IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, April 2025
Impact Factor: 7.67

Credit Card Fraud Detection using Machine Learning

Dipali Sanjay Khedkar and Prof. Rashmi Kulkarni
Department of Information Technology
Siddhant College of Engineering, Pune, India
dipalikhedkar799@gmail.com

Abstract: *The increased use of financial transactions on the internet has also enabled credit card fraud to flourish and challenge the credibility and reliability of electronic payment systems. Traditional rule-based approaches to detecting fraud have proved ineffective in detecting latent patterns of fraud that lead to high levels of false alarms and undetected fraud. This paper introduces a machine learning-based credit card fraud detection system using Logistic Regression and Random Forest classifiers. Both models are trained and tested on a massive Kaggle dataset comprising over 550,000 anonymized credit card transactions. Robust data preprocessing methods like normalization, encoding, and class balancing are utilized to enhance the performance of the models. The models are contrasted based on accuracy, precision, recall, and F1 score to evaluate their capacity to identify fraudulent transactions. Results show that the Random Forest algorithm gives improved performance, with 99.95% accuracy and 100% precision, due to its ensemble learning attribute that averts overfitting. Though simpler, Logistic Regression is a reasonable baseline withan interpretable output and fast computation. Ensemble-based models yield a scalable and more accurate fraud detection platform, as shown in the results. Future research explores the deep learning paradigms in federated learning for better privacy and real-time detection features to facilitate secure financial systems.*

Keywords: Credit Card Fraud Detection, Machine Learning, Support Vector Machine, k-nearest Neighbors, Decision Tree, Random Forest, Imbalanced Data

I. INTRODUCTION

Financial technologies have changed howindividuals in the fast-changing digital age transact. Credit cards are today one of the most convenient and used payment modes in online and offline stores. As e-commerce across the globe expands and the financial world goes digital, transactions by credit cards increase exponentially. Although this change brings record speed and ease, it has also heightened vulnerability to fraud. Credit card fraud is now among the most common cybercrimes, with a high impact on consumers, merchants, and financial institutions.

Credit card fraud is the unauthorized use of credit card information for financial benefits. It encompasses a broad set of methods, from physical theft and skimming to advanced ones such as phishing, identity theft, and card-not-present (CNP) attacks. Unauthorized transactions cause direct monetary losses, erode customers' confidence, and reduce trust in electronic payment systems. Thus, developing efficient, responsive, and scalable fraud detection systems is a concern in financial cyber-security.

Traditionally, anti-fraud systems have been dependent to a large extent on rule-based solutions. Rule-based solutions use manually defined rules to detect suspicious transactions, such as large deals or border-transcending transactions. Rule-based systems are highly rigid and even effective in detecting known behavior. Criminals continue evolving new techniques to stay ahead of closely worded rules. This makes time-proven measures ineffective in the long term. Second, rule-based systems are most likely to generate high false positives—indicating legitimate transactions as fraud, impacting customer satisfaction, reputational harm, and operational inefficiencies.

By contrast, machine learning (ML) techniques offer a better solution by learning from historical data to identify subtle patterns typical of fraud. Unlike static rules, ML models can evolve with new trends in fraud and improve their

DOI: 10.48175/IJARSCT-25301

ISSN
2581-9429
IJARSCT

performance by adding new data. These models handle large datasets, uncover hidden relationships among features, and make predictions based on statistical learning concepts. Consequently, ML-based systems can increase fraud detection rates, reduce false positives, and enable proactive countermeasures against dynamic attacks.

This research will utilize a system to identify credit card fraud using Logistic Regression (LR) and Random Forest (RF) algorithms. One of the most basic but oldest algorithms in performing binary classification tasks, Logistic Regression, is utilized worldwide in solving fraud detection cases because Logistic Regression provides a good baseline model for most cases in fraud detection cases. On the other hand, Random Forest is a robust ensemble learning technique that constructs numerous decision trees and combines their predictions to improve the prediction capability and avoid overfitting. Its ability to perform well with unbalanced datasets and identify nonlinear relationships renders it highly suitable for fraud detection applications where the majority class (regular transactions) significantly outweighs the minority class (suspicious transactions) in numbers.

