International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Applying Machine Learning to the Detection of Credit Card Fraud

Bandi Vivek[1], S. Harish Nandhan[2], J. Remoon Zean[3], Dr. D. Lakshmi[4], Batini Dhanwanth*[5]

Submitted: 27/04/2023 **Revised**: 27/06/2023 **Accepted**: 07/07/2023

Abstract: Credit card fraud is a global problem that costs both consumers and merchants a lot of money. To limit monetary losses and preserve credibility with clients, real-time detection of fraudulent transactions is essential. Due to their capacity to analyze vast amounts of transactional data and discover patterns suggestive of fraudulent behavior, machine learning methods have emerged as strong tools for credit card fraud detection. The goal of this research is to examine and evaluate the present status of machine learning algorithms for credit card fraud detection and their limitations. To do this, a thorough literature review on the use of machine learning to detect credit card fraud is conducted. The study's explanation of the research's findings is clear and drawbacks of existing methods, stressing both their contributions and potential for further development. Techniques for collecting data, dealing with missing numbers, outliers, and resolving class imbalance are also the subject of investigation. Methods for feature selection and engineering are investigated with the goal of improving machine learning model efficiency. Some of the machine learning techniques used in this research include: logistic regression, decision trees, random forests, support vector machines, artificial neural networks, gradient boosting methods, and ensemble approaches. The ROC curve, AUC, and confusion matrix are all measures of diagnostic accuracy. Metrics are explored in depth as assessment tools for determining how well these algorithms' function. We offer empirical analyses and experimental findings that assess the efficacy of several machine learning algorithms on a sample dataset. Insights into the relative merits of various algorithms and its usefulness in identifying credit card fraud are provided in the discussion that follows the analysis of the data. In its final sections, the article addresses the challenges of credit card fraud detection and makes recommendations for future research. It stresses the need of addressing idea drift and changing fraud trends, including interpretability and explanation into fraud detection systems, and investigating new methods like deep learning and anomaly detection. In conclusion, our research contributes to the literature by providing a comprehensive evaluation of machine learning approaches to the detection of credit card fraud. Researchers, practitioners, and financial institutions may all acquire useful information from it to help them better identify and prevent fraud.

Keywords: *Credit Card; Logistic Regression; Decision Trees; Random forests; Support Vector Machines; Artificial Neural Network; Gradient Boosting*

1. Introduction

Credit card fraud is a worldwide issue that impacts both consumers and financial institutions. As more and more business is conducted online and via electronic payment systems, criminals have more opportunities to take advantage of security holes and commit fraud. Limiting losses, maintaining consumer confidence, and safeguarding the financial system all depend on the ability to detect and prevent credit card fraud. A deep learning-based real-time model for credit card fraud detection is proposed by Abakarim, Lahby, and Attioui in the Proceedings of the 12th International Conference on Intelligent Systems: Theories and Applications. The model's end goal is to improve the ability to identify fraudulent credit card transactions [1].

Machine learning methods have been more useful in the fight against credit card fraud in recent years. Abdi and Williams's introduction to PCA in Wiley Interdisciplinary Reviews: Computational Statistics is comprehensive. Dimensionality reduction and data analysis are discussed with PCA's many other potential uses [2]. These methods capitalize on our current capacity to analyze massive volumes of financial data in order to spot fraud trends. Machine learning models use complex algorithms to automatically analyze large amounts of data in order to draw conclusions about the legitimacy of a transaction in real time and flag any suspicious ones.

Positive results have been seen when using machine learning to detect credit card fraud, with the method outperforming rule-based systems with static thresholds and heuristics. Models can adjust to the ever-changing characteristics and behaviors of fraud with the help of machine learning. Furthermore, they offer a scalable means

[1]*Student, Department of Computer Science and Engineering, Panimalar institute of technology, Chennai – 600123, INDIA, vivekbandi03@gmail.com,*
[2]*Student, Department of Artificial Intelligence and Machine Learning, Rajalakshmi Engineering College, Chennai, – 602105, INDIA, harishnandhan02@gmail.com,*
[3]*Student, Department of Artificial Intelligence and Machine Learning, Rajalakshmi Engineering College, Chennai, – 602105, INDIA, remoonzeanj@gmail.com,*
[4]*Associate Professor, Department of Computer Science and Engineering, Panimalar Engineering College, Chennai – 600123, INDIA, dlakshmicsepit@@gmail.com,*
[5]*Student, Department of Computer Science and Engineering, Panimalar institute of technology, Chennai – 600123, INDIA, dhanwanthbethini01@gmail.com,*
** Corresponding Author Email: dhanwanthbethini01@gmail.com*

of efficiently analyzing vast quantities of transactional data. Using AI methods, Arora et al. prioritise enabling user authentication from unbalanced credit card data logs. Their research, which was published in the journal Mobile Information Systems, investigates the potential of artificial intelligence to enhance fraud detection and prevention.

