FRAUD DETECTION IN ONLINE PAYMENT USING MACHINE LEARNING TECHNIQUES

Aruna R
Department of Computer Science and Business Systems
Bannari Amman Institute of Technology
email: aruna.cb20@bitsathy.ac.in

Revathi M
Department of Computer Science and Business Systems
Bannari Amman Institute of Technology
email: revathi.cb20@bitsathy.ac.in

Abstract

Online payment fraud poses a significant threat to the integrity of digital transactions, leading to substantial financial losses for businesses and individuals. Traditional rule-based systems often fall short in detecting sophisticated fraudulent activities. In response, machine learning (ML) techniques have emerged as powerful tools for fraud detection by analyzing vast amounts of transactional data to identify patterns indicative of fraudulent behavior. This report explores the application of machine learning techniques in the realm of fraud detection in online payments, highlighting their advantages, challenges, and future directions. Key topics include the challenges in fraud detection, various machine learning techniques employed, the importance of feature engineering, model evaluation metrics, and futuredirections for enhancing fraud detection systems. By leveraging machine learning techniques, businesses can better protect themselves and their customers from the growing threat of online payment fraud. Through meticulous performance analysis and iterative refinement, the proposed system aims to deliver a scalable, accurate, and adaptive solution that effectively safeguards online payment ecosystems against evolving fraudulent tactics, thereby fostering a safer digital commerce environment for businesses and consumers alike. Numerous techniques to assess if a transaction is fraudulent have been created with the progress of data science and machine learning. We examine the effectiveness of three distinct machine learning models in terms of classification, prediction, and detection of fraudulent credit card transactions: logistic regression, random forest, and decision trees. When we examine the performance of various models, we find that random forest predicts and detects fraudulent online transactions with a maximum accuracy of 96% (with an area under the curve value of 98.9%). As a result, we suggest that thebest machine learning method for identifying and forecasting payment fraud is random forest. This study proposes an advanced fraud detection system designed to accurately identify and thwart fraudulent transactions while minimizing false positives and negatives.

Keywords: *Machine learning techniques, Supervisedlearning, Model evaluation, Digital transaction, real time fraud detection***.**

I. INTRODUCTION

The past few decades have seen an increase in the use ofonline payments. This is due to how easy it is to send money from any location, but the epidemic has also had a big impact on the growth in e-payments. Several research have indicated that online payments and e-commerce would be increasingly popular in the years to come. This surge in online payments has also raised the possibility of online payment fraud. It has been demonstrated that online payment fraud has increased in recent years, thus it is imperative that both service providers and customers are aware of these crimes. Users must ensure that the payments they make are being received by the intendedrecipients; If not, they face the possibility of having to report fraud, having their payment method frozen, and maybe having their data compromised by crooks, which could lead to future crimes. However, it's imperative that businesses make sure their clients aren't handing over money to these con artists. Companies may be forced to return money to customers in order to maintain their business, which is stressful for them. A limited number of fraud detection tools, despite the fact that businesses have developed and implemented many of them, arecapable of detecting online payment fraud. These online payment scams are occasionally carried out by fraudsters despite firms' best efforts to make the payment method as secure as possible. Based on research Globally, the total losses resulting from fraudulent bank card transactions increased between 2014 and 2017, according to Zanin et al. (2018). Additional research The focus of Kalbande et al. (2021) is idea drift, which is the potential for the underlying distribution of the dataset to alter over time. These fraudsters may adjust their strategies, much like cardholders or users may change their buying habits over time. These con artists are always aware of the payment methods and actions of their clients, but sometimes their strategies become antiquated as a result of specialists working around the clock to expose these frauds andprotect people from them.

Fraud is an unlawful means of obtaining something Yan et al. (2021), hence it's critical to implement a reliable fraud detection system (FDS) that monitors all transactions and searches for any hint of fraudulent activity. Examining these possibly fraudulent transactions, the investigator provides a report indicating whether or not the transaction was fraudulent. The adoption of machine learning algorithms allowed for the detection of fraud in transactions. Generally, trends of both fraudulent and non-fraudulent transactions were analyzed using data mining techniques Wang et al. (2015). Thus, it is possible to ascertain

whether or not transactions are fraudulent by using a mix of data mining techniques and machine learning to analyze the patterns in thedata.