The credit card fraud detection data utilized here consists of more than 550,000 anonymized transactions obtained from Kaggle and depict European cardholders' behavior. Owing to the inherent class imbalance in which the fraudulent transactions are a minuscule portion of the dataset, special care is taken for preprocessing techniques like normalization, feature encoding, and oversampling using Synthetic Minority Over-sampling Technique (SMOTE). These operations are crucial in making the models robust and avoiding biased learning.

Model evaluation in fraud discovery contexts is not as accurate overall and is misleading in strongly skewed datasets. A model labeling every transaction as genuine could easily retain high accuracy due to the overwhelming majority of the transactions not being fraudulent. Still, it would fail at its primary role: finding frauds. Therefore, this paper targets precision, recall, and F1-score—those metrics that more accurately reflect the model's fraud-detection ability without triggering too many false positives. Precision is the proportion of actual frauds out of all transactions flagged, whereas recall (or sensitivity) approximates the model's capability to detect all instances of actual fraud. The F1 score is balanced, taking precision and recall into account and providing an overall performance measure.

Past research has established the effectiveness of machine learning algorithms in identifying fraud. For example, ensemble algorithms such as Random Forest and XGBoost have outperformed single classifiers reliably as they combine the outputs of a collection of base learners. In a study, Xuan et al. (2018) listed the advantages of Random Forest in minimizing false negatives in detecting fraud, crediting its effectiveness due to diversity in its component trees and randomization covered while training. Even though typically eclipsed by more advanced models, Logistic Regression is still a choice since it is understandable and transparent—virtues highly prized in finance where the interpretability of models must be ensured to ensure compliance and auditability.

Aside from algorithmic use, the study also touches on fraud detection usability and ethics. The banking institutions must apply the ML models in an open, fair, and secret manner when dealing with data. Discrimination against training data should be prevented to avoid biased results like over-marking transactions within a specific geographic location or demographic. Other than that, laws such as the General Data Protection Regulation (GDPR) require personal financial information with a high sensitivity to be treated carefully. Through these mistakes, the present study is on the ethical use of AI and is necessary to render fraud detection software traceable and explainable.

The research approach here is a well-structured pipeline. The dataset is first preprocessed by cleaning, normalization, and balancing it. The data is then separated into training, validation, and test sets to assess the model's generalizability. Preprocessed data is further employed to train the logistic regression and random forest model with hyperparameter tuning for the best results. Finally, the models are compared using standard classification metrics, and strengths and weaknesses are discussed. Comparative analysis identifies the optimal strategy regarding detection rate, computational cost, and robustness.

This research's findings are expected to contribute to the fraud detection body of knowledge by restating the viability of interpretable models like Logistic Regression and ensemble methods like Random Forest. As much as there is growing interest in deep learning techniques like neural networks, the complexity and low interpretability make them restrictively applicable for sensitive domains like finance. This study advocates for an equitable approach that balances accuracy, interpretability, scalability, and compliance.

The key motivations of this research are as follows:

Breaking Legacy Constraints: Acknowledging the limitations of rule-based systems and the potential of machine learning algorithms to overcome these constraints because they can learn from changing fraud patterns.
Employing Logistic Regression and Random Forest: These orthogonal models are employed to create an interpretable and predictive model for fraud detection.
Asymmetric Dataset Handling: Utilizing dataset balancing methods and comparison evaluation metrics such that the models will be able to identify minority-class suspicious transactions effectively.
Ethical and Responsible AI Promotion: Putting fairness, transparency, and privacy at the forefront of our fraud detection model building and deployment.
Real-World Implementation Support: Providing ideas for designing real-world fraud detection systems for banks, gaining customers' trust, and preventing economic loss.

II. LITERATURE SURVEY

Numerous papers have been devoted to machine learning approaches to detecting credit card fraud, offering thoughtful commentary on the algorithm's performance and matters of real-world deployment. A pioneering study by Prajal Save et al. [1] introduced a multi-stage system incorporating Luhn's algorithm for initial card number screening, followed by behavioral analysis based on outlier detection and address match checks. The model uses the Bayes Theorem to enhance decision-making and dynamically update the probability of fraud. This is a blend of statistical analysis and probabilistic inference, making fraud classification more reliable.

