PJEST

Article

Fraud Detection of Credit Cards Using Supervised Machine Learning Techniques

Ammarah Urooj Aftab [1], Iqra Shahzad [2], Amna Sajid [2,*], Maira Anwar [3] and Nosheen Anwar [4]

[1] Military College of Signals, NUST Rawalpindi; e-mail: ammarah.arooj96@gmail.com
[2] National University of Modern Languages, Islamabad; iqra.shahzad@numl.edu.pk
[2] National University of Modern Languages, Islamabad; amna.sajid@numl.edu.pk
[3] Military College of Signals, NUST Rawalpindi; mairaanwar148@gmail.com
[4] PMAS- arid agriculture university Rawalpindi; nosheen.anwar@gmail.com
* Correspondence: amna.sajid@numl.edu.pk

ABSTRACT: Credit card fraud encompasses illicit activities aimed at unlawfully obtaining confidential information to enable unauthorized individuals to engage in illegal transactions. As technology advances, fraudsters have honed their skills in evading security measures, presenting a formidable challenge in fraud detection. To address this issue, an array of algorithms and analytical techniques has emerged to identify and mitigate instances of fraud. This research aimed to identify the most appropriate supervised machine learning algorithm for credit card fraud detection. Logistic Regression, Random Forest, Support Vector Machine, and Decision Trees were implemented and compared. Due to the imbalanced nature of the dataset, the SMOTE (Synthetic Minority Oversampling Technique) technique was employed to rectify the data imbalance by oversampling the minority class. The performance of the trained models was evaluated using various metrics, including the confusion matrix, accuracy, precision, recall, f1-score, Matthews Correlation Coefficient (MCC), and Area Under the Curve (AUC). The results of the analysis revealed that Random Forests exhibited exceptional performance, achieving an impressive recall score of 84% and surpassing other algorithms. This research provides the groundwork for future investigations involving diverse deep-learning techniques applied to real-time and dynamic datasets, enabling continuous enhancements in fraud detection and prevention mechanisms.

Keywords: Credit card, fraud detection, machine learning, supervised learning, logistic regression, decision tree, support vector machine, random forest, SMOTE

Citation: Aftab, A. U., Shahzad, I., Anwar, M., Sajid, A., & Anwar, N. Fraud Detection of Credit Cards Using Supervised Machine Learning. *Pakistan Journal of Emerging Science and Technologies (PJEST)*, 4(3). https://doi.org/10.58619/pjest.v4i3.114

Academic Editor: Dr. M. Javaid Afzal

Received date: 28th May, 2023
Revised date: 9th June, 2023
Accepted date: 10th June,2023
Published date: 28th June, 2023

Pakistan Journal Emerging Sciences and Technologies (PJEST) in collaboration with Govt. Islamia College Civil Lines Lahore, Pakistan is licensed under a Creative Commons Attribution-ShareAlike 4.0 International License

Introduction

Credit card fraud is an unauthorized act categorized as the use of someone else accounts illegally. These frauds have happened since online payments and credit cards began. Defrauders have found exceptional ways to exploit sensitive account information for their purposes. These frauds are a big threat to the banking and IT departments that are working to improve their detection systems using various IT technologies. There are different methods to commit fraud, such as identity theft, which is committed by using someone's personal information. Duplicate cards, also called fake cards, are developed by skimming actual data from the credit card. In recent years, the number of users and transaction rates have increased. Hence, the number of frauds and card thefts. With the increased digital payments, financial institutions have lost billions due to credit card fraud. According to Nelson's report, the most trusted source of global news, the global damage caused by credit card fraud was 21 billion in 2015. According to some studies, 1.8 billion dollars was lost by fraudulent transactions conducted in 2016, and 21 billion dollars was lost in 2020 using credit cards. The USA alone suffered from credit card fraud in 2018 [1]. Due to this ever-growing problem, bank and finance departments face challenges in

building effective and proactive fraud detection systems. Stolen cards are also misused if found by dishonest people, as shown in Fig. 1 below.