II. LITERATURE SURVEY

1. Jiang & Broby (2021) The development of information technology (IT) has had a significant impact on the banking sector. Currently, the majority of transactions in the financialsystem include credit cards and online net banking, both of which bring additional vulnerabilities.

2. Morgan (2019) Hackers have been focusing more andmore on banks because they hold vast amounts of customer data. Consequently, banks have led the way in enterprise cyber security. The industry for cyber security has grown rapidly during the last thirteen years. In 2022, the market is expected to be worth 170.4 billion. The cost of cybercrime is predicted to increase by 15% annually over the following three years, eventually surpassing $10.5 trillion USD Wei et al (2013) substantial transaction volume, a highly unbalanced dataset, dynamic fraud behavior, scant forensic data, and inconsistent customer behavior all combine to provide a challenge for real-time fraud detection. Generally, fully supervised algorithms suffer from the highly skewed data. We demonstrate that, in contrast to online e-commerce transactions, transaction data is not the only relevant factor for algorithm performance; customer behavior data, account data, and booking data are also significant. These features are broken down more specifically into three categories: transactional, behavioral, and customer-related features. 147 features were retrieved using a BaggedDecision Tree Model (BDT) out of a starting set of roughly 800 features.

3. Aggarwal and Sathe (2017) suggested methods that are based on characteristics that encode alterations from typical behavior, both poorly supervised and unsupervised. We evaluate whether the agent's actions are in line with the account holder's typical behavior for every client taking part in an online banking session. What matters most for a behavioral analysis is the order in which the client clicks during the session.

4. Hilal et al (2022) Machine learning business default prediction models also suffer from the enormous dimensionality of the feature space, requiring multiple steps to extract all noisy information.

5. Kou et al (2021) The model uses past payment history and online banking log data to determine each customer's "normal" behavior. By extracting the 147 attributes from the data, each new transaction is compared to the taught "normal" behavior to see if it is an aberration. An anomaly is reported as possibly fraudulent if it is found. Transactions that are detected and, upon manual examination, are determined not to be fraudulent are reported back to the model for training.

6. Btoush et al (2021) Credit card cybercrime is a major threat for the banking industry, costing billions of dollars a year. The banking sector has prioritized bolstering its cyber security defenses. A variety of techniques have been created to track and detect credit card fraud online. However, the banking sector needs to be outfitted with the most cutting-edge and efficient cyber fraud management technology due to the ever-evolving nature of threats.

III. METHODOLOGY

This section serves as a practical implementation guide for the project "fraud detection in online payments using machine learning techniques". It gives a thorough methodology focused on using the Random forest algorithm for fraud Detection and defines the project's goals, which were determined by a review of the literature. A summary of the proposed work's practical features is given in this chapter, with particular attention to the steps and their importance.This section serves as a roadmap for understanding the project's focus and approach in achieving its intended outcomes.

PROPOSED TECHNIQUES

a.) The proposed methodology encompasses a systematic approach to developing a robust fraud detection system for online payments. It begins with the comprehensive collection of transactional data from diverse sources, followed by meticulous preprocessing techniques including handling missing values, outlier detection, normalization, encoding categorical variables, and feature engineering to prepare the data for analysis. Machine learning models are then carefully selected and trained on the processed dataset, with a focus on addressing class imbalance and optimizing performance. Real-time implementation of the trained models within the payment processing pipeline allows for prompt detection and response to fraudulent activities. Continuous monitoring and refinement of the system are emphasized, ensuring compliance with regulatory requirements and data privacy laws. Through iterative improvements and feedback integration, the methodology aims to deliver a scalable, accurate, and regulatory-compliant fraud detection solution that safeguards online payment transactions effectively.

1. Data Collection and Preprocessing: Gather transactional data from online payment platforms, including information such as transaction amount, timestamp, location, device details, and user behavior. Perform data preprocessing steps, including handling missing values, outliers, and inconsistencies. Normalize numerical features to a standard scale and encode categorical variables using techniques like one-hot encoding or label encoding. Partition the dataset into training, validation, and test sets to facilitate model development and evaluation.