Subsequently, Vimala Devi et al. [2] utilized three machine learning classifiers, Support Vector Machine (SVM), Random Forest, and Decision Tree, comparing their performance by prevalence-dependent and prevalence-independent metrics. The study demonstrated that Random Forest was superior to the other classifiers because of its ensemble property, minimizing overfitting and maximizing generalization on class-imbalanced datasets.

Further extending algorithmic contrasts, Popat and Chaudhary [3] examined an extensive variety of supervised techniques, including Decision Trees, Fuzzy Logic, Artificial Immune Systems, Neural Networks, Deep Learning, Logistic Regression, Naïve Bayes, SVM, and Genetic Algorithms. They contrast methodically outlier detection, clustering, and prediction algorithms, showing how machine learning techniques of such diverse types can offer complementary strengths for fraud detection.

Xuan Shiyang et al. [4] emphasized Random Forest, utilizing it to simulate transactional behavior. Models were trained on valid and fraudulent transactions via CART-based random trees, which improved detection by identifying subtle behavioral variations. The findings confirmed Random Forest's ability to minimize false negatives without compromising high accuracy, enhancing its dependability for fraud detection.

Vaishnavi Nath Dornadula and Geetha Sa [5]. They group cardholders by transaction value, using a sliding window to monitor changing behavior patterns. A feedback mechanism handled concept drift, allowing the system to respond to new fraud tactics. Experimented on a European credit card fraud data set, the model showed enhanced detection performance in real-time, high-volume settings.

Mittal et al. [6] contrasted supervised and unsupervised strategies, testing classic classifiers, deep neural networks, and combinations. Their findings concluded that although used less often, unsupervised algorithms performed better at dealing with data imbalance and identifying rare fraud instances, an essential benefit in highly skewed data.

Akila and Deepa [7] suggested a multi-algorithmic scheme that blended Anomaly Detection, K-nearest neighbor (KNN), Random Forest, K-means clustering, and Decision Trees. The model assigned a dynamic scam score to every transaction, and the best algorithm was chosen depending on contextual parameters. This adaptive scenario-based model indicated better accuracy for fraud cases, emphasizing the flexibility aspect of fraud detection pipelines at the algorithm level.

Xiaohan Yu et al. [8] designed a deep learning-based fraud detection system using Deep Neural Networks (DNN). Focal loss functions and data preprocessing handled data imbalance and maintained the model sensitive to minority-class fraudulent instances. The outcome proved the suitability of deep learning architectures in handling large, high-dimensional transactional datasets.

DOI: 10.48175/IJARSCT-25301

Siddhant Bagga et al. [9] compared nine machine learning algorithms, i.e., Logistic Regression, KNN, Random Forest, Quadrant Discriminative Analysis, Naïve Bayes, Multilayer Perceptron, AdaBoost, Ensemble Learning, and Pipelining. The study used the ADASYN oversampling technique for dataset balancing, and performance was measured based on accuracy, recall, F1-score, balanced classification rate, and Matthews correlation coefficient. Data balancing and ensemble techniques must be fused to make fraud detection precise.

Urban and Carrasco [10] investigated using Deep Neural Networks to reduce false positives in fraud detection systems. They analyzed alerts generated by a running Fraud Detection System (FDS), marking them as valid or false. The best-performing configuration achieved a 35.16% reduction in false positives with a 91.79% fraud detection rate, demonstrating deep learning's ability to eliminate spurious alerts without sacrificing detection performance.

Sevkli and Kibria [11] introduced a grid-search optimized deep learning model, comparing it with traditional Logistic Regression and SVM classifiers. The study demonstrated that hyperparameter tuning significantly improved model accuracy, underscoring the importance of optimization techniques in fraud detection pipelines.

Rejwan Bin Sulaiman et al. [12] extensively analyzed Random Forest, SVM, and Artificial Neural Networks, proposing a hybrid solution that integrates ANN with Federated Learning. This approach enhanced fraud detection accuracy while ensuring data privacy, a crucial advancement in compliance-driven financial environments. The study highlighted how hybrid architectures combining local learning with centralized model updates improve performance without compromising data security.

Btoush et al. [13] systematically reviewed 181 studies published between 2019 and 2021, covering supervised, unsupervised, and hybrid approaches. Their analysis identified significant challenges, including data imbalance, concept drift, and the need for real-time detection. The study emphasized the underutilization of semi-supervised and unsupervised methods, recommending further exploration of these approaches to enhance detection performance and resilience.

