Development of a Credit Card Fraud Detection Model

Sholanke Temitope Folasade[1] & Akano Olaitan Mary[2]

Department of Computer Science and Engineering, Obafemi Awolowo University, Ile-Ife
Corresponding Author: **Sholanke Temitope Folasade**

Abstract:
In the era of digitalization, utilization of credit cards is on the rise for acquiring goods through both online and offline avenues. Fraudulent credit card transactions have been on rise nowadays. This study used machine learning algorithms to detect fraudulent activities. The model was trained using machine learning algorithms logistic regression, random forest and xgboost. Implemented was carried out using HTML and CSS as a web application. The algorithms are compared and the one with greatest accuracy, precision, recall, and F1-score is considered the best algorithm for fraud prediction. Our findings indicates that XGboost has the highest accuracy of 99.86%, followed by Random Forest Classification with 99.84% and Logistic Regression with 99.41%.Random forest classification and XG Boost models demonstrated good performance in predicting fraudulent transactions, while the logistic regression model performed poorly in this regard. These results offer insight to target users about the performance of three different fraud detection models.

Keywords: Credit Card, Fraud Detection, Machine Learning, Transaction, Supervised Learning, Goods, Classification, Prediction, Transaction, Algorithms

1.0 Introduction

According to Bloomenthal (2021), a credit card is a thin rectangular piece of plastic or metal issued by a bank or financial services company that allows cardholders to pay for goods and services with merchants that accept cards for payment. Fraud is a misleading conduct done by someone, with the objective to get an illegal advantage or to harm someone else's (victim's) rights. Fraud detection involves monitoring the activities of populations of users in order to estimate, perceive or avoid objectionable behavior, which consist of fraud, intrusion, and defaulting. The detection model uses machine learning to recognize unusual credit card transactions and fraud. Credit card fraud detection is one of the most explored domains of fraud detection (Bolton *et al,* 2021) and relies on the automatic analysis of recorded transactions to detect fraudulent behavior.

Machine learning algorithms are employed to analyze all the authorized transactions and report the suspicious ones. Credit Card Fraud detection models identify suspicious events and report them to an analyst while letting normal transactions be automatically processed, the use of machine learning brings significant improvements to the process. Machine Learning uses two techniques, supervised or unsupervisedlearning. Supervised learning means that a model learns from previous examples and is trained on labeled data. Supervised learning uses the whole labeled dataset for training. The labels are known since card holders did identify the mismatch of a transaction, or an unusual transaction being identified by a credit card agency and confirmed by a credit card holder. The supervised methods have this disadvantage that if fraudsters change their patterns, (Mahdi, 2020) these models might not be able to detect them based on the old observations. In this case, training datasets come without any labels or instructions. This approach lags behind supervised

learning in terms of accuracy. But it is unrivaled when a business needs to find hidden fraud patterns and useful insights. This particular system uses supervised learning to detect fraud.