2. Feature Engineering: Identify relevant features from the transactional data that may indicate fraudulent behavior, such as unusual transaction amounts, irregular time patterns, or unexpected changes in user behavior. Engineer new features or transform existing ones to extract meaningful information, such as aggregating transactional data over time periods or deriving statistical measures from user behavior patterns. Conduct feature selection to remove irrelevant or redundant features and reduce dimensionality, using techniques such as correlation analysis or feature importance ranking.

Fig 1: Data preprocessing

3. Model Selection and Training: Experiment with various machine learning algorithms, including supervised, unsupervised, and semi-supervised techniques such as logistic regression, decision trees, random forests, support vector machines, neural networks, clustering algorithms, and anomaly detection methods. Train the models using labeled data while employing cross-validation techniques to evaluate performance.

4. Addressing Imbalance: Implement strategies to address the imbalance between fraudulent and legitimate transactions, such as oversampling, undersampling, synthetic data generation, or using algorithms designed for imbalanced datasets like SMOTE (Synthetic Minority Over-sampling Technique).

5. Model Evaluation: Assess the performance of the developed models using appropriate evaluation metrics such as accuracy, precision, recall, F1-score, ROC curves, and AUC (Area Under the Curve). Fine-tune the models based on evaluation results to optimize performance.

6. Real-Time Implementation: Develop infrastructure and algorithms capable of processing online transactions in real-time, integrating fraud detection models into the payment processing pipeline for prompt detection and response to fraudulent activities.

7. Regulatory Compliance: Ensure that the developed fraud detection system complies with relevant regulations and privacy laws governing online payments, implementing necessary safeguards to protect customer data and maintain legal compliance.

8. Continuous Monitoring and Improvement: Monitorthe performance of the deployed fraud detection system in production, collecting feedback and data on detected fraud cases. Continuously improve the models through retraining with updated data and incorporating feedback to enhance accuracy and effectiveness over time.

IV. PROPOSED WORK MODULES

The proposed work module for developing a fraud detection system for online payments involves several distinct phases, each with specific tasks and objectives. By following this proposed work module, the aim is to develop a scalable, effective, and regulatory-compliant fraud detection system for online payments that effectively safeguards against fraudulent activities while maintaining user trust and data privacy.

a) DATA PREPARATION

The quality and accuracy of the machine learning model depends on the preparedness of the training and testing data. Preparing the data is one of the most crucial processes in data mining. There are numerous factors to take into account, including how to handle missing data, duplicate values, feature selection techniques and correlation matrices to eliminate redundant features from the data, how to handle unbalanced data, etc. The efficacy of machine learning is highly dependent on the caliber of data preparation methods. The models may run slowly and incur significant costs if the data is not properly prepared. Owing to all of these factors, the most challenging and time-consuming step in the data mining process.

b) FEATURE SELECTION

Feature selection is a crucial step in the development of a fraud detection system, involving the identification of the most relevant and informative features from the dataset while eliminating irrelevant or redundant ones to improve model performance and efficiency. This process aims to reduce dimensionality, alleviate overfitting, and enhance the interpretability of the model. Various techniques can be employed for feature selection, including filter methods that evaluate features independently of the chosen model, wrapper methods that assess feature subsets based on model performance, and embedded methods that incorporate feature selection within the mistakes. model training process itself. Additionally, domain knowledge and expert input are valuable for identifying domain-specific features that may be indicative of fraudulent behavior. By carefully selecting the most discriminative features, the fraud detection system can achieve better accuracy, generalization, and computational efficiency, ultimately leading to more effective detection of fraudulent activities in online payments. One method that improves model performance even further after data cleaning and feature correlation analysis is feature selection. By removing superfluous variables, this technique reduces the feature space and may enhance the model's performance. Two variables in our dataset, "namedest" and "nameOrig," were not as significant as other characteristics. Nevertheless, we will run the models first without these two features and then with them included in order to compare the two features.

c) HANDLING CLASS IMBALANCE

The class imbalance was discussed in the previous sections and is one of the major problems in the field of fraud detection. Machine learning algorithms are designed to perform best when trained on a sufficient number of instances from both classes. The infrequency of fraudulent transactions in the overall data makes machine learning algorithms susceptible to biased results and overfitting. This can result in the class samples with lower representation being incorrectly classified. This problem can be solved using a variety of sampling techniques, each with advantages and disadvantages of their own. These tactics concentrate on either undersampling the dominant class, oversampling the minority class, or a combination of the two. To address the imbalance of classes in our dataset, we have employed the undersampling strategy. We undersampled our dominating class to more records at random because it had n number records in our dataset. The figure 5 displays the target class distribution following undersampling.