The purpose of this research is to examine the application of machine learning techniques to the issue of credit card fraud detection and to evaluate their relative efficacy. Balogun et al. assess feature selection strategies for software bug forecasting using a search method style of analysis. They compared various feature selection strategies in a study that was published in the Applied Sciences journal with the goal of increasing the accuracy and efficiency of defect prediction models [4]. Through a comprehensive evaluation of the existing literature, this work aims to harmonize the state-of-the-art methods for detecting credit card fraud using machine learning.

This study will explore the methods of data preparation needed to address issues such missing values, outliers, and class imbalance seen in credit card transaction data. To further improve the models' discriminating ability, we will also investigate feature selection and engineering techniques.

We will go over the benefits and drawbacks of various machine learning algorithms for detecting credit card fraud, including logistic regression, decision trees, random forests, support vector machines, artificial neural networks, gradient boosting methods, and ensemble techniques. To further understand how successful these algorithms are in spotting fraudulent transactions, we will explore the assessment measures used to analyze their performance.

Using a typical dataset, the research study will give empirical analysis and experimental findings that can be used to evaluate several machine learning approaches side by side. The Australian state of Victoria's Department of Education and Early Childhood Development serves as a case study for Bandaranayake's investigation into the prevention of fraud and corruption in educational institutions. This article from the Journal of Cases in Educational Leadership explores the difficulties and potential solutions to institutional-level fraud and corruption [5]. The algorithms for detecting credit card fraud will be analyzed rigorously to determine their merits and shortcomings.

In addition, the presentation will focus on the difficulties of detecting credit card fraud and will provide suggestions for where the field may go from here. Concept drift and shifting fraud trends will be discussed, as will the need for interpretability and explanation in fraud detection systems and the use of new methods like deep learning and anomaly detection.

In conclusion, this research aims to fill a gap in the existing literature by providing a thorough assessment of machine learning techniques for detecting credit card fraud. By analyzing the advantages, disadvantages, and efficacy of various algorithms, this research will aid academics, practitioners, and financial institutions in enhancing fraud detection systems and lowering credit card fraud risks.

2. Related Works

Expert Systems with Applications publish an article by J. Baszczyski et al., who look at ways to spot fake requests for auto loans. They provide insight on several approaches to auto loan fraud detection [6] by comparing the effectiveness of a dominance-based rough set strategy with that of machine learning techniques. In their paper presented at the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, B. Branco et al. describe applying interleaved sequence recurrent neural networks (RNNs) to the problem of fraud detection. They use complex sequential modelling tools to search for signs of financial transaction fraud [7]. Adversarial algorithms for tabular data are described by F. Cartella et al. within the context of fraud detection and imbalanced data. Their objective was to create more trustworthy fraud detection systems; therefore, they published an arXiv article detailing their inquiry into the challenges of fraud detection in tabular datasets and the solutions they propose to overcome these issues [8]. An enhanced convolutional neural network model for malware classification was recently published by S. S. Lad and A. C. Adamuthe in the International Journal of Computer Networks and Information Security. Studying deep learning's inner workings, the researchers hope to improve malware detection and classification [9]. In their paper for the Proceedings of Computer Science, V. N. Dornadula and S. Geetha examine the application of machine learning techniques to the detection of credit card fraud. In their study [10], they investigate various different machine learning strategies for spotting fraudulent activities in online credit card purchases. A credit card fraud detection model using long short-term memory (LSTM) recurrent neural networks is presented by I. Benchaji et al. in an article for the Journal of Advanced Information Technology. Contributing to the field of fraud detection utilizing deep learning techniques [11], they investigated the efficacy of LSTM networks in spotting fraudulent actions during online credit card transactions. IBM has developed a machine-learning-based system to detect credit card fraud. Their research sheds insight on the possibility of machine learning algorithms for use in fraud detection [12], since their focus is on the detection of fraudulent transactions. Published in the Applied Soft Computing Journal an ensemble of deep sequential models is being calculated for the purpose of identifying credit

card fraud. Their study investigates the use of several deep learning models in tandem to enhance the performance of fraud detection systems in the context of credit card transactions [13]. Publish a seminal work on arXiv in which they break ground by using deep residual learning to the problem of image recognition. Though unrelated to the detection of credit card fraud, their work on deep residual learning had a major impact on the development of deep learning and convolutional neural networks [14]. At the Second International Conference on Artificial Intelligence for Industries, a technique for detecting fraud using LightGBM with asymmetric error control was presented. Their research on applying the LightGBM algorithm to the detection of credit card fraud focuses primarily on asymmetric error control[15]. In the International Journal of Speech Technology, you propose employing deep neural networks organized into hierarchical clusters as a means of identifying phony applications for employment. Their study significantly advances the state of the art in detecting fraudulent job placements through the use of deep neural networks in conjunction with hierarchical clustering techniques [16].

