JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Fraud Identification in Banking Transactions with Machine Learning Technique in Financial Management

Krishna Gupta
Applied Mathematics
Delhi Technological University
Delhi

Abstract*— The number of banking transactions increased as a consequence of the widespread use of credit cards as a payment mechanism due to the proliferation of e-commerce services and other technological advancements. Customers and the bank alike suffer enormous financial and reputational harm as a result of fraudulent conduct made possible by security holes in our banking systems. An estimated large sum of money is lost financially each year as a consequence of financial fraud in banks. Early discovery aids in the mitigation of fraud by allowing for the development of a countermeasure and the recovery of such losses. This research proposes a machine learning-based method to effectively aid in fraud detection. Comparing six popular ML algorithms—AdaBoost, NBC, SVM, KNN, ANN, and XGBClassifier—aims to identify the best model for fraud detection. Moreover, we addressed the problem of class imbalance by using the SMOTE. A 99.88% accuracy rate for fraud detection made the XGBoost Classifier the most effective classifier. This study demonstrates the remarkable accuracy score of the XGBoost Classifier in identifying financial fraud on balanced datasets. The information and conclusions offered here make a significant addition to the continuing work being done to create efficient fraud detection systems for a banking sector.

Keywords*— Fraud Identification, Banking Transactions, credit card frauds, machine learning, XGBoost.

I. INTRODUCTION

The contemporary era's banking systems are vital to world economies due to the fact that they enable monetary transactions and provide businesses and consumers with necessary services. Fraudulent activity, however, has the potential to destroy such organisations' reputations and result in enormous financial losses. Criminals are always coming up with new techniques to perpetrate fraud. Fraudsters' strategies are continually improving as technology advances, making traditional fraud detection systems difficult to stay up. Fraudsters always update their strategies to exploit new weaknesses, increasing the complexity and sophistication of their operations [1][2]. The frequency of theft, fraud, and fraud incidents in electronic banking is rising annually. Cybercrime experts continuously monitor and validate transaction systems and network infrastructure. Employing specialized threat response teams (CSIRTs) helps organizations maintain security and thwart cyber threats [3][4].

Financial institutions incur losses due to the inadequacy of conventional fraud detection systems in dealing with the ever-changing criminal landscape [1][5][6]. The primary target of cybercriminals is not banks; rather, it is unsuspecting users who lack IT expertise and are ignorant of the fundamentals of online security [3][7].As exposed in [8], Financial fraud affects not only the banking industry but also daily life, lowering confidence between institutions, upsetting financial markets, and so driving up living expenses. The growing frequency of fraudulent acts in the digital era has made the area of fraud detection employing ML algorithms on financial transaction data more and more significant. Organizations may proactively detect and prevent fraudulent activity by using ML approaches, which provide strong capabilities for identifying patterns and abnormalities in vast amounts of transactional data[9][10][11].

Frauds are often unavoidable once criminals swiftly adapt to these advancements in prevention technology, despite the fact that organisations use high standards and a broad range of fraud protection techniques. In order to help classify regular or fraudulent financial transactions, ML approaches in this case provide assessment and prediction models. ML is defined as a data analysis technique that gives the computer an update or modification of its operations with respect to the prediction of any event or controlling device. allowing for an use of ML to assess, forecast, and identify fraudulent efforts inside a financial system. These unfavourable factor occurrences may be lessened, increasing public trust in the organisation and the financial system [12][13][14]. Strive to improve upon the

inadequacies of an existing fraud detection systems by employing ML on unbalanced data with SMOTE balancing.

1.1 Research contribution of work

The importance of this study rests in the fact that it seeks to address a pressing issue for banking and financial institutions: the need to improve fraud detection in financial transactions. A difficulty in detecting fraudulent transactions arises from the fact that extremely unbalanced databases are difficult to manage. The study's overarching goal is to provide better tools for protecting financial transactions by improving fraud detection systems through the employ of modern ML techniques, like thorough data preprocessing, feature selection, and performance evaluation. The research contribution of this work as:

- Uses a practical credit card transaction dataset to test fraud detection algorithms. This real-world data ensures the practical applicability and relevance of the proposed algorithms in real financial environments.
- Applies data cleaning, scaling, and SMOTE for better model performance. These preprocessing steps are crucial for enhancing the quality of the dataset, ensuring accurate and reliable model performance.
- Compares KNN, Naïve Bayes, SVM, AdaBoost, ANN, and XGBoost for fraud detection. By comparing the performance of these models across various metrics, the study identifies the most effective algorithms for detecting fraudulent transactions.
- Uses Information Gain for feature selection and conducts correlation analysis. Furthermore, the fundamental characteristics of the dataset may be better understood with the help of a thorough correlation analysis, which sheds light on the correlations between various variables.
- Provides detailed evaluation of model F1-score, recall, accuracy, and precision, highlighting XGBoost and AdaBoost as top performers. The results demonstrate that XGBoost achieves the highest accuracy (99.88%) while AdaBoost shows the best overall performance considering all metrics.

1.2 Organization of the paper

This paper's reminder is set up as follows: We evaluate the relevant state-of-the-art in Section II. The proposed approach to credit card fraud detection is presented in Section III, together with the dataset, pre-processing, scaling, balancing, features election, algorithms, framework, and evaluation metrics. The assessment findings of the conducted experiments are covered in Section IV, and Section V offers suggestions for further research to wrap up the article.

II. LITERATURE REVIEW

The last 10 years have seen a significant increase in the attention given to fraud identification in banking transactions. An outline of ML approaches used in CCFD is given in this section. An increasing amount of scholarly works has put forward strategies to improve the identification of fraud. The following is an overview of recent, relevant studies.