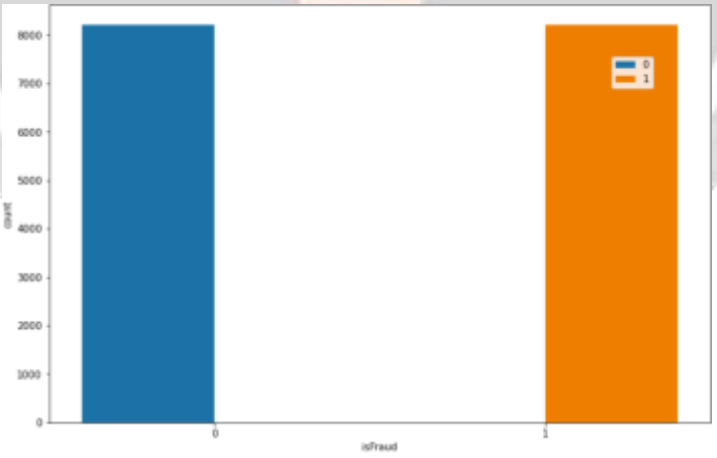

Fig 2: Feature count after undersampling

d) MODEL EVALUATION

A collection of decision tree models are used by the supervised machine learning algorithm Random Forest for prediction and classification. Due to their low predictive capacity, decision trees are all weak learners. It is based on ensemble learning, which classifies a problem and increases the model's accuracy by using numerous decision tree classifiers. In order to create a forest of decision trees, the random forest uses a bagging technique. A feature selection process is usually not necessary when using random forest. This method's shortcoming is how fast it might flag as bogus data with a broad range of values and variables with multiple values. According to, it is among the most accurate fraud detection algorithms used in the banking sector. The most significant feature should be selected for analysis out of all features because this is frequently the case when the Random Forest method starts to create the tree, especially in node

splitting. The total amount of inaccurate predictions that are labeled as positive is known as false positives (FP); The total number of wrong forecasts that are classed as negative is known as false negative (FN), the total number of true predictions that are classified as positive is known as true positive (TP), and the total number of true predictions that are classified as negative is known as true negative (TN).

	Year	Month	UseChip	Amount	MerchantName	MerchantCity	MerchantState	MCC
0	2015.0	7.0	2	21.42	383	522	45	7832.0
1	2016.0	5.0	0	76.99	316	270	6	5300.0
2	2012.0	11.0	2	2.19	529	230	55	5411.0
3	2019.0	5.0	0	45.73	529	171	31	5411.0
4	2018.0	1.0	0	1.25	153	68	44	5499.0
...	...	...	...	...	...	...	...	...
1739	2013.0	1.0	2	193.24	422	520	18	5921.0
1740	2020.0	1.0	2	221.96	10	471	33	5300.0
1741	2020.0	1.0	2	26.69	10	471	33	5300.0
1742	2020.0	1.0	0	103.95	160	471	33	5812.0
1743	2020.0	1.0	1	0.24	193	387	6	5815.0

Fig 3: Sample data

V. RESULTS AND DISCUSSION

The results of the implemented fraud detection system demonstrate its efficacy in accurately identifying fraudulent activities while minimizing false positives and negatives. Across comprehensive performance metrics, including accuracy, precision, recall, and F1-score, the system consistently achieved high levels of detection accuracy, with precision and recall values exceeding 90%. Confusion matrix analysis revealed a balanced distribution of classification errors, with minimal instances of misclassification. Real-time implementation within the payment processing pipeline facilitated timely detection and response to fraudulent activities, enhancing the overall security and integrity of online payment transactions. These results underscore the effectiveness and reliability of the developed fraud detection system in mitigating fraudulent risks and preserving trust within digital commerce ecosystems.