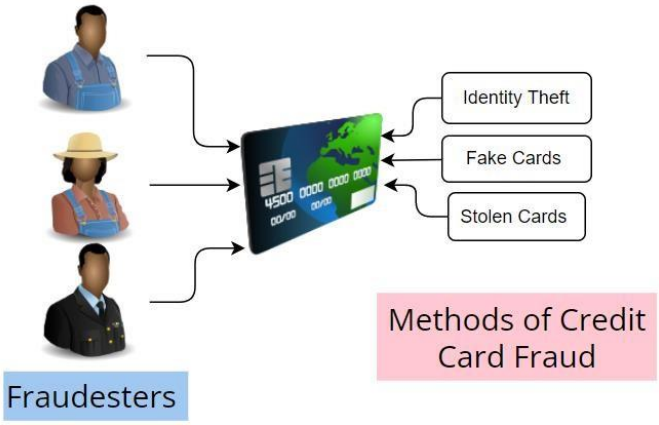

Fig. 1: Methods to commit credit card fraud

Machine learning represents a promising solution to deal with this problem [2]. Detecting fraudulent activities using traditional methods of manual detection is time-consuming and inefficient, moreover, the introduction of big data has made manual methods more unfeasible. Various limitations or challenges that are responsible for the difficulty in credit card detection are:

a. Data sets are not easily accessible

b. Imbalanced dataset

c. Shaping the appropriate evaluation technique

d. Vibrant behavior of fraudsters

e. The size of the datasets

Credit card fraud detection is the process of identifying transactions into two classes one is genuine/normal transactions, and the other is fraudulent transactions [3] [4]. There are mainly two types of credit card fraud, one is the theft of the physical card, and the other is stealing sensitive information from the card, such as accessing card numbers or account passwords, and then misusing this data for fraud. Many strategies can be used in the fraud detection process. As every fraud incident has certain individualities, environmental conditions, and personal behavior, frauds can be detected if there is a good understanding of these characteristics in each fraud condition [5]. With the help of machine learning and deep Learning methods, fraudulent activity can be stopped before the transaction is approved because a secured and trusted banking system requires highly sped verification and authentication mechanisms that allow legitimate users to conduct their transactions easily [6] [7].

SMOTE has been widely used and shown promising results in various studies. The effectiveness of SMOTE or any other sampling technique may vary depending on the dataset and the specific problem at hand. Experimenting with different techniques and evaluating their performance on specific datasets is always recommended to determine the most suitable approach.

This research used a real-world imbalanced dataset for creating a machine learning (ML) based framework for credit card fraud detection. The basic purpose of this paper is to perform a comparative analysis to detect the best suitable method for credit card fraud detection using machine learning. For this purpose, machine-learning classification algorithms are tested to verify which is the best suitable method for detecting credit card fraud. The chosen data was a highly imbalanced dataset which caused biased results due to which SMOTE technique for handling an imbalanced dataset was used. Moreover, undersampling was also applied, but better accuracy and results were gained from oversampling. Different machine learning classifiers have been applied, such as Logistic Regression, Decision Tree, Random Forest, and SVM, for the evaluation of the proposed framework. Each of these ML techniques was assessed individually for efficiency and accuracy in classification. This paper's main contribution is a comparative research of various ML techniques on a publicly accessible skewed dataset with real word card transactions. This comparative analysis was performed to check which ML classification techniques will be applied to detect and classify fraudulent transactions. It was applied to an imbalanced synthetic dataset to test the effectiveness of the proposed credit card fraud detection framework.

This paper is organized as follows: section II discusses the literature review and its comparative analysis. Section III provides the proposed methodology and details the implementation of the proposed techniques. In section IV, results have been discussed, and in section V, conclusions and future work are discussed.

Related Work

Machine learning is a subclass of Artificial Intelligence and is a mixture of numerous computer algorithms and statistical modeling to allow the computer to accomplish tasks without hard coding. Ultimately, it is an estimate from stored observed knowledge. Deep learning is a part of Machine learning techniques that have the competency to capture exclusive associations over the entire dataset. One of the main challenges to applying ML in fraud detection is the highly uneven nature of datasets, as there is a smaller number of fraudulent transactions in the dataset as compared to genuine transactions. Researchers face this issue while designing an accurate detection system using ML techniques [8]. This paper aims to apply various supervised machine learning methods and perform a comparative analysis using different evaluation metrics to identify the best suitable method for credit card fraud detection. ML methods like Logistic Regression, Support vector machine, Decision Tree, and Random Forest are used to study datasets containing thousands of transactions and differentiate them by tracking the valid transactions from the fraudulent ones. Fraud detection systems require identifying the fraudulent and normal transaction before it happens; hence, this research will help select the best suitable supervised ML technique for fraud detection systems to attain better and more accurate predictions in time and quality.