This research proposes a ML-based method to effectively contribute to fraud detection [15]. The AI-based strategy will speed up the verification process to minimise damage and fight counterfeit goods. This study looks at several intelligence algorithms that were trained on a public dataset to find the correlation between specific traits and fraud. This research makes use of a resampled dataset to lessen its significant class imbalance and then applies the proposed approach to analyse the data more accurately.

In [16], suggested a detection framework and used SVM supplemented with quantum annealing solvers to build it using a QML technique. Twelve additional ML techniques were implemented after assess a detection performance of a QML application. Two datasets were used to evaluate the performance of the QML application and these ML implementations. One dataset was a time series of severely unbalanced bank loans, while the other was a non-time series dataset of mildly imbalanced credit card transactions in Israel. The results show that the quantum enhanced SVM is faster and more accurate than the competitors when used to the dataset of bank loans.

In[17], explore the possibility of identifying fraudulent transactions by using the credit card fraud dataset in conjunction with two ANN classifiers: MLP and ELM. Some of the criteria used to evaluate these classifiers include classification time, accuracy, recall, and precision. In terms of accuracy, the findings show that ELM classifiers achieve 95.46% and MLP classifiers 97.84%. But ELM can see fraudulent transactions coming up next second.

In[18], effectively manage the relative importance of valid and fraudulent transactions, think about integrating a voting classifier with class weight adjustable hyperparameters. The majority voting ensemble learning technique may also be used to assess the effectiveness of the integrated algorithms. With ROC-AUC0.95, precision0.79, recall0.80, F1 score0.79, and MCC0.79, LightGBM and XGBoost both achieve the top level. By using DL and the Bayesian optimisation technique, they are able to tune the hyperparameters to match an impressive set of criteria, including a ROC-AUC0.94, precision0.80, recall0.82, F1 score0.81, and MCC0.81. In comparison to the most cutting-edge methods, this is a significant improvement.

In[1], compares four popular machine learning algorithms—SVM, XGBoost, DT, and LR—in an effort to find the optimal model for fraud detection. Utilising the SMOTE allowed us to go further into the issue of class imbalance. Among the models tested, the XGBoost Classifier had the highest accuracy rate of 88% in detecting fraud. They used SHAP and LIME research to improve overall comprehension and reveal how the XGBoost model makes decisions.

A LSTM-RNN is suggested as a model for detecting fraud instances[19]. Further improvement in performance is achieved with the use of an attention mechanism. This kind of model has shown to be quite effective in situations such as fraud detection, when the data sequence consists of vectors with complex interconnected characteristics. There are a number of classifiers that LSTM-RNN is pitted against, including ANN, NB, and SVM. The experimental findings show that our suggested model is quite accurate and generates impressive outcomes.

In[20], provide an algorithmic approach to detecting fraud in financial transaction data using ML. Developing a trustworthy model that can identify fraudulent transactions while reducing the number of false positives is our main goal. There are two stages to the system's operation: engineering features and training the model. They begin by extracting useful characteristics from the transaction data via rigorous feature engineering. Customer behaviour history, location, time of day, and transaction amount are some of these characteristics. They furthermore use other data sources, such as IP geolocation databases and blacklists, to bolster the fraud detection capabilities.

This table 1 provides a concise overview of the approaches and performance metrics used in various studies on fraud detection in banking transactions. It also highlights areas for future research and potential improvements.

Table 1: Summary of the related work on fraud detection in banking transactions

References	Methodology	Performance	Limitations & Future Work
[15]	AI-based model using various intelligent algorithms	Improved accuracy (specific metrics not provided)	Further enhancement in AI models for real-time applications
[16]	QML with SVM enhanced by quantum annealing solvers	Quantum enhanced SVM outperformed others in speed and accuracy	Exploration of more quantum algorithms and datasets
[17]	Artificial Neural Network classifiers (MLP and ELM)	MLP: 97.84% accuracy, ELM: 95.46% accuracy (ELM is faster for prediction)	Integration of additional neural network architectures for improved performance
[18]	Class weight-tuning with voting classifier, majority voting ensemble method (LightGBM, XGBoost)	LightGBM and XGBoost: ROC-AUC = 0.95, F1 score = 0.79, MCC = 0.79, precision = 0.79, recall = 0.80; DL with Bayesian optimization: ROC-AUC = 0.94, F1 score = 0.81, MCC = 0.81, precision = 0.80, recall = 0.82	Further optimization of hyperparameters and exploration of more ensemble techniques
[1]	Comparison of SVM, XGBoost, Decision Tree, Logistic Regression with SMOTE for class imbalance	XGBoost: 88% accuracy; SHAP and LIME used for model interpretability	Examination of additional imbalance techniques and model explainability methods
[19]	LSTM-RNN with attention mechanism	High accuracy compared to Naive Bayes, SVM, and ANN	Further testing with different RNN architectures and larger datasets
[20]	Two-step process: feature engineering and model training	Financial transaction data with external data sources (IP geolocation, blacklists)	Improvement in feature engineering methods and integration of more diverse external data sources

III. METHODOLOGY

The proposed methodology for fraud detection involves preprocessing the "credit card" dataset through cleaning, scaling, and balancing with SMOTE shows in figure 1. Key features are selected using the Information Gain method. The data is divide into training and validation sets, and various machine learning models—KNN, NB, XGBoost, SVM, AdaBoost, and ANN—are trained and evaluated employing metrics like F1-score, recall, accuracy, and precision to enhance fraud detection and minimize false positives.

The following methodology steps discussed below:

3.1 Data Collection

In order to make a result of a suggested method useful in real-world scenarios, we use an actual dataset in this work. We examine a dataset called "credit card," which includes 284,807 records of credit card customers' two-day purchases in September 2013. The remaining transactions are all valid, with the exception of 492 fraudulent ones. There is a significant imbalance in the dataset since the positive class (frauds) represents just 0.172% of all transactions. You can obtain this dataset at https://www.kaggle.com/mlg-ulb/ creditcardfraud. Table 2 provides an overview of the characteristics and factors.