Patricia Rodríguez Vaquero [14] integrated upcoming machine learning techniques, including Genetic Algorithms with Random Forest (GA-RF), Decision Trees (GA-DT), and Artificial Neural Networks (GA-ANN). Generative Adversarial Networks (GANs) with Modified Focal Loss were also explored for class imbalance and adapting fraud patterns. The findings emphasized hybrid models and federated learning to develop resilient, privacy-centered fraud detection systems, particularly in high-risk, data-sensitive environments.

Oketola et al. (2023) [15] critically examine some machine-learning techniques applied to credit card fraud detection. It encompasses supervised algorithms such as Logistic Regression, Decision Trees, Random Forest, Support Vector Machine, Naïve Bayes, and K-Nearest Neighbors and unsupervised such as K-means clustering. The authors comprehensively discuss data preprocessing methods, such as feature selection, data cleaning, and class imbalance handling, for improved model performance. Furthermore, the article compares these methods with performance metrics like precision, accuracy, recall, F1-score, and AUC-ROC, which outline each method's weaknesses and strengths. Issues like model interpretability, data drift, and restricted accessibility are presented as areas of research that identify areas of research to be done in the topic at hand, e.g., real-time fraud detection systems, deep learning architecture, and ensemble learning. This book is an excellent source for fraud detection practitioners and researchers interested in developing more robust and accurate fraud detection mechanisms.

III. METHODOLOGY

The system for detecting credit card fraud proposed uses a comprehensive, multi-stage method to achieve high detection rates while maintaining data privacy. The method adopts a federated learning architecture to combine data preprocessing, machine learning model training, testing, and iterative improvement. The system is dynamic in adapting to new fraud tactics and provides consistent model performance. The system design follows a series of steps: data gathering and preprocessing, then model training and testing, and then culminating in real-time prediction implementation. Below is the proposed system's block diagram:

DOI: 10.48175/IJARSCT-25301

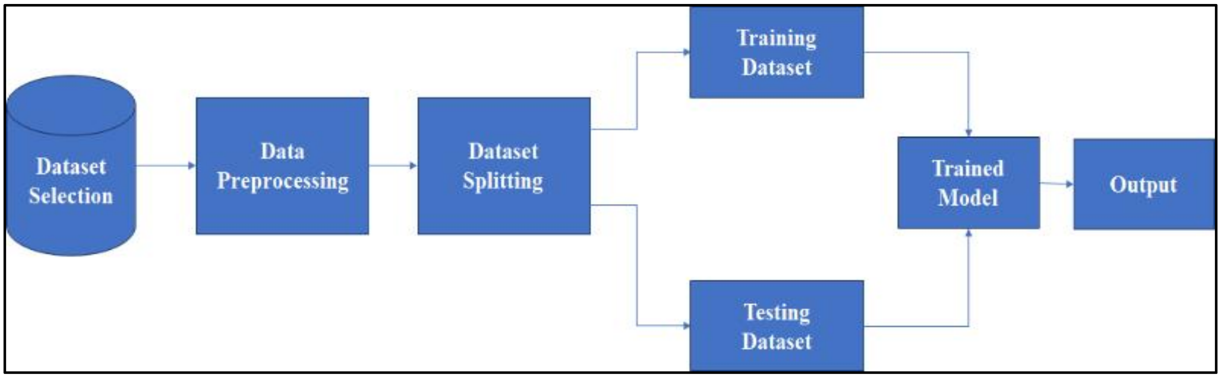

Figure : Block diagram of the proposed system

A. Data Collection and Preprocessing

The data utilized by the system is the "Credit Card Fraud Detection Dataset 2023," which contains more than 550,000 anonymized credit card transactions of European cardholders. The data records various fraud patterns with geographical specificity, which is crucial due to various fraud patterns across regions.