2.0 Review of Related Works

Uloko*et al.* (2021) in their work used machine learning to detect credit card fraud. The study aimed at providing solutions by examining various methods previously used for fraud detection, bringing out their strengths and weaknesses. It utilizes the strength of the Random Forest Algorithm. Random Forest is an algorithm for classification and regression. It is an ensemble of decision tree classifiers. The output of the Random Forest classifier is the majority vote amongst the set of tree classifiers. To train each tree, a subset of the full training set is sampled randomly. Then, a decision tree is built in the normal way, except that no pruning is done and each node splits off the full feature set. Training is fast, even for large data sets with many features and data instances, because each tree is trained independently of the others. The Random Forest algorithm has been found to be resistant to overfitting and provides error (without having to do cross-validation) through the "out-of-bag" error rate that it returns. The model recorded an accuracy of 99.9% and also figures of 1.000, 0.500 and 0.200 gotten from the Sensitivity, Specificity and False Alarm tests. Parmar*et al,* (2020) explores the presentation of K-Nearest Neighbor, Decision Trees, Support Vector Machine (SVM), Logistic Regression, Random Forest, and XGBoost for credit card fraud detection. Dataset of credit card transactions is accrued from Kaggle and it includes a sum of 2,84,808 credit card transactions of an EU financial institution dataset. It depicts doubtful transactions as fraud and labels it "high quality class" and actual ones as the "poor class".To figure out the best algorithm is generally appropriate for the issue of distinguishing fraud instances, various measures for algorithm checking have been utilized. Often utilized measurements for deciding the consequences of ML algorithms are Precision and F1 Score. The examination concluded that KNN gives the best outcomes for the given example and gives the exact classification of whether transactions are fraud or not. The set up utilizes various evaluation metrics, for example, precision and F1 Score. Selection of features and dataset balancing have demonstrated to be critical in accomplishing critical outcomes. The future work should be contributed towards finding out about resampling strategies that will support us with decreasing skewness proportion of the datasets and apply deep learning procedures.

Benchaji*et al.,* (2021) worked on credit card fraud detection model based on LSTM Recurrent Neural Networks.The work aimed to capture the historic purchase behavior of credit card holders with the goal of improving fraud detection accuracy on new incoming transactions. It employs long short-term memory (LSTM) networks as a sequence learner to include transaction sequences. It has an accuracy of 99.5%. The work of Saini *et al.* (2020), used machine learning algorithms called outliers such as Local Outlier Factor and Isolation Forest Algorithm to detect anomalous activities with the aim of detecting fraudulent transactions while minimizing the incorrect fraud classifications. The algorithms are a part of sklearn. The ensemble module in the sklearn package includes ensemble-based methods and functions for the classification, regression and outlier detection. Local Outlier Factor is an unsupervised outlier detection algorithm. 'Local Outlier Factor' refers to the anomaly score of each sample. It measures the local deviation of the sample data with respect to its neighbors. More precisely, locality is given by k-nearest neighbors, whose distance is used to estimate the local data. The Isolation Forest 'isolates' observations by arbitrarily selecting a feature and then randomly selecting a split value between the maximum and minimum values of the designated feature. Recursive partitioning can be represented by a tree, the number of splits required to isolate a sample is equivalent to the path length root node to the terminating node. The average of this path length gives a measure of normality and the decision function which we use. Once the anomalies are detected, the system can be used to report them to the concerned authorities.

3.0 Methodology

In developing a credit card fraud detection model, the dataset was collectedfrom a German bank dating back to 2006. The dataset consists of 10 rows and 23 columns, each row represents one instance or data point, and there are 10 such rows in the dataset. The number of columns (23 in this case) refers to the different attributes or features associated with each instance. The dataset comprises valuable fraudulent measurements, including,

i. trans_date_trans_time
ii. cc_num
iii. merchant
iv. category
v. amt
vi. first
vii. last
viii. gender
ix. street
x. city
xi. state
xii. zip
xiii. lat
xiv. long
xv. city_pop
xvi. job
xvii. dob
xviii. trans_num
xix. unix_time
xx. merch_lat
xxi. merch_long
xxii. is_fraud

An essential component within the dataset is the target variable, denoted as "is_fraud." This binary attribute holds significant importance in the context of credit card fraud detection, as it signifies whether a transaction is indicative of fraud or not. To streamline the classification procedure, the "is_fraud" variable is encoded with the values 0 and 1, representing the absence or presence of fraud, respectively. This distinct categorization enables supervised learning algorithms to glean insights from the data and formulate precise forecasts based on the predefined target categories. The dataset was further preprocessed through data cleaning, data transformation and feature selection. The data was split into train and test using the machine learning algorithms logistic regression, random forest and xgboost.