TABLE 2. The features of the credit-card fraud dataset that is used in this paper.

Variable Name	Description	Type
V1, V2, ..., V28	Transaction feature after PCA transformation	Integer
Time	Seconds elapsed between each transaction with the first transaction	Integer
Amount	Transaction Value	Integer
Class	fault or Default	0 or 1

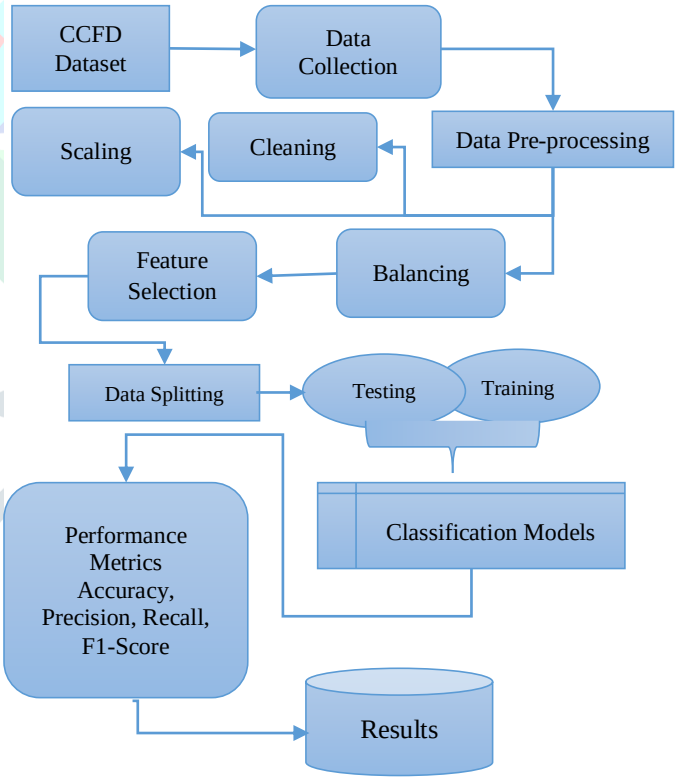

Figure 1: Flowchart of Fraud Identification in Banking Transactions

3.2 Data Preprocessing and Visualization

Pre-processing data is an essential stage in any research project including data analysis since it guarantees the quality and correctness of the data prior to the use of any analytical methods. This stage involves several key tasks, including data cleaning, scaling, balancing, and feature selection. These phases described as:

Data cleaning: Data cleaning addresses missing values, outliers, and inconsistencies, which can otherwise lead to biased or incorrect results.

Figure 2: Fraud class histogram with the imbalanced dataset

The vast majority of transactions are legitimate. This striking difference is shown in the following graphic (refer to Figure 2).

Data scaling: Data scaling adjusts the scales of the data, facilitating better comparisons and enhancing a performance of ML algorithms. Data characteristics or independent variable ranges may be standardised using the scaling technique. Data normalisation is another name for it in data processing, and it's usually done in the data pre-processing stage. Thus, the MinMaxScaler approach was used in this study to rescale the characteristics from 0 to 1. This method's strength is that it employs statistical approaches that are insensitive to outliers and do not alter the data's variance (Equation (1)) [21].

$$x' = \frac{x - min(x)}{max(x)} - min(x) \ldots\ldots (1)$$

Equation (1) above illustrates this: x denotes an original value, x' denotes a scaled value, max is a feature value's upper limit, and min denotes its lower bound.

SMOTE: A situation known as unbalanced classification occurs when prediction models are built using classification datasets that have a large disparity between the classes [22]. To deal with imbalanced datasets, one approach is to oversample the minority class. Even though these examples don't provide the model any more information, the simplest approach is to replicate instances from the minority class. As an alternative, new instances might be produced by merging the old ones. We call this kind of minority class data augmentation the SMOTE [23]. We used the SMOTE method to balance the dataset. As shown in Figure 3, the class feature is currently balanced with 50% of transactions being fraudulent and 50% not fraudulent.

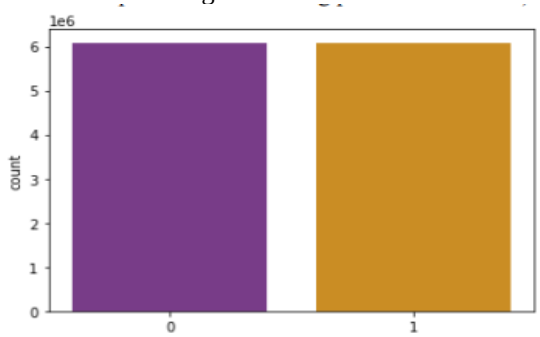

Figure 3: Bar graph after data balanced

Correlation Analysis: A statistical technique called correlation analysis seeks to determine the link among two or more variables [24][25]. The program does calculations that provide a correlation coefficient between -1 and +1. At its core, the concept is that variables are positively correlated when the coefficient is positive, negatively correlated when the coefficient is negative, and completely uncorrelated when the coefficient is zero. It is not always true that changing one variable causes a change in the other just because there is a connection between them. The basic characteristics of the dataset may be discovered by means of correlation analysis. Results of the dataset correlation analysis are shown in Figure 4.