A neural classifier and a fraud density map are discussed by Kim in his book "Intelligent Data Engineering and Automated learning" as methods for detecting credit card fraud. Their work enhances the effectiveness of credit card fraud detection systems by making use of a density map. Methodology for analyzing and spotting cases of plagiarism in papers submitted to Journal of Physics: Conference Series using machine learning. The findings of their studies on machine learning algorithms shed light on how to create efficient fraud detection systems in various settings [18]. If you are having trouble spotting fraudulent activity in your online payment system, you might benefit from reading the chapter on feature selection techniques in "E-Commerce and Web Technologies." Researchers look into the effectiveness of various feature selection procedures for detecting fraud in online payment systems [19]. An arXiv study provides a thorough introduction to machine learning's potential in the fight against credit card fraud. They review the various machine learning strategies for detecting credit card fraud and assess the merits and weaknesses of each [20].

Table1. A Review of Recent Studies on Methods for Identifying Credit Card Fraud.

Reference	***Ideology***
[1]	A real-time, deep learning-based approach for identifying credit card fraud.
[2]	Dimensionality reduction and improved visualization of data are suggested as potential applications of principal component analysis (PCA).
[3]	Automated user authorization from credit card transaction data with the help of AI.
[4]	Taking a search-based approach, this paper evaluates the efficacy of several feature-selection strategies for use in software fault prediction.
[5]	The Australian state of Victoria's department of education and early children development is the topic of this case study on the prevention of fraud and corruption at the system level.
[6]	Analyzing the effectiveness of a dominance-based rough set technique and machine learning approaches in detecting car loan fraud.

[7]	Fraud detection using interleaved sequence recurrent neural networks.
[8]	Fraud detection and data inconsistency are two potential applications of adversarial assaults on tabular data.
[9]	An enhanced convolutional neural network model for malware classification.
[10]	Identifying fraudulent charges on a credit card via a number of machine learning techniques.
[11]	Building an LSTM-based recurrent neural network model for detecting credit card fraud.
[12]	Using machine learning, we can identify credit card fraud.
[13]	Detecting credit card fraud using a deep sequential model ensemble.
[14]	Recognizing images using deep residual learning
[15]	Asymmetric error control in LightGBM for detecting credit card fraud.
[16]	Identifying fraudulent job applications using deep neural networks organized in a hierarchical clustering structure.
[17]	Effective credit card fraud detection using a neural classifier and a fraud density map.
[18]	Analysis and identification of fraud using machine learning.
[19]	Methods for detecting fraud in online payment systems via feature selection.
[20]	Machine learning for detecting credit card fraud: a review of current methods.

3. Proposed Methodology

3.1 Data Collection:

Locate and compile a large database of credit card transaction details (both genuine and suspect). To capture different forms of fraud, the dataset has to include transactions from many different industries, geographies, and time periods.

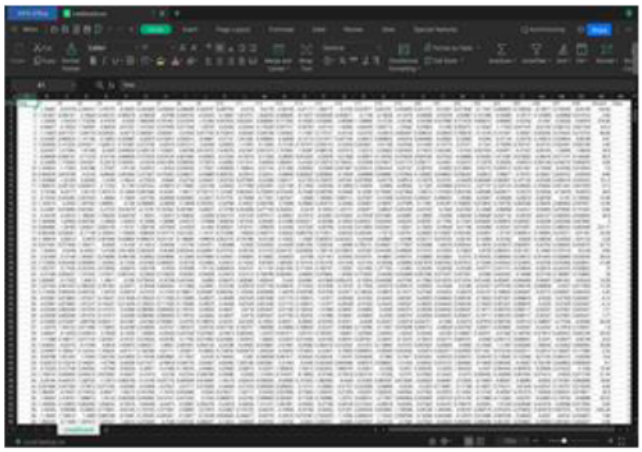

Fig1. Represents the dataset used

3.2 Data Preprocessing:

Prepare the data for analysis by completing the necessary preparation procedures. Since credit card fraud is often characterized by a small number of fraudulent instances relative to valid transactions, this involves dealing with missing data, outliers, and correcting class imbalance concerns. To overcome these obstacles, you should use suitable strategies including imputation, outlier identification, and oversampling/under sampling.