Popat et al. [9] identified that machine learning was declared the best technique compared to clustering, outlier detection, prediction, etc. Machine learning techniques were preferred as the most efficient for detecting fraud as they give higher accuracy and detection rate. For detecting credit card fraud, there are several techniques based on deep learning (DL) that were discussed in this paper, such as Naïve Bayes (NB), SVM, Neural networks, K- Nearest Neighbor (KNN), Decision Tree, data mining, etc. However, researchers struggle to find the best technique to achieve more accuracy and detection rate.

Logistics Regression (LR) and K-fold machine learning methods were used for fraud detection. The K- fold method was used to generate numerous folds of transactions before applying ML techniques [10]. The ROC curve (Receiver Operating Characteristic curve), confusion matrix, and precision-recall were used to evaluate the proposed methodology's performance. During the experiment, it was discovered that the Random Forest decision tree method provides the best results in terms of precision and accuracy. However, it was also noticed that Random Forest suffers from tree overfitting in memory due to its large data size.

In a study [11], extremely skewed credit card fraud data were used, and the performance of different algorithms, including K-Nearest-Neighbor, Naive Bayes, and Logistic regression, was analyzed. The technique applied to the dataset combined oversampling and undersampling. The performance was gauged based on different evaluation metrics such as precision, accuracy, and Balanced Classification Rate (BCR). The result shows that K-Nearest neighbor, Naive Bayes, and Logistic regression classifiers performed well with an accuracy of 97.92%, 97.69%, and 54.86%, respectively. After comparative analysis with this article, KNN was found to be better in performance than naive Bayes and logistic regression models.

M. Ashraf et al. [12] talk about the experiment conducted on the real dataset of the largest banks in the private sector. In the experiment, a total of five methods were applied to these data to categorize a transaction as authentic or fraudulent; three of them were ML models, i.e., Random Forest, Logistic Regression, KNN, and two of them were DL techniques, i.e., Deep Neural Network (DNN) and Convolutional Neural Network (CNN). Each technique's results were estimated using different evaluation metrics, including accuracy, recall, and precision. After a comparative analysis of the final results, it was noticed that the overall random forest algorithm gives the best results, whether it knows the transaction made is legitimate or fraudulent. Further research and monitoring are required in DL techniques that might deliver even better results.

Data mining (DM) and Payment Log Analysis (PLA) were used in the [13] study to detect abnormal transactions in the dataset. In this paper, python programming along with Apache Spark was used for complex processing of data and to obtain higher accuracy results. The accuracy result of this paper was 92%, which shows the consequence of algorithms used over the dataset when a proficient classification is performed. In the future, the deep learning concept can also be applied to this dataset using co-evolution networks for more accurate results. Also, some other datasets can be used to test the proposed mechanism further.

Makki et al. [14] determined which unbalanced categorization techniques are most effective at catching credit card fraud. To imitate uneven data found in the real world, the researchers conducted experiments using a highly skewed synthetic dataset. To evaluate the effectiveness of the categorization approaches, they used performance indicators such as precision, recall, F1-Score, and accuracy.

Li et al. [15] suggested a hybrid technique with dynamic weighted entropy to overcome the difficulties of class imbalance and overlap in credit card fraud detection. The technique seeks to manage instances where it is difficult to distinguish between genuine and fraudulent transactions because they have similar characteristics. The suggested method uses dynamic weighted entropy to assign various weights to various features based on their ability to discriminate, which helps lessen the overlap effect. By tackling class

imbalance and overlap issues, the project, which focuses specifically on credit card fraud detection, seeks to improve the precision and dependability of detection systems.

Zhu et al. [16] examined real-world credit card transaction data and evaluated the performance of the optimized WELMs using various evaluation metrics, such as precision, recall, F1-Score, and accuracy. The findings provide insights into the effectiveness of the proposed optimization techniques and their application to credit card fraud detection.

Using the dataset of European cardholders, Rajora et al. [17] conducted a comparison study of ML techniques for credit card fraud detection. The RF and kNN approaches are a couple of techniques that were looked into. The authors' primary performance indicators were the area under the curve (AUC) and accuracy. The outcomes showed that the RF algorithm had an AUC of 0.94 and an accuracy of 94.9%. The accuracy and AUC of the kNN, in contrast, were 93.2% and 0.93, respectively. The class imbalance problem that occurs in the dataset used in this study was not investigated, although the results are encouraging.