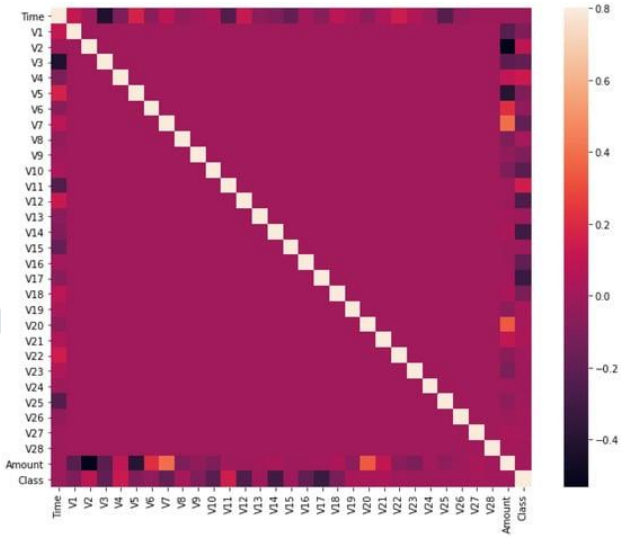

Figure 4. Correlation analysis.

The correlation matrix is graphically represented by the heatmap, where each pixel represents the correlation between two separate variables. A color-coded method is used to graphically display the correlation values, which may range from -1 to 1. This system uses many visual signals, with black representing negative correlation, white representing positive correlation, and red representing no correlation at all.

Feature Selection: "Time" and "Amount" are the only known characteristics; beyond that, we don't know anything else. By analysing the available characteristics, features election attempts to choose a subset that enhances a classifier's ability to detect credit card fraud[26][27]. The training data is dimensionally reduced using the information gain (IG) approach, which involves selecting the most significant characteristics. First, it determines if a credit card transaction is legal or fraudulent by looking for similarities between them. Then, it uses this information to determine which aspects are most important and gives them more weight [28]. There is evidence that the information acquisition approach is both computationally efficient and performs very well in terms of precision [29] [30]. Hence, the IG approach for feature selection is also taken into account in the suggested framework.

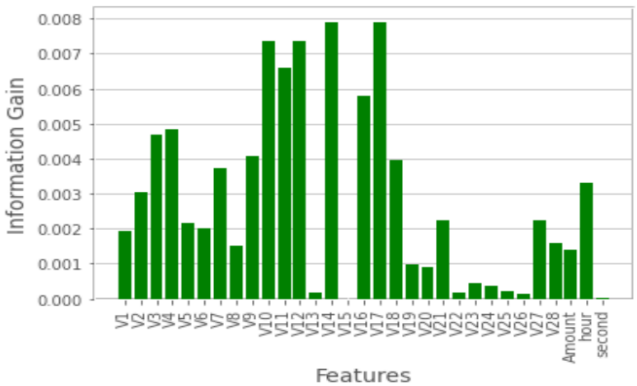

Figure 5. Feature importance with IG method.

The suggested methodology was tested using the top six characteristics retrieved using this manner (Figure 5, IG diagram).

3.3 Data Splitting

Five equal-sized subgroups with a uniform sample distribution across all classes are created at random from the dataset. Throughout a validation process, 20% of a dataset is kept aside for validation purposes, while the other 80% is used for training. This ensures that the suggested strategy is tested against the reserved data.

3.4 Classification Models

The ML models that the system will use to detect credit card fraud are covered in this section.

1) K-Nearest Neighbors

For issues involving classification and regression, this classifier is used. One advantage is that it lowers false alarm rates while increasing credit card detection rates. Similarity measurements are the basis for its operation. Therefore, it records all existing instances and arranges for new ones [9][31]. Utilizing statistical learning approaches, it functions admirably in supervised ML systems; this is because it employs a learning stage to acquire the information required for classifying significant differences. When using unsupervised learning approaches, however, training is unnecessary. The three elements that make up KNN are K value, distance metrics, and distance rule. Distance measures are used to determine each incoming data point's nearest neighbour. Using a distance rule, the new data point is classified according to its neighbours' attributes; the number of neighbours to compare it to is known as the K-value[32].

2) Naïve Bayes

This classifier is taught to anticipate future occurrences of the target class; it is a supervised ML model. It's well knowledge that NB is a successful probabilistic method that forecasts future events by using feature and class information from the dataset. This method is considered "naïve" as it treats every attribute independently based on the class variable, whether the attribute is present or not. However, "Bayes" explains how it finds the probability that the class is correct [33][34]. This method achieves respectable outcomes in a huge variety of challenging real-world applications, despite NB's relatively straightforward approach.

3) XGBoost

XGBoost, is now the go-to approach for practical ML applications. One kind of decision tree method that uses boosted gradients is XGBoost. Because of its strong model performance, memory resources, and quick execution speed, it is favoured above other GBMs. This method is a hybrid approach that fixes mistakes caused by current models by adding new models. XGBoost makes use of all available CPUs during training by including parallel computing to build trees. Applying the "max depth" parameter to begin tree pruning in the reverse order, rather than the conventional way (i.e., criterion first), greatly enhances XGBoost computing performance and speed. XGBoost uses a more structured method known as "formalisation" to prevent over-fitting and improve performance [35][18]. Many hyperparameters may be fine-tuned, such as the learning rate, the maximum tree depth, the number of trees, and the weights assigned to classes.

Model training: The XGBoost model was trained on the CCFD dataset with the following hyperparameters: 341 estimators, a maximum depth of 7, a subsample ratio of 0.9, a learning rate of 0.001, and a gamma (γ) value of 0.5. These parameters were selected to optimise performance for effectively identifying fraudulent transactions while minimising false positives, while also balancing the model's complexity and its ability to generalise from the training data. The resulting model achieved impressive metrics, demonstrating its efficacy in identifying fraudulent activities within the dataset.

4) Support Vector Machines (SVM)

The technique was developed in 1995. and it was first used to address particular classification and regression issues. The statistical learning approach is the foundation of this approach. The hyper-optimal level that optimizes category margin is defined. One of the most well-liked synthesis techniques is SVM. One of the supervised classification techniques, the input string and labels are provided. Structures that are determined by these sources' vector features. In order to completely separate these categories, this algorithm creates a super level that can be used to differentiate between the two classes. The margin is the separation between these two parallel lines. Support vectors are the points on border vectors[36].