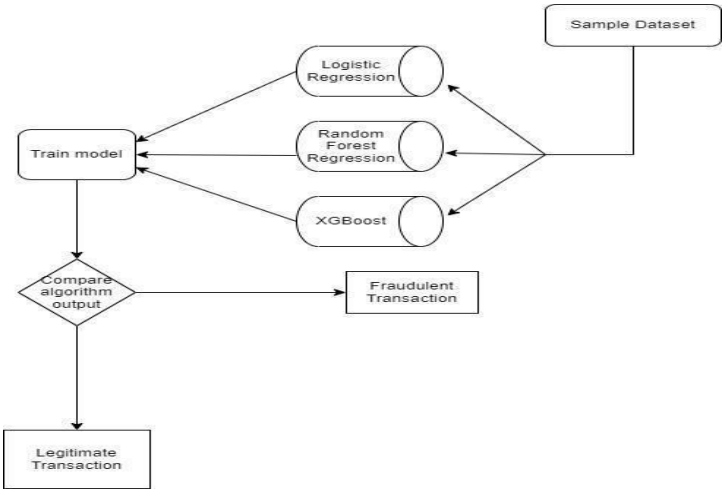

Figure 1: Proposed Model

Logistic regression is a statistical method used for binary classification, which involves predicting outcomes that fall into two distinct classes. The goal is to model the probability that a given input belongs to a specific class. The output of the logistic regression model is a logistic function (also called the sigmoid function), which maps any input value to a value between 0 and 1. This output can be interpreted as the estimated probability of the input belonging to the positive class.

Mathematically, logistic regression can be expressed as:

$P(y=1 \mid X) = 1 / (1 + e^{(-z)})$

Where:
- $P(y=1 \mid X)$ is the probability of the input belonging to the positive class.
- X represents the input features.
- e is the base of the natural logarithm.
- z is a linear combination of the input features and their associated weights.

The model is trained by finding the best set of weights that minimizes a specific loss function, often the logistic loss (also known as cross-entropy loss), which quantifies the difference between the predicted probabilities and the actual class labels.

Random Forest is a powerful and versatile ensemble learning technique used for classification and regression tasks in machine learning. It's particularly effective in handling complex datasets and improving prediction accuracy. Random Forest is an ensemble of decision trees, where each tree is built using a random subset of the data and a random subset of the features. Random Forests are widely used across various domains, including finance, healthcare, and natural language processing.

XGBoost, which stands for "Extreme Gradient Boosting," is a popular and highly effective machine learning algorithm that belongs to the gradient boosting family. It's designed for both classification and regression tasks and has gained significant attention and success in various machine learning competitions and real-world applications. XGBoost's popularity can be attributed to its exceptional predictive performance and its ability to handle complex datasets. The model was evaluated by getting the accuracy and visualized using a confusion

matrix. Furthermore, the model was implemented using HTML and CSS for client-side scripting. In testing the application, usability testing was conducted.

4.0 Results and Discussion

The code prints out the number of false positives it detected and compares it with the actual values. This is used to calculate the accuracy score and precision of the algorithms. These results along with the classification report for each algorithm is given in the output as follows, where class 0 means the transaction was determined to be valid and 1 means it was determined as a fraud transaction. Figure 2 shows the accuracy and confusion matrix of logistic regression. It has a precision and recall of 0.00, and an F1-score of 0.00 for the fraudulent class, the precision for class 0 (non-fraudulent transactions) is 0.99, indicating a high proportion of correctly predicted non-fraudulent transactions.

However, the precision for class 1 (fraudulent transactions) is 0.00, which means that none of the predicted fraudulent transactions were actually classified correctly. Figure 3 shows the accuracy and confusion matrix of the random forest algorithm. It achieved a precision of 0.96, recall of 0.77, and F1-score of 0.85 for the fraudulent class, which indicate that the model accurately predicted a significant majority of fraudulent transactions, the precision for class 0 (non-fraudulent transactions) is 1.00, indicating a high proportion of correctly predicted non-fraudulent transactions. Figure 4 shows the evaluation of xgboost algorithm. It achieved a precision of 0.94, recall of 0.83, and F1-score of 0.88 for the fraudulent class. These metrics indicate that the model also performed well in detecting fraudulent transactions, the precision for class 0 (non-fraudulent transactions) is 1.00, indicating a high proportion of correctly predicted non-fraudulent transactions. The precision for class 1 (fraudulent transactions) is 0.94, which means that a significant majority of the predicted fraudulent transactions were classified correctly.