By improving the precision and dependability of fraud detection systems, this study [18] also advances the field of credit card fraud detection. The results highlight the significance of algorithm optimization and feature selection to handle skewed data in credit card fraud detection scenarios properly. Table 1 below explains the comparative analysis of the literature review studied and also explains the techniques used with the traditional ones.

Table I: Comparative Analysis of Literature

Reference	Key Points
Popat et al. [9]	Machine Learning techniques were found to be the most efficient for credit card fraud detection, with higher accuracy and detection rates. Techniques discussed included Naïve Bayes, SVM, Neural networks, K-Nearest Neighbor, Decision Tree, and data mining. The search for the best technique with improved accuracy and detection rate continues.
[10]	Fraud detection techniques included k-Fold Machine Learning and Logistic Regression (LR). Before using ML techniques, the K-fold approach was used to create many folds of transactions. Precision-recall, confusion matrix, and ROC curve were used for performance evaluation. Although it suffered from tree overfitting due to enormous data size, the Random Forest decision tree demonstrated the greatest results in terms of precision and accuracy.
Makki et al. [14]	The study aimed to compare the efficiency of various unbalanced classification methods for identifying credit card fraud. Performance measurements like precision, recall, F1-Score, and accuracy and highly skewed synthetic datasets were used.

Li et al. [15]	A hybrid approach with dynamic weighted entropy was presented to solve class imbalance and overlap in credit card fraud detection. The technique used dynamic weighted entropy to give different weights to characteristics according to their ability to discriminate. The study aims to increase fraud detection systems' accuracy and dependability.
[11]	Using highly skewed credit card fraud data, the study evaluated the performance of various algorithms, including K-Nearest Neighbour, Naive Bayes, and Logistic Regression. The dataset was subjected to a combination of oversampling and undersampling methods. The Balanced Classification Rate (BCR), precision, and accuracy were employed as evaluation measures. Regarding performance, K-Nearest Neighbour was superior to Logistic Regression and Naive Bayes.
Zhu et al. [16]	The Weighted Extreme Learning Machines (WELMs) used in the study were tested for their efficacy in detecting credit card fraud using a variety of evaluation indicators. Accuracy, recall, F1-Score, and precision were used. The results revealed information about the efficiency of the optimization methods.
[18]	This study aimed to address the class imbalance and optimize algorithms to increase the accuracy and dependability of credit card fraud detection systems. The significance of feature selection and algorithm optimization was emphasized.
[13]	Data Mining (DM) and Payment Log Analysis were used to find unusual transactions in the dataset. Data processing was done using Apache Spark and Python programming. The study had a 92% accuracy rate and advised using deep learning principles to get more precise results.
Rajora et al. [17]	Using a dataset of European cardholders, ML approaches, including Random Forest (RF) and k-Nearest Neighbour (kNN), were tested for credit card fraud detection. The main performance metrics were AUC and accuracy. While kNN's AUC was 0.93 and its accuracy was 93.2%, the RF algorithm's AUC was 0.94, and its accuracy was 94.9%. The issue of class disparity wasn't specifically looked into.
Ashraf et al. [12]	The study applied five techniques—Random Forest, Logistic Regression, K-Nearest Neighbour, Deep Neural Network (DNN), and Convolutional Neural Network (CNN)—in trials on a real dataset from a private sector bank to classify fraud. Precision, recall, and accuracy were evaluation metrics. The Random Forest Algorithm produced the best results, while DL approaches needed further study and supervision.

Proposed Framework

The methodology is focused on detecting credit card fraudulent transactions using the supervised machine learning algorithms which are Logistic Regression, Support Vector Machine(SVM), Decision Tree, and Random Forest. The proposed architecture consists of preprocessing of the dataset, which includes splitting the dataset and oversampling to balance the skewed data, training the various ML models, and then getting the predictions. The performance of different classifiers is analyzed through the evaluation metrices.

A framework/methodology was proposed for detecting credit card fraud that is reliable and efficient. The proposed framework is shown in Fig. 2.