The data is anonymized to ensure observance of privacy legislation such as GDPR by concealing identifiable information while transactional integrity is retained. The procedure is essential to enable fraud detection without exposing sensitive user information. The second fraud detection system design procedure is data preprocessing, a serious procedure whose impact directly affects model performance and reliability. Missing values must be addressed first so that data will be complete and no inaccuracy or bias is added during training. Missing or null values can derail the learning process, leading to incorrect patterns and lower model accuracy. Secondly, feature scaling normalizes quantitative features such as transaction values. Normalization is used to scale features so that large-scale variables do not dominate small-scale variables, thereby improving the convergence and stability of machine learning algorithms. Additionally, encoding methods convert categorical variables such as merchant categories or transaction types to numerical form. This is required because most machine learning algorithms take numerical input and are not inherently able to handle categorical data. The data is finally balanced through techniques such as the Synthetic Minority Over-sampling Technique (SMOTE) to hold the highly imbalanced classes. Fewer than 0.5% of all data are generated transactions, and the models identify helpful patterns. SMOTE creates artificial samples from the minority class, such that training is done from a more balanced set of samples, which, as a result, has a more remarkable ability to identify rare suspect instances.

B. Model Training

In this study, the system employs two basic machine learning algorithms: Logistic Regression and Random Forest. Logistic Regression is a well-established statistical model applied in binary classification to predict the likelihood that a transaction is fraudulent or legitimate. It is valued for being easy to interpret, computationally efficient, and straightforward, and therefore acts as a good baseline for fraud detection problems. On the other hand, Random Forest is a bagging algorithm that aggregates the prediction of several decision trees to maximize overall classification accuracy and avoid overfitting risk. By aggregating output from many trees, Random Forest enhances model stability and generalization, particularly for unbalanced and complex data. To facilitate practical training and testing, the dataset is divided into 75% training, 15% validation, and 10% testing to allow the models to generalize to unseen data properly. Logistic Regression and Random Forest models are incrementally trained with continuous tuning of their parameters to optimize the top performance metrics such as precision, recall, F1-score, and accuracy. These. These are particularly crucial fraud detection application scenarios. The. Data is highly imbalanced: The. Misclassification costs—particularly false negatives—could be high.

DOI: 10.48175/IJARSCT-25301

C. Real-Time Prediction and Evaluation

The final phase involves real-time transaction classification. Each incoming transaction is evaluated using the trained model, which outputs a fraud probability score. Transactions with a high probability of fraud are immediately flagged for manual review or automatic intervention, depending on the system's deployment configuration.

D. Performance Evaluation

Performance testing of the trained models is the last step. Various metrics like Precision, Recall, F-score, and Accuracy are used to test the performance of the dialect recognition algorithm. The F-score balances precision and recall while accuracy estimates overall correctness. Precision estimates the correctness of optimistic predictions, while recall estimates the correctness of marking positive examples. All these measurements combined test how well the system identifies and differentiates between Marathi dialects.

The precision, recall, F1 score, and accuracy evaluate the performance of the given system. The measures used for classifying the tasks are usually the accuracy, precision, recall, and F1 score. While examining a few properties of a classifier's prediction, they tell us valuable information about its performance. Explain each of them individually:

Accuracy: By computing the ratio of accurate predictions to total predictions, accuracy assesses the overall accuracy of the classifier's predictions. It has the following definition:

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

where the numbers represent the amount of accurateoptimistic predictions (TP), accuratepessimistic predictions (TN), false optimistic predictions (FP), and false pessimistic predictions (FN). Although accuracy gives a broad picture of the classifier's performance, unbalanced datasets might not be a good fit for accuracy.

Precision: The percentage of accurately anticipated positive cases among all positively predicted instances is the topic of precision analysis. It is calculated as:

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

Precision provides insight into the classifier's ability to avoid false positives. A higher precision indicates a lower rate of misclassifying negative instances as positive.

Recall (Sensitivity or True Positive Rate): The percentage of accurately anticipated positive events among all actual positive instances is known as recall. It is calculated as:

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

Recall highlights the classifier's ability to identify positive instances correctly, and it is beneficial when the goal is to minimize false negatives.

F1 score: Recall and accuracy are combined into one statistic, the F1 score, which balances both measurements. It is computed as the harmonic mean of recall and accuracy.:

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

Accuracy and recall are balanced by considering erroneous positives and false negatives in the F1 score. It is helpful when there is an unequal distribution of classes or when recall and precision are equally critical.