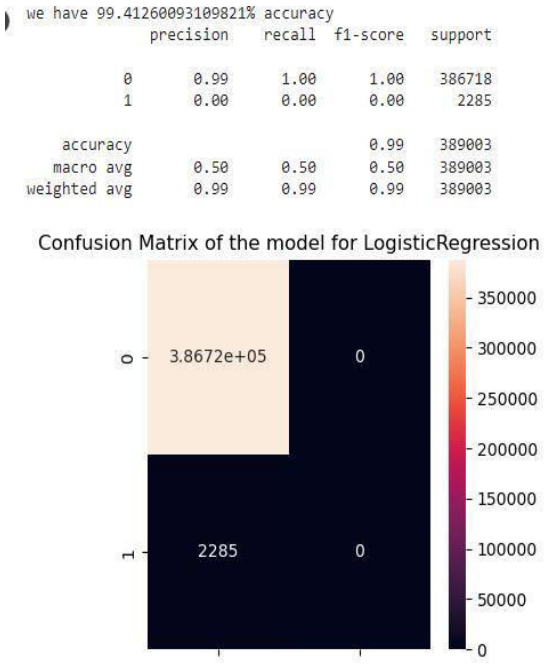

Figure 2: **Confusion matrix of Logic Regression Algorithm**

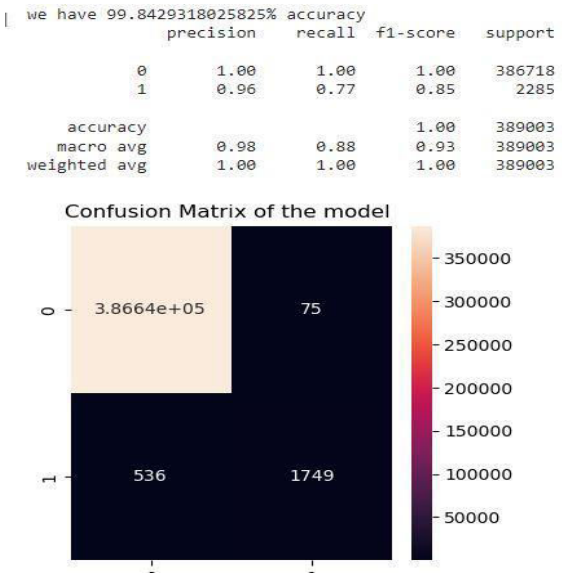

Figure 3: Confusion matrix of Random Forest Algorithm

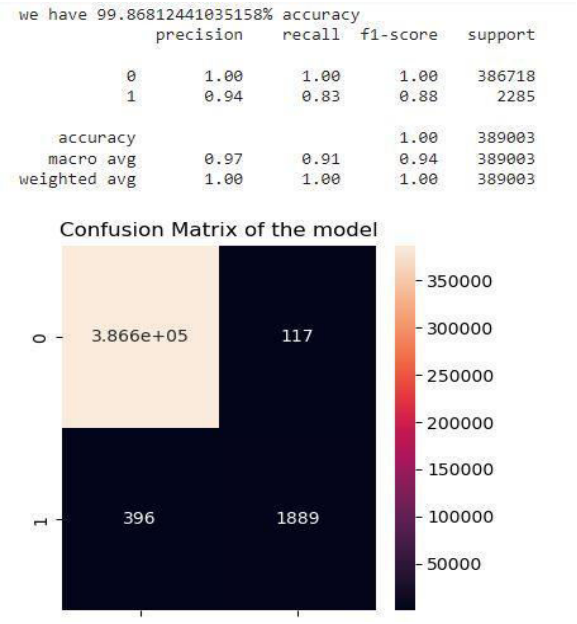

Figure 4: Confusion matrix of Xgboost Algorithm

4. 1 Graphical User Interface

This section shows the various modules that make up the interface of the mobile application with which users can interact with the system. Figure 5 shows the detection page of the web application, where the required inputs are filled and the result of the input field is then shown in figure 6.