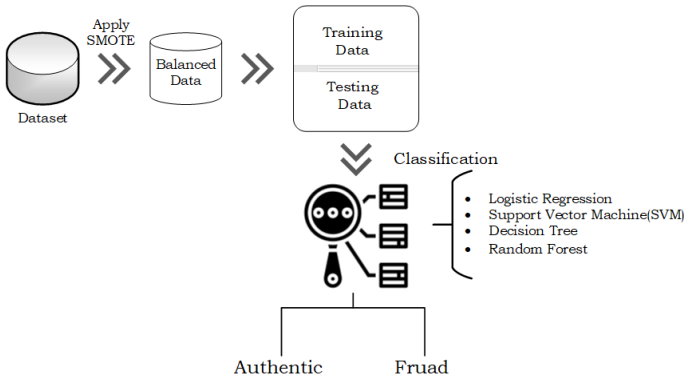

Fig. 2: Proposed Methodology

- The data set chosen is a real-world dataset European credit card holders produced. Out of the 284,807 total transactions, 492 are fraudulent ones.

- Applying the oversampling SMOTE technique to address the class imbalance in credit card fraud datasets since the dataset is significantly skewed and imbalanced.

- Extracted was a balanced dataset with an equal ratio of fraudulent and non-fraudulent/legitimate transactions.

- Division of dataset into training and test data.

- Testing ML algorithms Logistic Regression, Decision Tree, Random Forest, and SVM to elevate the performance of the proposed framework.

- To conduct a comparative analysis using the following metrics: F1 score, accuracy, recall, and precision.

The performance metrics used to assess the effectiveness of the proposed approaches include precision-recall, F1-Score, and accuracy to see the results. For this purpose, a highly skewed dataset was used. These ML techniques were assessed individually to verify effectiveness and classification quality. For detecting credit card fraud, our study uses a highly unbalanced synthetic dataset; this may provide a special dimension to this research. This study aims to fill and identify the existing and significant gaps in the existing body of knowledge. The implementation process of ML techniques to get accurate predictions for fraud detection consists of the following steps shown in Fig. 3.

- Import required libraries

- Read the dataset
- Empirical data analysis (finding null and duplicate values)
- Selecting features and target columns
- Split the dataset (Train & Test)
- Balancing the dataset with SMOTE
- Train the model
- Test the model
- Evaluate the model

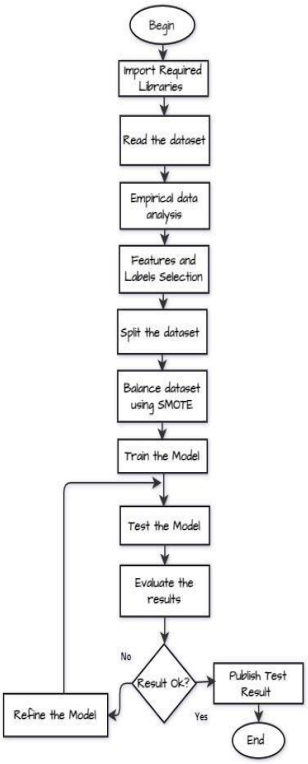

Fig. 3: Implementation Process

Dataset

European credit card dataset [19] was used for this research. This dataset contains the transactions made through credit cards in 2 days in September 2013 by credit cardholders. This dataset was highly imbalanced and contained 492 fraudulent transactions out of a total of 284,807 transactions. The dataset contains the 'class' feature, which shows whether a transaction is a fraud or not, i.e., 0 shows the transaction is non-fraudulent, and 1 shows the transaction is fraudulent. The dataset was highly imbalanced as the ratio of fraudulent transactions is much less than normal. Therefore, preprocessing of data was required to achieve better performance results.

PJEST

Preprocessing

The dataset was highly imbalanced, to normalize the dataset SMOTE (Synthetic Minority Oversampling Technique) method was applied which is effective for imbalanced datasets [20]. After oversampling, Table I shows a dataset containing an equal distribution of fraudulent and non-fraudulent/legitimate transactions.

Table II: Dataset distribution before and after sampling

Results	Before Sampling	After Sampling
Fraud Cases	1.78%	50%
Legitimate cases	98.22%	50%

Implementation

Implementing detection algorithms is done in Python using various libraries like Pandas, NumPy, Matplotlib, Seaborn, Sklearn, and Imblearn. Credit card fraud detection is a classification problem, i.e., the class feature in the dataset represents whether a transaction is fraudulent or genuine. Supervised machine learning algorithms are used for implementation. This experiment was conducted in Jupyter, using the Anaconda platform. We have selected logistic regression, random forest, decision tree, and SVM for implementation and made a comparison on the basis of evaluation metrics.