5) AdaBoost

The term "AdaBoost" refers to an ensemble approach that uses ML methods. The majority of AdaBoost estimators are one-level decision trees, which are also called DT with a single split. One popular term for these trees is decision stumps. In this approach, while constructing a model, each data point is treated equally. Prioritising the incorrectly categorised points follows. More weight is assigned to all points with higher weights in the following model. Training models will continue until the stated error is decreased[37].

6) ANN

ANN built on biological neural networks have the potential to teach computers reinforcement learning techniques that are similar to those used by humans. Each neural network begins with a fundamental building block called a perceptron. The basic components of a perceptron are an input, a processor, and an output. The "feed-forward" concept is followed by a perceptron, which means that inputs are transmitted to neurons, which process them and then produce output [38].

3.5 *Evaluation Metrics*

To ensure that our comparisons are fair, we employ the commonly used metrics for assessments, which include recall, F1-score, accuracy, and precision. A model classification results can generate a confusion matrix. In our trials, a positive number shows a fraudulent transaction and a negative number displays a valid one. Any transaction that has been identified as fraudulent is represented as a true positive (TP). The amount of valid transactions that were incorrectly marked as fraudulent is known as false positives (FP). When transactions are correctly identified as valid, we see a true negative (TN), and when they are misclassified as legal, we see a false negative (FN). Equations (2) through (5) provide the mathematical formulations of the metrics that were used.

$$\text{Accuracy} = \frac{\text{TP} + \text{T}N}{TP + TN + FN + FP} \dots\dots\dots\dots\dots\dots (2)$$

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

$$Precision = \frac{TP}{TP + FP} \dots\dots\dots\dots\dots\dots (4)$$

$$\text{F1} - \text{score} = \frac{2(\text{precision} \times \text{recall})}{\text{precision th recall}} \dots\dots (5)$$

The amount of accurate predictions produced by the model is known as ***accuracy***, and it serves as a measure of the classifier's overall performance. Because it provides a high value for even

a single fraudulent transaction, this criterion does not provide excellent results when dealing with imbalanced data. The ***recall*** metric measures how well the classifier identifies real instances of fraudulent transactions. In order to gauge the classifier's dependability, ***precision*** is used. As a harmonic average of the recall and precision dimensions, the ***F1-Score*** accounts for both false positives and negatives.

IV. RESULT ANALYSIS AND DISCUSSION

In this section offers an outcomes of ML models for CCFD system in python simulation with NumPy, pandas-learn and seaborn libraries on HP i7Core Laptop. Results provide according to confusion matrix, recall, precision, accuracy, and f1-score. Also compare the best model with other existing models for fraud detection.

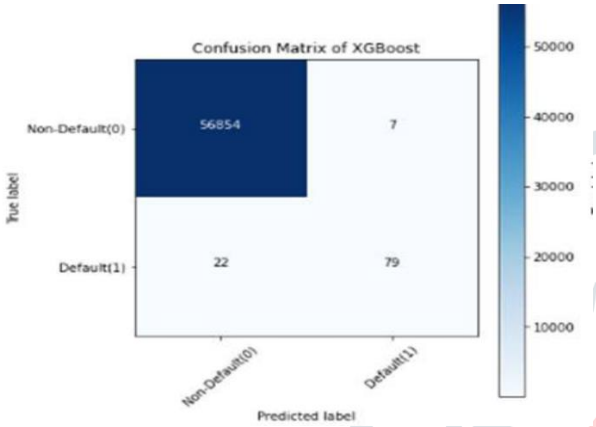

Figure 6: Confusion matrix of XGBoost model for fraud detection

Figure 6 illustrates the XGBoost model's confusion matrix, which gives a thorough performance report for fraud detection. It reveals that out of 56,854 instances that were deemed non-fraudulent, the model properly recognised 79 instances as fraudulent. However, it also misclassified 7 non-fraudulent cases as fraudulent (false positives) and 22 fraudulent cases as non-fraudulent (false negatives). This matrix is important for evaluating a model's accuracy and reliability, highlighting areas for potential improvement in distinguishing between fraudulent and non-fraudulent cases.

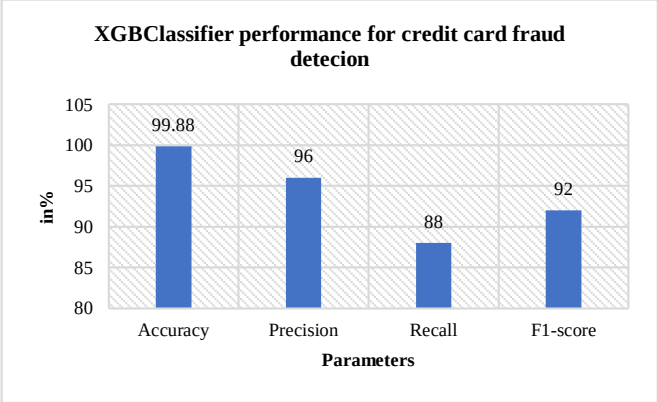

Figure 7: Parameters performance of XGBoost model for fraud detection

An XGBoost model for fraud detection demonstrates outstanding performance shows in figure 7, achieving an accuracy of 99.88%, precision96%, recall88%, and an F1-score92%. This indicates that the model is highly effective in correctly identifying fraudulent transactions (high accuracy and precision) while also capturing a significant portion of actual fraudulent cases (recall), providing a balanced and reliable detection capability.