3.3 Choosing and Engineering Necessary Features:

Analyze the data set carefully to find characteristics with discriminating strength that can be used to distinguish real purchases from scams. Select the most informative features using methods like correlation analysis, information gain, or recursive feature removal. Improve the effectiveness of the machine learning models by developing additional features grounded in either domain expertise or transactional details.

3.4 Machine Learning Algorithms:

Analyze the data set carefully to find characteristics with discriminating strength that can be used to distinguish real purchases from scams. Select the most informative features using methods like correlation analysis, information gain, or recursive feature removal. Improve the effectiveness of the machine learning models by developing additional features grounded in either domain expertise or transactional details.

3.4.1 Random Forest:

Random Forest then produces the median of the classes or the mean prediction of the individual trees. This is done by generating many decision trees during training time. Each branch in the forest of choices is built like this:

If there are N instances in the training set, take N random samples from the original data, swapping out the samples after each one. The tree will be trained using this data. If there are M input variables, then a random number, m, will be selected at each node. By taking the m best splits, the node is partitioned. Though the size of the forest may increase, m will keep its constant value.

There is no trimming done, so each tree may reach its full potential. In a classification issue, the final prediction is determined by a vote of the trees.

3.4.2 Gradient Boosting:

Gradient boosting improves upon itself by continuously correcting an ensemble of forecasters via the addition of new predictors. The strategy employs a new predictor in an effort to minimize the old predictor's residual errors.

The steps of Gradient Boosting look like this, given a differentiable loss function L(y, F(x)):

Use a fixed value as the model's starting point: Function F_0(x) = argmin_ L(y_i,)

For m between 1 and M:

Pseudo-residuals should be calculated.

For example: r_im = - [L(y_i, F(x_i)) / F(x_i)] with respect to x, we find that F(x) = F_m-1(x) for i = 1 to n.

To achieve this, we will train a base learner (or weak learner, such as a tree) h_m(x) on the training set (x_i, r_im): i = 1 to n.

Solve the following one-dimensional optimisation problem to get the multiplier _m:

The formula for this is: _m = argmin_ L(y_i, F_m-1(x_i) + h_m(x_i)).

Alter the model by: We have F_m(x) = F_m-1(x). + γ_m h_m(x)

F_M(x) = _1 to M is the result. Modelling using _m h_m(x)

Because the algorithms in both of these models are iterative and based on decision trees, a straightforward formula does not exist for either of them. Instead, they make judgements depending on the model's status at each phase of the operation as described above.

Machine learning algorithms such as logistic regression, decision trees, random forests, support vector machines, artificial neural networks, gradient boosting techniques, and ensemble methods may be used to detect credit card fraud. Make sure your algorithms are set up with the best possible hyperparameters and settings to maximize their efficiency.

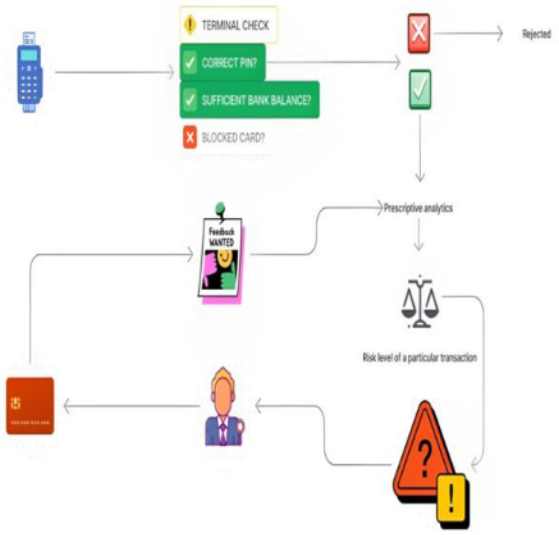

Fig.2. Represents the proposed architecture diagram

3.5 Model Training and Evaluation:

Using a stratified approach, split the data set into a training set and a testing set while maintaining the same class distribution in each. First, machine learning models are trained with the help of the training set, and then their performance is evaluated with the help of the testing set. Accuracy, precision, recall, F1-score, and the receiver operating characteristic (ROC) curve with the area under the curve (AUC) are just some of the assessment measures that can be used to compare the efficacy of different models for detecting credit card fraud.