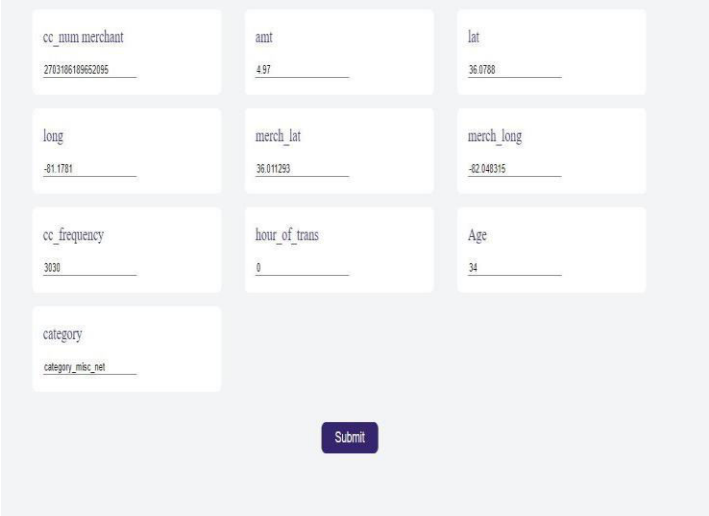

Figure 5: Detection Page

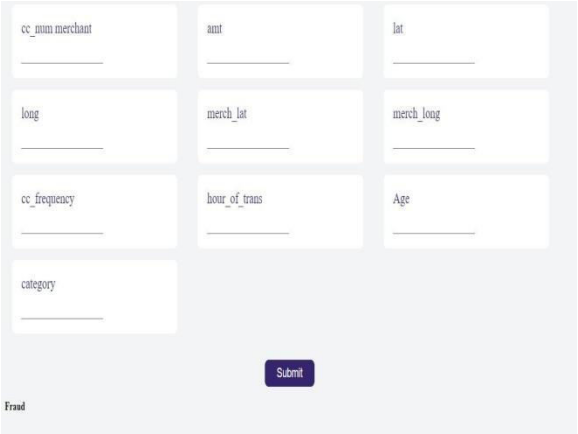

Figure 6: **Result page**

4.2 Result Evaluation

The web application developed was evaluated by 10 participants randomly selected from the previous population. The analysis of the responses indicated that about 75% found the web app user friendly. Also 80% users found the web app easy to navigate. About 80% of users did not experience lag when using the web app. System Usability Scale (SUS) returned 85.5% score out of maximum of 100 on the application usability score.

5.0 Conclusion

Credit card fraud represents a clear instance of criminal deceit. Within this work done, a comprehensive compilation of prevalent fraudulent techniques has been presented, accompanied by their respective methods of identification. Recent advancements in this realm have been examined and analyzed. This study offers an intricate exposition on the application of machine learning to enhance the efficacy of fraud detection. It expounds upon the algorithm employed, its pseudocode, implementation elucidation, and the outcomes of experimental trials. Random forest classification and XGBoost models are noted to have demonstrated good

performance in predicting fraudulent transactions, while the logistic regression model performed poorly in this regard. This indicates that the model struggled to correctly identify fraudulent transactions. XGboost has the highest accuracy of 99.86%, followed by Random Forest Classification with 99.84% and Logistic Regression with 99.41%.