Table 3: Machine learning models comparison for fraud detection

ML models	Accuracy	Precision	Recall	F1-score
AdaBoost[39]	97.55	95.85	99.41	97.59
Naïve bayes[39]	78.33	69.82	99.75	82.14
SVM[40]	94.21	94.2	94.2	94.2
KNN[40]	93.68	94.5	94.2	94.2
ANN [41]	95.48	98.27	86.36	92.63
XGBClassifier	**99.88**	**96**	**88**	**92**

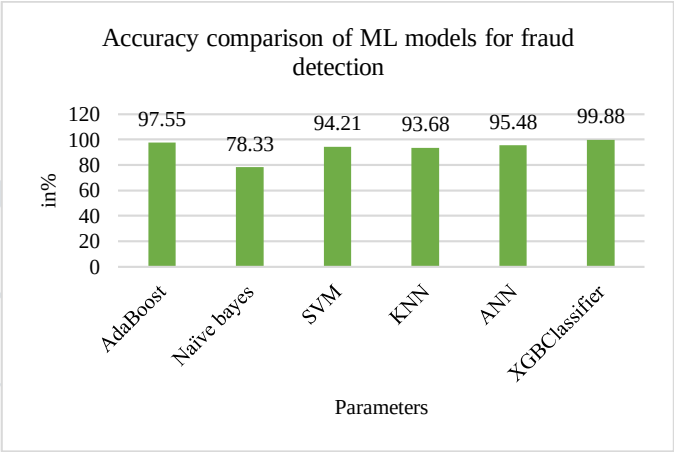

Figure 8: Accuracy bar graph of comparison with ML models for fraud detection

In Figure 8, the XGBClassifier shows the highest accuracy at 99.88%, followed by AdaBoost at 97.55%. ANN, SVM, and KNN also perform well with accuracies of 95.48%, 94.21%, and 93.68%, respectively. Naïve Bayes, however, lags significantly behind with an accuracy of 78.33%, indicating that it may not be as effective for this particular task.

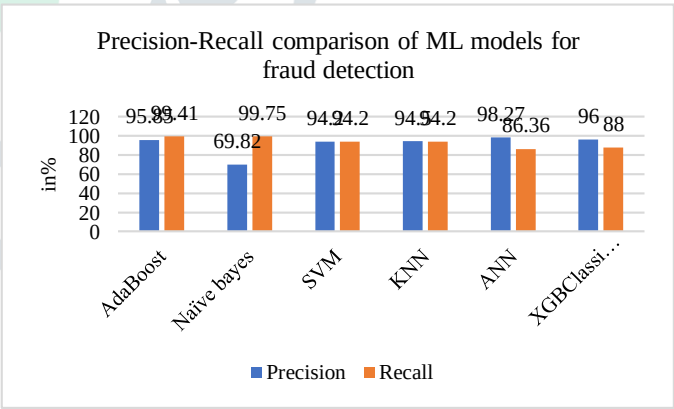

Figure 9: P-R bar graph of comparison with ML models for fraud detection

The Precision-Recall (P-R) bar graph in Figure 9 highlights the precision and recall values for the different models. AdaBoost exhibits high precision (95.85%) and exceptional recall (99.41%). Naïve Bayes, despite having the highest recall (99.75%), has the lowest precision (69.82%). SVM and KNN both have precision and recall around 94.2%. ANN has the highest precision (98.27%) but lower recall (86.36%). The XGBClassifier has a precision of 96% and a recall of 88%, indicating a balanced performance but not leading in either metric.

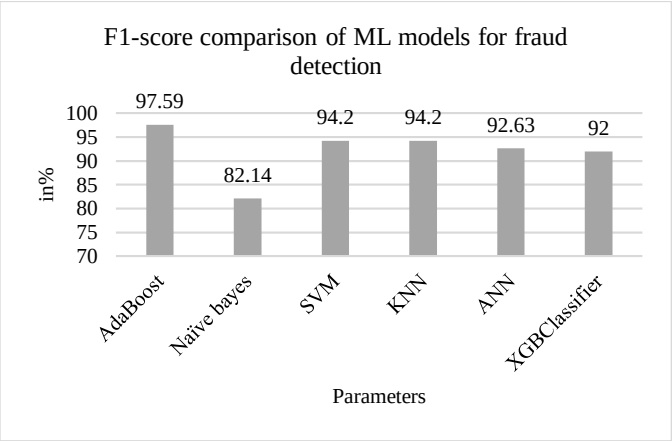

Figure 10: F1-Score bar graph of comparison with ML models for fraud detection

The F1-score bar graph in Figure 10 presents the harmonic mean of precision and recall, providing a single metric to evaluate the models. AdaBoost leads with an F1-score of 97.59, reflecting strong overall performance. SVM and KNN both have F1-scores of 94.2%. ANN's F1-score is 92.63, while XGBClassifier has 92. Naïve Bayes has the lowest F1-score at 82.14, highlighting its imbalance between precision and recall.

3.6 Discussion

The comparison of ML models for fraud detection reveals that while XGBClassifier and AdaBoost have the highest accuracy, AdaBoost stands out with the best overall performance considering all metrics. Naïve Bayes, despite its high recall, suffers from low precision, making it less reliable. Models like SVM and KNN show consistent and balanced performance across all metrics. The ANN model, with its high precision, may be preferable in scenarios where minimizing false positives is crucial. Overall, the choice of model should consider the specific requirements of the fraud detection task, such as the acceptable trade-off between precision and recall.

V. CONCLUSION AND FUTURE SCOPE

Recognising fraudulent conduct in the financial sector is very crucial because of the high stakes involved. Resolving imbalances in datasets gets more difficult when the number of valid transactions significantly exceeds the number of fraudulent ones. The CCFD challenge with imbalanced datasets was examined in this study. Finally, the "credit card" dataset shows that there have been major advances in fraud detection with the use of several ML models. The preprocessing steps, including data cleaning, scaling, and SMOTE balancing, were crucial in improving model performance. Among the models tested, XGBoost and ANN showed superior results, effectively balancing the detection of fraudulent transactions with minimizing FP. An evaluation measures displayed that precision, recall, and F1-score offered a more thorough assessment, but accuracy alone was inadequate because of the unbalanced nature of the dataset. In comparison to other models already in use, we suggested using machine learning and the XGBoost technique to enhance fraud detection performance with an accuracy of 99.88%. Financial management fraud detection systems may be significantly improved by integrating strong preprocessing methods with modern algorithms, according to the research. To get around the problem of missing values, future study may concentrate on data preparation methods. Furthermore, it would be beneficial to explore various feature extraction and selection approaches in the credit card industry to ascertain their effect on prediction accuracy. In order to find a most accurate hybridised model in a domain indicated earlier, future research should primarily focus on investigating which of the modern ML algorithms is the most suitable.