These measures are essential in binary classification problems since there are positive and negative classes. Calculating them separately for every class and then averaging them (e.g., micro-averaging, macro-averaging) can also be used for multi-class classification problems.

DOI: 10.48175/IJARSCT-25301

IV. RESULT AND DISCUSSION

To evaluate the performance of the suggested credit card fraud detection system, Logistic Regression, and Random Forest classifiers were both trained and compared on a real-world highly imbalanced data set. Preprocessing was performed on the data set; it was split into training, validation, test sets, and SMOTE-balanced to overcome the scarcity of fraudulent transactions. Accuracy, precision, recall, and F1-score were utilized to compare each model as performance measures. These are decisive steps in fraud detection in which false positives lead to legitimate transactions being declined, and false negatives lead to fraudulent transactions remaining undetected. The results of the model evaluation are given in Table I below.

Table 1: Performance analysis of ML algorithm for credit card fraud detection

Algorithm	Precision (%)	Recall (%)	F1-Score (%)	Accuracy (%)
Logistic Regression	92	79	84	99.90
Random Forest	98	89	93	99.95

Table I identifies that the Random Forest model significantly outperforms Logistic Regression on all the performance metrics. While Logistic Regression provides a good accuracy of 99.90%, its recall value of 79% specifies that it fails to detect some of the fraudulent transactions. However, Random Forest possesses an accuracy of 99.95% and a perfect 98% precision, i.e., most of the transactions it identifies as fraud are indeed fraud. Furthermore, it also has a very high recall of 89%, and hence, it can identify nearly all fraud cases, resulting in an F1-score of 93% with strength.

The above results highlight the strength of ensemble learning in fraud detection. Despite its simplicity and interpretability, Logistic Regression cannot pick up on the complex nonlinear relationships generally present in fraud cases. It performs pretty well but is constrained in recall, a critical metric in fraud detection since it is the metric of the model's ability to identify actual frauds. On the other hand, Random Forest performs excellently, owing to its ability to reduce variance by having numerous decision trees, each trained on random subsets of data and attributes. Its ensemble nature enables it to detect complex patterns and relationships that a linear model like Logistic Regression might overlook.

The findings validate that Random Forest is better than Logistic Regression in credit card fraud detection applications. It provides better accuracy and almost flawless fraud detection, reducing false positives and false negatives to the barest minimum. These findings validate the application of ensemble-based models in actual fraud detection systems, particularly where stability and reliability are of utmost importance. Future research can also delve deeper into deep learning-based methods and real-time deployment architectures to improve detection performance in changing environments.

V. CONCLUSION

The performance test, as analyzed by some of the most significant performance metrics such as precision, recall, F1-score, and accuracy, indicated that Random Forest considerably performs better than Logistic Regression in terms of performance with more excellent fraud detection rates without increasing false positives and false negatives to a considerable degree. Even though Logistic Regression has interpretability and computational advantages, it lags in identifying complex patterns associated with fraudulent patterns. Conversely, Random Forest's ensemble approach is more accurate, reliable, and ideal for real-world operational fraud detection systems. The findings above highlight the strength of ensemble learning to detect fraud. Though easy to interpret and simple, Logistic Regression fails to capture the complex nonlinear relationships that always prevail in fraud situations. It performs well but is constrained by recall because it is the most critical measure in fraud detection, as it measures the model's ability to identify actual fraud. Random Forest, however, performs exceptionally well because it can minimize variance by using multiple decision trees, each trained on random sets of features and data. Its collaborative structure makes it capable of detecting faint patterns and relationships that a linear model such as Logistic Regression may fail to identify.

The results confirm that Random Forest is superior to Logistic Regression for use in credit card fraud detection systems. It is more accurate and near-perfect in detecting fraud, minimizing false positives and negatives to the minimum. These results confirm the use of ensemble models in actual fraud detection systems, especially where

DOI: 10.48175/IJARSCT-25301

reliability and stability are high. Future studies can also explore deep learning-based techniques and real-time deployment platforms to advance detection in changing environments.

REFERENCES

[1]. P. Save, P. Tiwarekar, K. N., and N. Mahyavanshi, A Novel Idea for Credit Card Fraud Detection using Decision Tree,‖ Int. J. Comput. Appl., vol. 161, no. 13, pp. 6–9, 2017, doi: 10.5120/ijca2017913413.