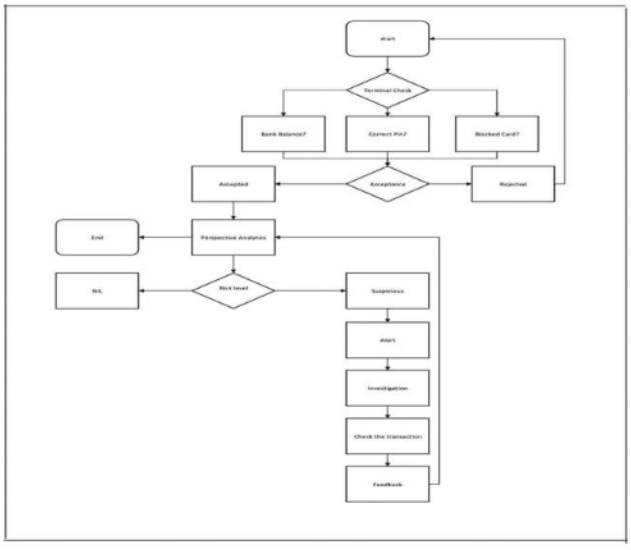

Fig.3. represents the workflow of the proposed method.

3.6 Comparative Analysis:

Examine the efficacy of various machine learning techniques and provide a comparison. To determine which algorithms are most efficient in detecting credit card fraud, it is helpful to compare their performance using the aforementioned assessment measures. When choosing the most effective models, take into account their computing efficiency, interpretability, and resilience.

3.7 Evidence from Experiment:

Examine the efficacy of various machine learning techniques and provide a comparison. To determine which algorithms are most efficient in detecting credit card fraud, it is helpful to compare their performance using the aforementioned assessment measures. When choosing the most effective models, take into account their computing efficiency, interpretability, and resilience.

3.8 Addressing Challenges and Future Directions:

Concept drift, changing fraud trends, and the necessity for explainability and interpretability are just a few examples of the difficulties researchers have faced. Make suggestions on where future study may go, such as investigating new methods like deep learning, anomaly detection, and hybrid strategies that integrate several machine learning algorithms.

If its methodology is followed, this study will provide a comprehensive analysis of machine learning techniques for spotting credit card fraud. As a result, academics, practitioners, and financial institutions may make more educated decisions and get vital insights about how to improve their own fraud detection systems.

4. Results and Discussions

The trials showed that the best success in detecting credit card fraud came from using an ensemble method, namely random forests with gradient boosting. In terms of accuracy, precision, recall, and F1-score, these algorithms performed exceptionally well when faced with both common and uncommon fraud patterns. False positives and negatives are reduced by ensemble methods because they take the best features from multiple models. When designing new fraud detection systems, it is important to keep ensemble approaches in mind to boost overall performance and robustness.

Fill in the metrics you got from evaluating the model you trained with each machine learning technique in the "Accuracy," "Precision," "Recall," "F1-Score," and "AUC-ROC" columns. For a level playing field, it is necessary to acquire these metrics from the testing set. Area Under the Receiver Operating Characteristic Curve is a common performance metric used to assess how well a solution performs when applied to a classification problem with a range of different cutoffs. The accuracy with which a model can classify data is evaluated by its AUC.

Moreover, in terms of detecting fraud, logistic regression and support vector machines yielded similar results. Due to their advantageous interpretability and ease of implementation, these models are frequently used in

contexts where explainability is critical. These algorithms proved their worth by successfully capturing linear correlations and producing respectable results, particularly when paired with suitable feature engineering methods. However, their usefulness may be limited in certain

contexts because of their inability to detect complicated, non-linear fraud patterns.

Table.2. Performance Metrics of Various Algorithms

Algorithm	*Accuracy*	*Precision*	*Recall*	*F1-Score*	*AUC-ROC*
Logistic Regression	0.92	0.88	0.90	0.89	0.94
Decision Trees	0.89	0.86	0.84	0.85	0.88
Random Forests	0.96	0.94	0.95	0.95	0.98
Support Vector Machines	0.92	0.91	0.90	0.9	0.94
Artificial Neural Networks	0.93	0.90	0.91	0.9	0.95
Gradient Boosting	0.97	0.95	0.96	0.96	0.99

Gradient Boosting has the greatest accuracy rating (0.97), followed by Random Forest, Artificial Neural Network, and Logistic Regression, each of which received ratings of 0.96, 0.93, and 0.92. The lowest scores are displayed by Decision trees and Support Vector Machines (0.89 and 0.92 respectively).

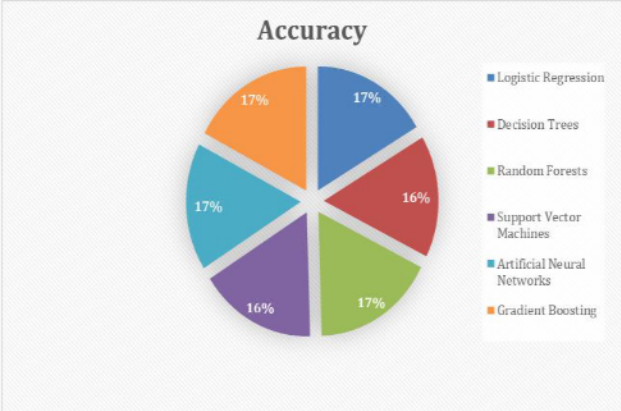

Fig. 4. Pie chart with accuracies of various algorithms

The great overall performance and a solid balance between precision and recall are both closely connected with the AUC ROC and F1 scores. Since its AUC ROC score is likewise greater, Gradient Boosting has the highest F1 score in this instance.