REFERENCES

[1] S. M. N. Nobel *et al.*, "Unmasking Banking Fraud: Unleashing the Power of Machine Learning and Explainable AI (XAI) on Imbalanced Data," *Inf.*, vol. 15, no. 6, pp. 1–22, 2024, doi: 10.3390/info15060298.

[2] S. A. Pranav Khare*1, "THE IMPACT OF MACHINE LEARNING AND AI ON ENHANCING RISK-BASED IDENTITY VERIFICATION PROCESSES," *Int. Res. J. Mod. Eng. Technol. Sci.*, vol. 06, no. 05, pp. 1–10, 2024.

[3] M. Srokosz, A. Bobyk, B. Ksiezopolski, and M. Wydra, "Machine-Learning-Based Scoring System for Antifraud CISIRTs in Banking Environment," *Electron.*, vol. 12, no. 1, pp. 1–17, 2023, doi: 10.3390/electronics12010251.

[4] S. Arora and P. Khare, "AI/ML-Enabled Optimization of Edge Infrastructure: Enhancing Performance and Security," *Int. J. Adv. Res. Sci. Commun. Technol.*, vol. 4, pp. 230–242, 2024.

[5] M. K. Vinita Rohilla, Sudeshna Chakraborty, "Research Article Artificial Intelligence and Metaheuristic-Based Location-Based Advertising," *scholar.google*, 2022.

[6] P. Khare, "Transforming KYC with AI : A Comprehensive Review of Artificial Intelligence-Based Identity Verification," vol. 10, no. 12, pp. 525–531, 2023.

[7] S. Mathur., "Supervised Machine Learning-Based Classification and Prediction of Breast Cancer," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12(3), pp. 0–3, 2024.

[8] J. K. Afriyie *et al.*, "A supervised machine learning algorithm for detecting and predicting fraud in credit card transactions," *Decis. Anal. J.*, vol. 6, no. November 2022, pp. 1–12, 2023, doi: 10.1016/j.dajour.2023.100163.

[9] S. Arora and S. R. Thota, "Using Artificial Intelligence with Big Data Analytics for Targeted Marketing Campaigns," pp. 593–602, 2024, doi: 10.48175/IJARSCT-18967.

[10] M. H. R Tandon, A Sayed, "Face mask detection model based on deep CNN techniques using AWS," *Int. J. Eng. Res. Appl. www. ijera. com*, vol. 13, no. 5, pp. 12–19, 2023.

[11] P. Khare, "AI-Powered Fraud Prevention : A Comprehensive Analysis of Machine Learning Applications in Online Transactions," vol. 10, no. 9, pp. 518–525, 2023.

[12] S. R. Thota and S. Arora, "Neurosymbolic AI for Explainable Recommendations in Frontend UI Design - Bridging the Gap between Data-Driven and Rule-Based Approaches," no. May, pp. 766–775, 2024.

[13] S. Arora and P. Khare, "Optimizing Software Pricing : AI-driven Strategies for Independent Software Vendors," no. May, pp. 743–753, 2024.

[14] M. Â. L. Moreira *et al.*, "Exploratory analysis and implementation of machine learning techniques for predictive assessment of fraud in banking systems," *Procedia Comput. Sci.*, vol. 214, no. C, pp. 117–124, 2022, doi: 10.1016/j.procs.2022.11.156.

[15] R. Achary and C. J. Shelke, "Fraud Detection in Banking Transactions Using Machine Learning," in *Proceedings of the International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics, ICIITCEE 2023*, 2023. doi: 10.1109/IITCEE57236.2023.10091067.

[16] H. Wang, W. Wang, Y. Liu, and B. Alidaee, "Integrating Machine Learning Algorithms With Quantum Annealing Solvers for Online Fraud Detection," *IEEE Access*, 2022, doi: 10.1109/ACCESS.2022.3190897.

[17] F. Z. El Hlouli, J. Riffi, M. A. Mahraz, A. El Yahyaouy, and H. Tairi, "Credit Card Fraud Detection Based on Multilayer Perceptron and Extreme Learning Machine Architectures," in *2020 International Conference on Intelligent Systems and Computer Vision, ISCV 2020*, 2020. doi: 10.1109/ISCV49265.2020.9204185.

[18] S. K. Hashemi, S. L. Mirtaheri, and S. Greco, "Fraud Detection in Banking Data by Machine Learning Techniques," *IEEE Access*, 2023, doi: 10.1109/ACCESS.2022.3232287.

[19] J. Femila Roseline, G. B. S. R. Naidu, V. Samuthira Pandi, S. Alamelu alias Rajasree, and D. N. Mageswari, "Autonomous credit card fraud detection using machine learning approach☆," *Comput. Electr. Eng.*, 2022, doi: 10.1016/j.compeleceng.2022.108132.

[20] A. Narender Kumar, "Fraud Detection using Machine Learning Algorithms on Financial Transaction Data," *Int. J. Res. Publ. Rev. J. homepage www.ijrpr.com*, vol. 4, no. 8, pp. 2046–2060, 2023, [Online]. Available: www.ijrpr.com

[21] E. F. Malik, K. W. Khaw, B. Belaton, W. P. Wong, and X. Chew, "Credit Card Fraud Detection Using a New Hybrid Machine Learning

Architecture," *Mathematics*, 2022, doi: 10.3390/math10091480.