6. 0 Recommendation and Future Work

Future work can be tailored towards researchers extending the model to handle multiple classes of credit cards (e.g. Visa, MasterCard, American Express etc.) and also consider creating an ensemble of multiple models to leverage the strengths of different models and improve overall prediction accuracy.

References

1. Alfaiz N. S. and Suliman M. F. (2022). Enhanced Credit Card Fraud Detection Model Using Machine Learning. *Multidisciplinary Digital Publishing Institute.* 11, 662.
2. Alharbi A., Alshammar M., Okon O., Amerah A., Rauf H., Alyami, H. and Meraj T. (2022). A Novel text2IMG Mechanism of Credit Card Fraud Detection:A Deep Learning Approach. *Multidisciplinary Digital Publishing Institute.* 11(5), pp.756.
3. Anusiba O., Okechukwu O., Ekwealor, O. and Anusiba A. (2022). The Application of Hidden Markov Model in Credit Card Fraud Detection System. *International Journal of Innovative Science and Research Technology.* 10(2), 2347-4890.
4. Ayoub M. and Khalid J. (2022). Credit Card Fraud Detection by Improved SVDD,*Proceedings of the World Congress on Engineering.* 8(9), pp.32-37.
5. Benchaji I., Samira, D. and Bouabid O. (2021). Credit Card Fraud Detection Model Based on LSTM Recurrent Neural Networks. *Journal of Advances in Information Technology.* 12(2), pp.113-118.
6. Bloomenthal, A. (2021). Credit Card: What It Is, How It Works, and How to Get One, www.investopedia.com
7. Fati, S. and Alfaiz N. (2022). Enhanced Credit Card Fraud Detection Model Using MachineLearning. *Multidisciplinary Digital Publishing Institute.* 11(4), pp.66.
8. Fayomi A., Eleyan, D. and Eleyan A. (2021). A Survey Paper On Credit Card Fraud Detection Techniques. *Research Gate*. 10(09), pp.72-79.
9. Mahdi R. (2019). Anomaly Detection using Unsupervised Methods: Credit Card Fraud Study. *International Journal of Advanced Computer Science and Applications.* 10(11).
10. Li W., Wu, C. and Ruan S. (2022). CUS-RF-Based Credit Card Fraud Detection with imbalanced Data. *Journal of Risk Analysis and Crisis Response.* 12(3), pp.110-123.
11. Parmar J., Patel, A. and Savsani M. (2021). Credit Card Fraud Detection Framework-A Machine Learning Perspective. *International Journal of Advanced Computer Science and Applications.* 7(6), pp.431-435.
12. Saini A., Sarkar, S. and Ahmed S. (2020). Credit Card Fraud Detection Using Machine Learning and Data Science. *International Journal of Scientific Research in Science and Technology.* 8(9).
13. Swarna, B., and Shivaleela, S. (2021). Credit Card Fraud Detection System Using MachineLearning. *Journal of Emerging Technologies and Innovative Research.* 8(7): 2349-5162.

14. Trivedi1 N., Sarita S., Lilhore, U., and Sharma, S. (2020). An Efficient Credit Card Fraud Detection Model Based on Machine Learning Methods. *International Journal of Advanced Science and Technology*. 29(5), pp. 3414 – 3424.
15. Uloko F., John-Wendy N., Abu, I. and Osayande B. (2021). Analysis Of Machine Learning Credit Card FraudDetectionModels. *Global Scientific Journals.* 9(8), pp.2320-9186.
16. Vaishnavi, N. and Geetha S. (2019). Credit Card Fraud Detection using Machine Learning Algorithm. *Procedia Computer Science.* 165, pp.631-641.
17. Zhang Y., Lu H., Lin H., Qiao, X., and Zheng H. (2022). The Optimized Anomaly Detection Models Based on an Approach of Dealing with Imbalanced Dataset for Credit Card Fraud Detection. *Mobile Information Systems*. ID: 8027903.