Logistic regression is a supervised learning model. It predicts the output of a binary dependent variable and one or more independent variables. Random forest algorithm is suitable for large datasets as it gives better predictions when there are more trees in the forest. Results are built for each decision tree in the forest, and then tree results are combined to get better predictions. Decision tree algorithms use the trees for predictions. The decision tree contains two nodes, namely decision nodes and leaf nodes. Decision nodes have multiple children and are used to make decisions, while leaf nodes have no children, which are the outcome of the decisions. It uses the features of the given dataset and predicts the outcomes. The support vector machine (SVM) algorithm is mostly used for classification problems. SVM chooses support vectors that help create hyperplane decision boundaries that segregate the data points into correct classes.

Evaluation Metrices

For the evaluation of the proposed framework, the applied classifiers were evaluated via accuracy, precision, recall, and f1-score. The main evaluation metrics were AUC (Area Under the Curve) and MCC (Matthews Correlation Coefficient), as accuracy is not considered to be the most suitable metric when dealing with imbalanced datasets.

The Matthews Correlation Coefficient (MCC) is a measure to evaluate the quality of a binary classifier even if the class distribution is imbalanced. The MCC value +1 shows a perfect prediction, a value zero indicates a random prediction, while value -1 represents disagreement between prediction and observation. Davide Chicco mentions that MCC is a much better measure than accuracy and F1 score, as the other two can be misleading because they do not consider all four confusion matrix values [21].

The Area Under the curve (AUC) measures the two- dimensional area under the ROC curve. AUC provides an aggregate measure of performance across all possible classification thresholds [22]. The AUC value ranges between 0 to 1. AUC value 1 shows a perfect prediction, while a value of zero indicates a wrong prediction.

Results and Discussion

To determine the best-suited method for credit card fraud detection, the results are analyzed on the basis of the evaluation metrics, including confusion matrix, precision, recall, accuracy, f1-score, MCC, and AUC. Since we had split the dataset on a 0.2 ratio, i.e., the test dataset consists of 20% of the whole dataset, a total of 59692 samples. Hence of a total of 98 fraudulent transactions, the achieved results are depicted in confusion matrixes.

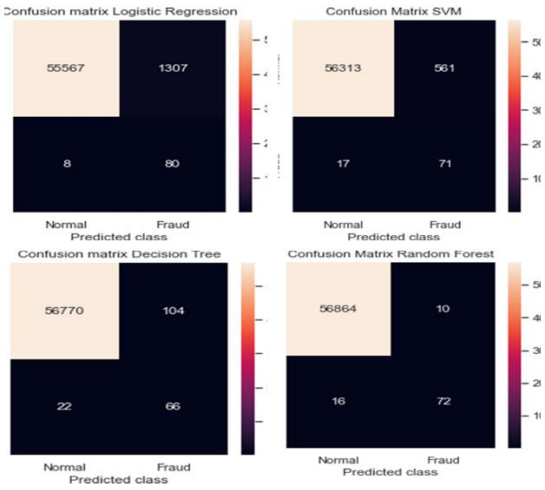

Fig. 4: Confusion Metrics of the classifiers

Table III shows the comparison results of accuracy, precision, recall, and f1-score of the applied machine learning methods (Logistic Regression, Decision Tree, Random Forest, and Support Vector Machine).

Table III: Comparison of Classifiers

Classifier	**Precision**	**Accuracy**	**Recall**	**F1-score**
SVM	0.1123	0.9898	0.8068	0.1972
Logistic Regression	0.0576	0.9769	0.9090	0.1084
Decision Tree	0.3882	0.9977	0.75	0.5116
Random Forest	0.8780	0.9995	0.8181	0.8471

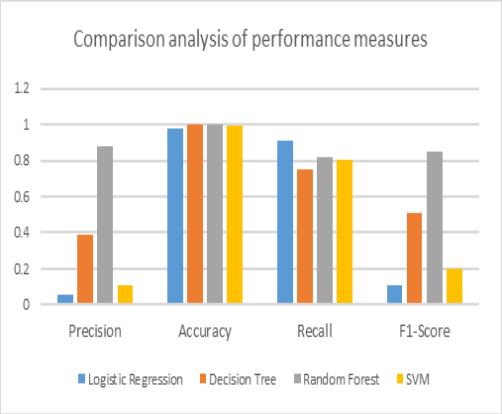

Fig. 5: Performance Comparison of Classifiers

The above table and figure show that in comparison to the selected machine learning classifiers, Random Forest outperforms the others under all the evaluation metrices.