[22] S. Mathur and S. Gupta, "An Enhanced Edge Detection Using Laplacian Gaussian Filtering Method from Different Denoising Images," *Int. J. Intell. Syst. Appl. Eng.*, vol. 12, no. 18s, pp. 313–323, 2024.

[23] P. C. Y. Cheah, Y. Yang, and B. G. Lee, "Enhancing Financial Fraud Detection through Addressing Class Imbalance Using Hybrid SMOTE-GAN Techniques," *Int. J. Financ. Stud.*, vol. 11, no. 3, pp. 1–17, 2023, doi: 10.3390/ijfs11030110.

[24] J. Thomas, "Optimizing Bio-energy Supply Chain to Achieve Alternative Energy Targets," *J. Electr. Syst.*, vol. 20, no. 6, 2024.

[25] M. T. Islam, K. M. Hasib, M. M. Rahman, A. N. Tusher, M. S. Alam, and M. R. Islam, "Convolutional Auto-Encoder and Independent Component Analysis Based Automatic Place Recognition for Moving Robot in Invariant Season Condition," *Human-Centric Intell. Syst.*, 2022, doi: 10.1007/s44230-022-00013-z.

[26] J. Cui, C. Yan, and C. Wang, "Learning Transaction Cohesiveness for Online Payment Fraud Detection," in *ACM International Conference Proceeding Series*, 2021. doi: 10.1145/3448734.3450489.

[27] X. J. Zhong *et al.*, "Natural alkaloid coptisine, isolated from Coptis chinensis, inhibits fungal growth by disrupting membranes and triggering apoptosis," *Pharmacol. Res. - Mod. Chinese Med.*, 2024, doi: 10.1016/j.prmcm.2024.100383.

[28] M. Rakhshaninejad, M. Fathian, B. Amiri, and N. Yazdanjue, "An Ensemble-Based Credit Card Fraud Detection Algorithm Using an Efficient Voting Strategy," *Comput. J.*, 2022, doi: 10.1093/comjnl/bxab038.

[29] A. A. Taha and S. J. Malebary, "An Intelligent Approach to Credit Card Fraud Detection Using an Optimized Light Gradient Boosting Machine," *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2971354.

[30] and R. N. N.-S. Sini Sunny, jennifer Houg, Shibu Navaneeth, Sayed Aniqa, Afortude John Kofi, "Abstract P2073: Hyperbaric Oxygen Therapy Protects The Myocardium From Reductive Stress-induced Proteotoxic Remodeling," *Circ. Res. logo*, vol. 133, 2023, [Online]. Available: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=afRDlOoAAAAJ&citation_for_view=afRDlOoAAAAJ:9yKSN-GCB0IC

[31] S. C. Vinita Rohilla, Mandeep Kaur, "An Empirical Framework for Recommendation-based Location Services Using Deep Learning," *Eng. Technol. Appl. Sci. Res.*, vol. 12, no. 5, pp. 9186–9191, [Online]. Available: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=zlcFgwEAAAAJ&citation_for_view=zlcFgwEAAAAJ:eQOLeE2rZwMC

[32] Y. Jain, N. Tiwari, S. Dubey, and S. Jain, "A comparative analysis of various credit card fraud detection techniques," *Int. J. Recent Technol. Eng.*, 2019.

[33] V. Rohilla, D. S. Chakraborty, and D. R. kumar, "Random Forest with Harmony Search Optimization for Location Based Advertising," *Int. J. Innov. Technol. Explor. Eng.*, 2019, doi: 10.35940/ijitee.i7761.078919.

[34] M. Zareapoor, S. K. . Seeja.K.R, and M. Afshar Alam, "Analysis on Credit Card Fraud Detection Techniques: Based on Certain Design Criteria," *Int. J. Comput. Appl.*, 2012, doi: 10.5120/8184-1538.

[35] A. Rath, A. Das Gupta, V. Rohilla, A. Balyan, and S. Mann, "Intelligent Smart Waste Management Using Regression Analysis: An Empirical Study," in *Communications in Computer and Information Science*, 2022. doi: 10.1007/978-3-031-07012-9_12.

[36] E. Esenogho, I. D. Mienye, T. G. Swart, K. Aruleba, and G. Obaido, "A Neural Network Ensemble with Feature Engineering for Improved Credit Card Fraud Detection," *IEEE Access*, 2022, doi: 10.1109/ACCESS.2022.3148298.

[37] K. Randhawa, C. K. Loo, M. Seera, C. P. Lim, and A. K. Nandi, "Credit Card Fraud Detection Using AdaBoost and Majority Voting," *IEEE Access*, 2018, doi: 10.1109/ACCESS.2018.2806420.

[38] A. RB and S. K. KR, "Credit card fraud detection using artificial neural network," *Glob. Transitions Proc.*, 2021, doi: 10.1016/j.gltp.2021.01.006.

[39] B. S. A.-N. and S. S. A.-N. Mosa M. M. Megdad, "Fraudulent Financial Transactions Detection Using Machine Learning," *Int. J. Acad. Inf. Syst. Res.*, vol. 6, no. 3, pp. 30–39, 2022.

[40] A. R. Khalid, N. Owoh, O. Uthmani, M. Ashawa, J. Osamor, and J. Adejoh, "Enhancing Credit Card Fraud Detection: An Ensemble Machine Learning Approach," *Big Data Cogn. Comput.*, 2024, doi: 10.3390/bdcc8010006.

[41] S. El Kafhali, M. Tayebi, and H. Sulimani, "An Optimized Deep Learning Approach for Detecting Fraudulent Transactions," *Inf.*, vol. 15, no. 4, pp. 1–25, 2024, doi: 10.3390/info15040227.