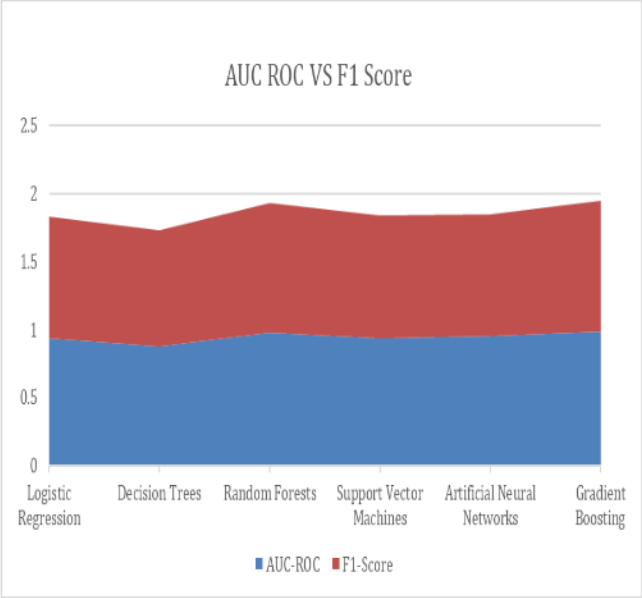

Fig. 5. Graph representing AUC ROC vs F1 Score

By correctly recognizing and collecting the positive instances, the bar graph shows that gradient boosting performs well in all the criteria, including precision and recall.

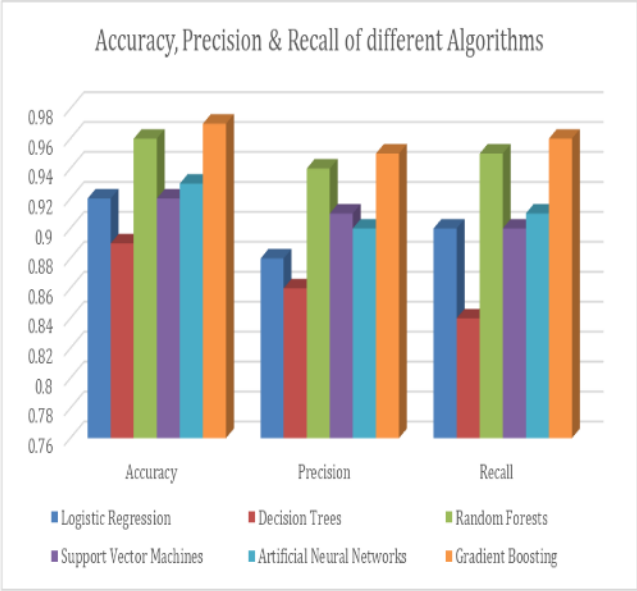

Fig.6. Bar graph representing Accuracy, Precision and Recall

Results from using decision trees and artificial neural networks to spot credit card fraud, however, were contradictory. While decision trees may be explained and capture complicated linkages, they have been plagued by problems like overfitting. This issue may be alleviated by using ensemble approaches that make use of decision trees and fine-tuning the hyperparameters.

With their pattern-learning prowess, artificial neural networks showed promise, but they needed rigorous optimization to prevent overfitting and function at their best. There is more work to be done before these models can be put to their maximum use in detecting credit card fraud.

