibits intricate patterns. The ability to learn from massive amounts of data contributes to improved generalization.

Conventional models may struggle with high model complexity or may require significant parameter tuning to accommodate complex data distributions.

Hence from this study, we have shown that DNNs can be more robust to imbalanced datasets, especially when combined with oversampling techniques like ADASYN. The end-to-end learning and non-linear transformations allow the model to adapt to class imbalances more effectively. Whereas, conventional models may face challenges in adapting to imbalanced datasets, and oversampling alone may not be sufficient to overcome these challenges.

In general, the advantages of a DNN with ADASYN over conventional machine learning with SMOTE often stem from the deep learning model's ability to automatically learn complex, hierarchical representations from raw data. The end-to-end learning process and the adaptability of DNNs make them well-suited for scenarios with intricate and high-dimensional data distributions.

V. CONCLUSION

The consequences of fraud can include financial losses, legal liabilities, damaged reputations, and compromised data security. As fraudsters employ increasingly sophisticated techniques, the need for robust and adaptive fraud detection and prevention systems has never been greater. Machine learning plays a pivotal role in addressing these challenges. Detecting fraud is a complex and dynamic task due to several challenges. Therefore, balancing fraud detection accuracy with the need to provide a frictionless and enjoyable shopping experience for legitimate users with deep neural networks is a critical task that is explored in this research. Hence, we proposed a DNN model in combination with ADASYN for accurate detection of e-commerce fraud. Experimentation on python shows that the proposed DNN with ADASYN model achieved the best and highest classification accuracy of 97.8% as against the existing algorithm including DT with SMOTE which achieved 91%, NB with SMOTE which achieved 95% and RF with SMOTE which achieved 95% respectively. thus, from the experiment, it is noticed that addressing data class imbalance using techniques like ADASYN and SMOTE can positively impact fraud detection accuracy by mitigating the challenges posed by imbalanced datasets. The successful development of the proposed method has extended the detection accuracy, precision, recall and F-score of the methods compared to other classical machine learning methods. These techniques contribute to better model generalization, reduced overfitting, and improved sensitivity in capturing fraud instances. Thus, this enhances the effective fraud detection system for e-commerce security and trustworthiness of the platform protect users from fraudulent activities, reduce financial losses, and preserve the platform's reputation.

It's essential to consider the specific characteristics of the dataset and the computational resources available when choosing the most suitable approach. Hence, this was a major shortcoming of the study. We recommend that further research should consider the specific characteristics of the dataset and the computational resources available when choosing the most suitable approach.

ACKNOWLEDGMENT

We appreciate the expert support of our supervisor Prof. A. Y. Gital ab Prof. A. M Kwami, Yau for their guidance towards the success of this research.

REFERENCES

[1]. Wang, S., et al. Session-based fraud detection in online e-commerce transactions using recurrent neural networks. in Machine Learning and Knowledge Discovery in Databases: European Conference, ECML PKDD 2017, Skopje, Macedonia, September 18–22, 2017, Proceedings, Part III 10. 2017. Springer.

[2]. Zhang, G., et al., efraudcom: An e-commerce fraud detection system via competitive graph neural networks. ACM Transactions on Information Systems (TOIS), 2022. **40**(3): p. 1-29.

[3]. Saputra, A., Fraud detection using machine learning in e-commerce. International Journal of Advanced Computer Science and Applications, 2019. **10**(9).

[4]. Salman, A., et al., Automatic fish detection in underwater videos by a deep neural network-based hybrid motion learning system. ICES Journal of Marine Science, 2020. **77**(4): p. 1295-1307.

[5]. Ijaz, M.F., et al., Hybrid prediction model for type 2 diabetes and hypertension using DBSCAN-based outlier detection, synthetic minority over sampling technique (SMOTE), and random forest. Applied sciences, 2018. **8**(8): p. 1325.

[6]. Das, R., et al. An oversampling technique by integrating reverse nearest neighbor in SMOTE: Reverse-SMOTE. in 2020 international conference on smart electronics and communication (icosec). 2020. IEEE.

[7]. Susan, S. and A. Kumar, The balancing trick: Optimized sampling of imbalanced datasets—A brief survey of the recent State of the Art. Engineering Reports, 2021. **3**(4): p. e12298.