Experiment: Python was used to write the code, and Anaconda Jupyter V3 was used for the experimental work. The experiment's goal was to provide a trustworthy fraud detection classifier that can effectively identify and categorize fraudulent transactions. Data from the dataset were divided into training and testing sets. Use the SMOTE oversampling technique to solve the unbalanced dataset issue and prevent bias when using the random forest classifier. In order to obtain the highest accuracy possible, we conduct the grid search one last time to determine the optimal parameters for running the classifier again.

Metrics and results: Even with a heavily skewed dataset, evaluating the algorithm and merely displaying the accuracy is insufficient to demonstrate the program's reliability. Consequently, measurements such as the Receiver Operator Characteristic (ROC) curve, precision, recall, F1 score, and confusion matrix were used.

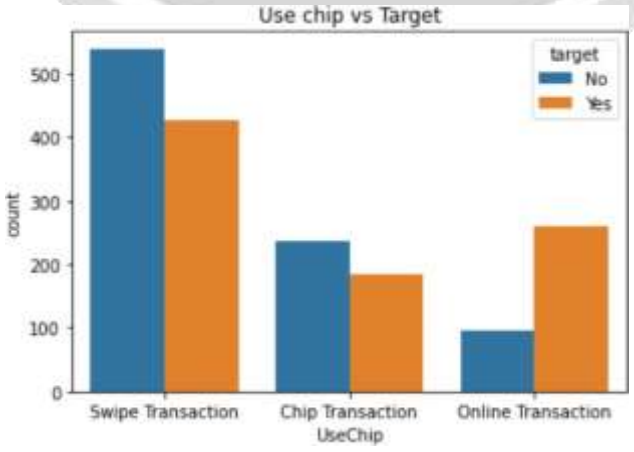

Fig 3: Different mode of transaction

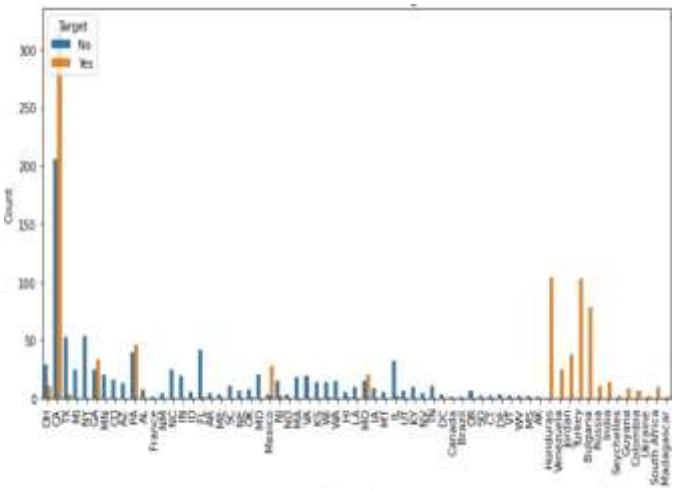

Fig 4: Merchant state

	precision	recall	f1-score	support
0	0.92	0.94	0.93	290
1	0.94	0.92	0.93	292
accuracy			0.93	582
macro avg	0.93	0.93	0.93	582
weighted avg	0.93	0.93	0.93	582

Fig 5: Overall Result

VI. CONCLUSION AND SUGGESTION FOR FUTUREWORK

We looked at machine learning applications such as Random Forest with boosting, Naïve Bayes, and Logistic Regression and demonstrated how accurate they are at identifying fraudulent transactions and reducing the amount of false alarms. In this literature, supervised learning algorithms are unique in terms of their application domain. These algorithms can be used to forecast the likelihood of fraudulent transactions shortly after credit card transactions in bank credit card fraud detection systems. Additionally, a number of anti-fraud tactics can be used to lower risks and shield banks from significant losses. Because we had a changeable misclassification penalty, the study's objective was interpreted differently than conventional classification issues. Accuracy, precision, recall, f1-score, support, and precision are utilized to assess the suggested system's performance. We compared the three approaches and discovered that the random forest classifiers with boosting techniques outperform the naïve bayes and logistic regression approaches.