[2]. J. Vimala Devi and K. S. Kavitha, Fraud Detection in Credit Card Transactions using Classification Algorithms,‖ Int. Conf. Curr. Trends Comput. Electr. Electron. Commun. CTCEEC 2017, pp. 125–131, 2018, doi: 10.1109/CTCEEC.2017.8455091.

[3]. R. R. Popat and J. Chaudhary, A Survey on Credit Card Fraud Detection Using Machine Learning,‖ Proc. 2nd Int. Conf. Trends Electron. Informatics, ICOEI 2018, no. Icoei, pp. 1120–1125, 2018, doi: 10.1109/ICOEI.2018.8553963.

[4]. S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, and C. Jiang, Random forest for credit card fraud detection,‖ ICNSC 2018 - 15th IEEE Int. Conf. Networking, Sens. Control, pp. 1–6, 2018, doi: 10.1109/ICNSC.2018.8361343.

[5]. V. N. Dornadula and S. Geetha, Credit Card Fraud Detection using Machine Learning Algorithms,‖ Procedia Comput. Sci., vol. 165, pp. 631–641, 2019, doi: 10.1016/j.procs.2020.01.057.

[6]. S. Mittal and S. Tyagi, Performance evaluation of machine learning algorithms for credit card fraud detection, Proc. 9th Int. Conf. Cloud Comput. Data Sci. Eng. Conflu. 2019, pp. 320–324, 2019, doi: 10.1109/CONFLUENCE.2019.8776925.

[7]. M. Deepa and D. Akila, ―Survey Paper for Credit Card Fraud Detection Using Data Mining Techniques, Int. J. Innov. Res. Appl. Sci. Eng., vol. 3, no. 6, p. 483, 2019, doi: 10.29027/ijirase.v3.i6.2019.483-489.

[8]. X. Yu, X. Li, Y. Dong, and R. Zheng, ―A Deep Neural Network Algorithm for Detecting Credit Card Fraud, Proc. - 2020 Int. Conf. Big Data, Artif. Intell. Internet Things Eng. ICBAIE 2020, pp. 181–183, 2020, doi: 10.1109/ICBAIE49996.2020.00045.

[9]. S. Bagga, A. Goyal, N. Gupta, and A. Goyal, ―Credit Card Fraud Detection using Pipeline and Ensemble Learning,‖ Procedia Comput. Sci., vol. 173, pp. 104–112, 2020, doi: 10.1016/j.procs.2020.06.014.

[10]. R. San Miguel Carrasco and M.-A. Sicilia-Urban, Evaluation of Deep Neural Networks for Reduction of Credit Card Fraud Alerts, IEEE Access, vol. 8, pp. 186421–186432, 2020, doi: 10.1109/access.2020.3026222.

[11]. G. Kibria and M. Sevkli, Application of Deep Learning for Credit Card Approval : A Comparison with Application of Deep Learning for Credit Card Approval : A Comparison with Two Machine Learning Techniques, no. January, pp. 0–5, 2021, doi: 10.18178/ijmlc.2021.11.4.1049.

[12]. R. B. Sulaiman, V. Schetinin, and P. Sant, "Review of Machine Learning Approach on Credit Card Fraud Detection," Human-Centric Intelligent Systems, vol. 2, pp. 55–68, 2022. DOI: 10.1007/s44230-022-00004-0.

[13]. E. A. L. Marazqah Btoush, X. Zhou, R. Gururajan, K. C. Chan, R. Genrich, and P. Sankaran, "A Systematic Review of Literature on Credit Card Cyber Fraud Detection using Machine and Deep Learning," PeerJ Comput. Sci., vol. 9, p. e1278, 2023. DOI: 10.7717/peerj-cs.1278.

[14]. P. Rodríguez Vaquero, "Literature Review of Credit Card Fraud Detection with Machine Learning Methods," Master of Science Thesis, Tampere University, 2023.

[15]. G. Oketola, T. Gbadebo-Ogunmefun, and A. Agbeja, "A Review of Credit Card Fraud Detection using Machine Learning Algorithms," Preprint, Dec. 2023. DOI: 10.13140/RG.2.2.22552.98562/1