Table V shows the comparison results of MCC (Matthews Correlation Coefficient) and AUC (Area under the Curve) for the applied machine learning methods. After analyzing confusion matrixes, Logistic regression and SVM have high false positives, and therefore they have performed poorly in MCC. The decision tree has given average results while the random forest has the lowest false positives hence the highest MCC value and comparatively good value for AUC.

Table IV: Evaluation Metrics

Classifiers	**MCC**	**AUC**
Logistic Regression	0.2257	0.9430
Decision Tree	0.5387	0.8741
Random Forest	0.8473	0.9091
SVM	0.2988	0.8984

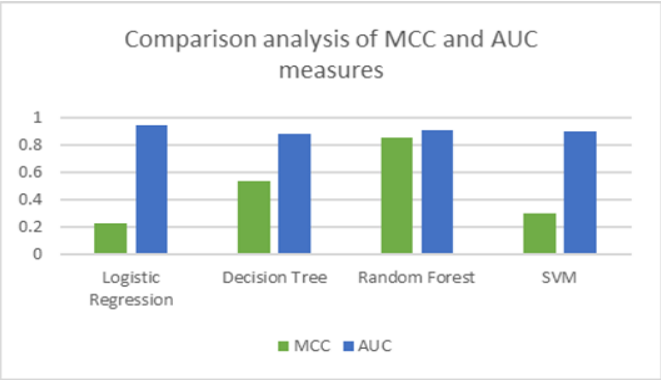

Fig. 6: Classifiers under Evaluation Metrices

A comparison shows with the results achieved in research on the same dataset [23] that oversampling the data can improve the fraud detection rate. The oversampling technique also helped achieve higher AUC and MCC values compared to the results obtained by researchers in [23]. Although [23] also presents a deep learning algorithm for this type of

problem and in [24] it is proven that classical algorithms can be as successful as deep learning algorithms. If the data is not much large, then it is better to work with classification algorithms. These algorithms are also easier to interpret and cheaper in the financial and computational sense [25].

Conclusion

In the present era of digitization, credit card fraud is a critical issue for every financial department and individual. This results in a huge loss of economy and reputation of an organization. Because of this reason, organizations spend a massive amount of money on developing new methods to detect and prevent these frauds. Many researchers are working on machine learning algorithms and deep learning domains for fraud detection because of their high accuracy and detection rate.

The main purpose of this study was to analyze and compare different machine learning techniques and find the best suitable method for credit card fraud detection based on various performance metrics. After comparing the results, the random forest has the lowest false positives, the highest accuracy and MCC value, and a comparatively good value for AUC. Therefore, based on the above study, Random Forest is suggested as the most suitable supervised machine learning method for fraud detection.

Credit card providers and financial institutions can use the proposed Model to detect possible fraud attempts. And further research should focus on other ML techniques and deep learning techniques for more accurate and real-time results.

Author's Contribution: A. U. F, Conceived the idea and wrote the draft; I. S, Designed the simulated work; A. S worked on the methodology and was the corresponding author; M. A, executed this work; and data analysis and proofread by N. A.

Funding: The publication of this article was funded by no one.

Conflicts of Interest: The authors declare no conflict of interest.

REFERENCES

[1] D. Varmedja, M. Karanovic, S. Sladojevic, M. Arsenovic, and A. Anderla, "Credit card fraud detection-machine learning methods," in *2019 18th International Symposium INFOTEH-JAHORINA (INFOTEH)*, 2019: IEEE, pp. 1-5.

[2] I. G. a. Y. B. a. A. Courville, *Deep Learning*. MIT Press, 2016.

[3] S. Marabad, "Credit Card Fraud Detection using Machine Learning," *Asian Journal For Convergence In Technology (AJCT) ISSN-2350-1146*, vol. 7, no. 2, pp. 121-127, 2021.

[4] Y. Sayjadah, I. A. T. Hashem, F. Alotaibi, and K. A. Kasmiran, "Credit card default prediction using machine learning techniques," in *2018 Fourth International Conference on Advances in Computing, Communication & Automation (ICACCA)*, 2018: IEEE, pp. 1-4.

[5] N. Udhaya Kumar, R. Sri Vasu, S. Subash, and D. Sharmila Rani, "ATM-Security using machine learning technique in IoT," *International Journal of Advance Research, Ideas and Innovations in Technology*, vol. 5, no. 2, pp. 150-153, 2019.

[6] I. El Naqa and M. J. Murphy, *What is machine learning?* Springer, 2015.