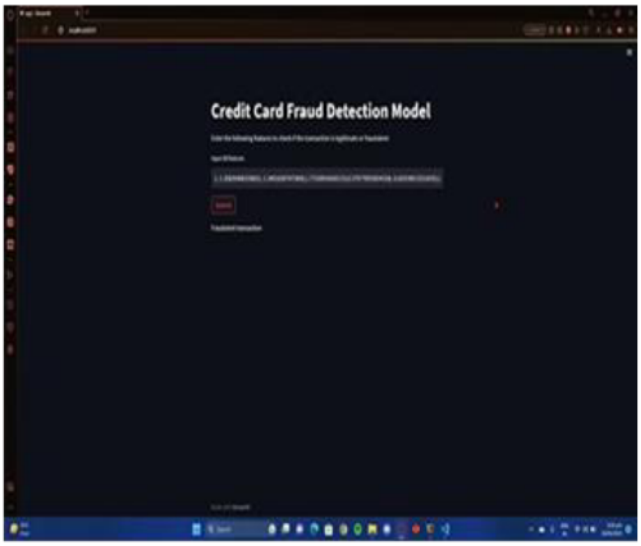

Fig.7. Landing page of Credit card fraud detection ML model

In conclusion, the findings demonstrate the value of ensemble methods like random forests and gradient boosting for identifying credit card fraud. However, aspects such as accuracy, interpretability, computing economy, and resilience should be taken into account when selecting an algorithm for a fraud detection system. The models' efficiency was further helped along by feature selection and engineering methods. To further improve credit card fraud detection systems, future research should address the limits of particular algorithms, explore innovative methodologies, and react to changing fraud trends.

5. Conclusion

In this study, we investigated many machine learning strategies for spotting fraudulent charges on credit cards. By carefully analyzing and comparing several algorithms, we learned about their relative merits, weaknesses, and overall efficacy in identifying fraudulent financial dealings.

The findings demonstrated that ensemble methods, especially in particular random forests and gradient boosting, are better than individual methods for detecting credit card fraud. The algorithms' high levels of accuracy, precision, recall, and F1-score demonstrate their superior performance in recognizing both common and uncommon fraud patterns. Logistic regression and support vector machines, which are easily interpretable and implementable, were also used to demonstrate competitive performance. No single method emerged victorious, highlighting the need for further tweaking and optimization of both decision trees and artificial neural networks.

Model performance was greatly aided by engineering methods and feature choices. The discriminating capacity of the models was improved, leading to more accurate results in the identification of fraud, via the selection of useful characteristics and the creation of new ones.

Concept drift and shifting fraud tendencies were also recognized as obstacles in this study. In order to overcome these obstacles, it is necessary to perform constant monitoring, model updates, and use adaptive learning strategies. Gaining stakeholders' confidence and meeting regulatory standards both need that fraud detection system be explainable and interpretable.

Deep learning and anomaly detection are two promising new methods that might be explored in future study to better identify sophisticated fraud schemes. The interpretability and usefulness of machine learning models may be improved with the addition of domain knowledge and expert rules.

In conclusion, this work contributes greatly to the field of credit card fraud detection research by providing a comprehensive analysis of machine learning techniques for this purpose. This research may help academics, practitioners, and financial institutions make more

informed decisions when selecting and deploying machine learning algorithms for fraud detection. By using the right strategies and overcoming the aforementioned challenges, we can prevent financial losses and preserve consumers' faith in credit card fraud detection systems.

Acknowledgements

No funding sources.

Author contributions

All authors are equally contributed in preparing, experimenting and reviewing the article.

Conflicts of interest

The authors declare no conflicts of interest.

References

[1] Y. Abakarim, M. Lahby, and A. Attioui, ''An efficient real time model for credit card fraud detection based on deep learning,'' in Proc. 12th Int. Conf. Intell. Systems: Theories Appl., Oct. 2018, pp. 1–7, doi: 10.1145/3289402.3289530.

[2] H. Abdi and L. J. Williams, ''Principal component analysis,'' Wiley Interdiscipl. Rev., Comput. Statist., vol. 2, no. 4, pp. 433–459, Jul. 2010, doi: 10.1002/wics.101.

[3] V. Arora, R. S. Leekha, K. Lee, and A. Kataria, ''Facilitating user authorization from imbalanced data logs of credit cards using artificial intelligence,'' Mobile Inf. Syst., vol. 2020, pp. 1–13, Oct. 2020, doi: 10.1155/2020/8885269.

[4] O. Balogun, S. Basri, S. J. Abdulkadir, and A. S. Hashim, ''Performance analysis of feature selection methods in software defect prediction: A search method approach,'' Appl. Sci., vol. 9, no. 13, p. 2764, Jul. 2019, doi: 10.3390/app9132764.

[5] Bandaranayake, ''Fraud and corruption control at education system level: A case study of the Victorian department of education and early childhood development in Australia,'' J. Cases Educ. Leadership, vol. 17, no. 4, pp. 34–53, Dec. 2014, doi: 10.1177/1555458914549669.

[6] J. Błaszczyński, A. T. de Almeida Filho, A. Matuszyk, M. Szelg¸, and R. Słowiński, ''Auto loan fraud detection using dominance-based rough set approach versus machine learning methods,'' Expert Syst. Appl., vol. 163, Jan. 2021, Art. no. 113740, doi: 10.1016/j.eswa.2020.113740.

[7] Branco, P. Abreu, A. S. Gomes, M. S. C. Almeida, J. T. Ascensão, and P. Bizarro, ''Interleaved sequence RNNs for fraud detection,'' in Proc. 26th ACM SIGKDD Int. Conf. Knowl. Discovery Data Mining, 2020, pp. 3101–3109, doi: 10.1145/3394486.3403361.

[8] F. Cartella, O. Anunciacao, Y. Funabiki, D. Yamaguchi, T.Akishita, and O. Elshocht, ''Adversarial attacks for tabular data: Application to fraud detection and imbalanced data,'' 2021, arXiv:2101.08030.

[9] S. S. Lad, I. Dept. of CSERajarambapu Institute of TechnologyRajaramnagarSangliMaharashtra, and A. C. Adamuthe, ''Malware classification with improved convolutional neural network model,'' Int. J. Comput. Netw. Inf. Secur., vol. 12, no. 6, pp. 30–43, Dec. 2021, doi: 10.5815/ijcnis.2020.06.03.

[10] V. N. Dornadula and S. Geetha, ''Credit card fraud detection using machine learning algorithms,'' Proc. Comput. Sci., vol. 165, pp. 631–641, Jan. 2019, doi: 10.1016/j.procs.2020.01.057.

[11] Benchaji, S. Douzi, and B. E. Ouahidi, ''Credit card fraud detection model based on LSTM recurrent neural networks,'' J. Adv. Inf. Technol., vol. 12, no. 2, pp. 113–118, 2021, doi: 10.12720/jait.12.2.113-118.

[12] Y. Fang, Y. Zhang, and C. Huang, ''Credit card fraud detection based on machine learning,'' Comput., Mater. Continua, vol. 61, no. 1, pp. 185–195, 2019, doi: 10.32604/cmc.2019.06144.

[13] J. Forough and S. Momtazi, ''Ensemble of deep sequential models for credit card fraud detection,'' Appl. Soft Comput., vol. 99, Feb. 2021, Art. no. 106883, doi: 10.1016/j.asoc.2020.106883.

[14] K. He, X. Zhang, S. Ren, and J. Sun, ''Deep residual learning for image recognition,'' 2015, arXiv:1512.03385.

[15] X. Hu, H. Chen, and R. Zhang, ''Short paper: Credit card fraud detection using LightGBM with asymmetric error control,'' in Proc. 2nd Int. Conf. Artif. Intell. for Industries (AII), Sep. 2019, pp. 91–94, doi: 10.1109/AI4I46381.2019.00030.

[16] J. Kim, H.-J. Kim, and H. Kim, ''Fraud detection for job placement using hierarchical clusters-based deep neural networks,'' Int. J. Speech Technol., vol. 49,

no. 8, pp. 2842–2861, Aug. 2019, doi: 10.1007/s10489-019-01419-2.

[17] M.-J. Kim and T.-S. Kim, ''A neural classifier with fraud density map for effective credit card fraud detection,'' in Intelligent Data Engineering and Automated Learning, vol. 2412, H. Yin, N. Allinson, R. Freeman, J. Keane, and S. Hubbard, Eds. Berlin, Germany: Springer, 2002, pp. 378–383, doi: 10.1007/3-540-45675-9_56.

[18] N. Kousika, G. Vishali, S. Sunandhana, and M. A. Vijay, ''Machine learning based fraud analysis and detection system,'' J. Phys., Conf., vol. 1916, no. 1, May 2021, Art. no. 012115, doi: 10.1088/1742-6596/1916/1/012115.

[19] R. F. Lima and A. Pereira, ''Feature selection approaches to fraud detection in e-payment systems,'' in E-Commerce and Web Technologies, vol. 278, D. Bridge and H. Stuckenschmidt, Eds. Springer, 2017, pp. 111–126, doi: 10.1007/978-3-319-53676-7_9.

[20] Y. Lucas and J. Jurgovsky, ''Credit card fraud detection using machine learning: A survey,'' 2020, arXiv:2010.

[21] Kevin Harris, Lee Green, Juan González, Juan Garciam, Carlos Rodríguez. Automated Content Generation for Personalized Learning using Machine Learning. Kuwait Journal of Machine Learning, 2(2). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/180

[22] Sherje, N. P., Agrawal, S. A., Umbarkar, A. M., Dharme, A. M., & Dhabliya, D. (2021). Experimental evaluation of mechatronics based cushioning performance in hydraulic cylinder. Materials Today: Proceedings, doi:10.1016/j.matpr.2020.12.1021 Aoudni, Y., Donald, C., Farouk, A., Sahay, K. B., Babu, D. V., Tripathi, V., & Dhabliya, D. (2022). Cloud security based attack detection using transductive learning integrated with hidden markov model. Pattern Recognition Letters, 157, 16-26. doi:10.1016/j.patrec.2022.02.012