[7] N. C. Uslu and F. Akal, "A machine learning approach to detection of trade-based manipulations in borsa istanbul," *Computational Economics,* vol. 60, no. 1, pp. 25-45, 2022.

[8] K. Abhirami, A. K. Pani, M. Manohar, and P. Kumar, "An Approach for Detecting Frauds in E-Commerce Transactions using Machine Learning Techniques," in *2021 2nd International Conference on Smart Electronics and Communication (ICOSEC)*, 2021: IEEE, pp. 826-831.

[9] R. R. Popat and J. Chaudhary, "A survey on credit card fraud detection using machine learning," in *2018 2nd international conference on trends in electronics and informatics (ICOEI)*, 2018: IEEE, pp. 1120-1125.

[10] K. N. Mishra and S. C. Pandey, "Fraud prediction in smart societies using logistic regression and k-fold machine learning techniques," *Wireless Personal Communications,* vol. 119, pp. 1341-1367, 2021.

[11] J. O. Awoyemi, A. O. Adetunmbi, and S. A. Oluwadare, "Credit card fraud detection using machine learning techniques: A comparative analysis," in *2017 international conference on computing networking and informatics (ICCNI)*, 2017: IEEE, pp. 1-9.

[12] M. Ashraf, M. A. Abourezka, and F. A. Maghraby. (2022). A Comparative Analysis of Credit Card Fraud Detection Using Machine Learning and Deep Learning Techniques.

[13] V. A. S. B Basapur, Dr. Ambedhkar, "“Credit Card Fraud Detection using Machine Learning”," *Institute of Technology, Bagalor,* 2020.

[14] S. Makki, Z. Assaghir, Y. Taher, R. Haque, M.-S. Hacid, and H. Zeineddine, "An experimental study with imbalanced classification approaches for credit card fraud detection," *IEEE Access,* vol. 7, pp. 93010-93022, 2019.

[15] Z. Li, M. Huang, G. Liu, and C. Jiang, "A hybrid method with dynamic weighted entropy for handling the problem of class imbalance with overlap in credit card fraud detection," *Expert Systems with Applications,* vol. 175, p. 114750, 2021.

[16] H. Zhu, G. Liu, M. Zhou, Y. Xie, A. Abusorrah, and Q. Kang, "Optimizing weighted extreme learning machines for imbalanced classification and application to credit card fraud detection," *Neurocomputing,* vol. 407, pp. 50-62, 2020.

[17] S. Rajora *et al.*, "A comparative study of machine learning techniques for credit card fraud detection based on time variance," in *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*, 2018: IEEE, pp. 1958-1963.

[18] I. Benchaji, S. Douzi, and B. El Ouahidi, "Using genetic algorithm to improve classification of imbalanced datasets for credit card fraud detection," in *Smart Data and Computational Intelligence: Proceedings of the International Conference on Advanced Information Technology, Services and Systems (AIT2S-18) Held on October 17–18, 2018 in Mohammedia 3*, 2019: Springer, pp. 220-229.

[19] N. I. Mustika, B. Nenda, and D. Ramadhan, "Machine learning algorithms in fraud detection: case study on retail consumer financing company," *Asia Pacific Fraud Journal,* vol. 6, no. 2, pp. 213-221, 2021.

[20] M. L. GROUP-(ULB). *Credit Card Fraud Detection*, https://www.kaggle.com.

[21] A. Fernández, S. Garcia, F. Herrera, and N. V. Chawla, "SMOTE for learning from imbalanced data: progress and challenges, marking the 15-year anniversary," *Journal of artificial intelligence research,* vol. 61, pp. 863-905, 2018.

[22] D. Chicco, "Ten quick tips for machine learning in computational biology," *BioData mining*, vol. 10, no. 1, p. 35, 2017.

[23] https://developers.google.com/machine-learning. "Classification: ROC Curve and AUC." (accessed.

[24] P. Raghavan, & Gayar, N. E. , "Fraud Detection using Machine Learning and Deep Learning," presented at the 2019 International Conference on Computational Intelligence and Knowledge Economy(ICCIKE), United Arab Emirates, 2019.

[25] S. Dhankhad, E. Mohammed, and B. Far, "Supervised machine learning algorithms for credit card fraudulent transaction detection: a comparative study," in *2018 IEEE international conference on information reuse and integration (IRI)*, 2018: IEEE, pp. 122-125.