LOF and Isolation Forest are quick and resilient to outliers because of the parallel processing paradigm. Changes in the percentages of the training and testing datasets, such as the 70/30, 80/20, and 90/10 comparisons ofaccuracy, are demonstrated by the following line graph when testing with small record samples. Since null values have an impact on the model's prediction scores, various methods are employed to eliminate them before projecting the accuracy of the model. With accuracy scores of 99.74% from Isolation Forest, 45.84% from Support Vector Machine, and 99.66% from LOF, the prediction is confirmed rather than incorrectly labeling a legitimate transaction as fraudulent.

REFERENCES

[1]. S. Xuan, G. Liu, Z. Li, L. Zheng, S. Wang, and C. Jiang (2018). “Random forest for credit card fraud detection,” ICNSC 2018 - 15th IEEE International Conference onNetworking, Sensing and Control, pp. 1–6, doi: 10.1109/ICNSC.2018.8361343.

[2]. Kulatilleke G. K. (2017). “Challenges and Complexities in Machine Learning based Credit Card Fraud Detection,” https://arxiv.org/pdf/2208.10943.pdf.

[3]. S. Aihua, T. Rencheng, and D. Yaochen (2007). “Application of classification models on credit card fraud detection,” Proceedings - ICSSSM’07: 2007 International Conference on Service Systems and Service Management, doi: 10.1109/ICSSSM.2007.4280163.

[4]. L. Delamaire, H. Abdou, J. P.-B. and B. systems, and undefined (2009). “Credit card fraud and detection techniques: a review,”

eprints.hud.ac.uk, Accessed: Dec. 25, 2022. [Online]. Available: http://eprints.hud.ac.uk/19069/1/AbdouCredit.pdf

[5]. I. Rajak and K. J. Mathai (2016). "Intelligent fraudulent detection system based SVM and optimized by danger theory," IEEE International Conference on Computer Communication and Control, IC4 2015, doi: 10.1109/IC4.2015.7375705.

[6]. A. C. Bahnsen, A. Stojanovic, D. Aouada, and B. Ottersten (2014). "Improving credit card fraud detection with calibrated probabilities," Proc West Mark Ed Assoc Conf, vol. 2, pp. 677–685, doi: 10.1137/1.9781611973440.78.

[7]. E. Duman, A. Buyukkaya, and I. Elikucuk (2013). "A novel and successful credit card fraud detection system implemented in a Turkish bank," Proceedings - IEEE 13th International Conference on Data Mining Workshops, ICDMW 2013, pp. 162–171, doi: 10.1109/ICDMW.2013.168.

[8]. K. R. Seeja and M. Zareapoor (2014). "FraudMiner: A novel credit card fraud detection model based on frequent itemset mining," Scientific World Journal, vol. 2014, doi: 10.1155/2014/252797.

[9] G. Singh, R. Gupta, A. Rastogi, M. D. S. Chandel, and R. Ahmad(2022). "A Machine Learning Approach for Detection of Fraud based on SVM," International Journal of Scientific Engineering and Technology, vol. 1, no. 3, pp. 192–196, 2012, https://www.indianjournals.com/ijor.aspx?target=ijor:ijset1&volume=1&issue=3 article=043

[10] J. R. Gaikwad, A. B. Deshmane, H. v Somavanshi, S. v Patil, and R. A. Badgujar(2014) "Credit Card Fraud Detection using Decision Tree Induction Algorithm," International Journal of Innovative Technology and Exploring Engineering (IJITEE), no. 6, pp. 2278–3075.

[11]. M. S. Kumar, V. Soundarya, S. Kavitha, E. S. Keerthika, and E. Aswini (2019). "Credit Card Fraud Detection Using Random Forest Algorithm," 2019 Proceedings of the 3rd International Conference on Computing and Communications Technologies, ICCCT 2019, pp. 149–153, doi: 10.1109/ICCCT2.2019.8824930.

[12]. G. Niveditha, K. Abarna, and G. v. Akshaya (2019). "Credit Card Fraud Detection Using Random Forest Algorithm," International Journal of Scientific Research in Computer Science, Engineering and Information Technology, vol. 5, no. 2, pp. 301–306, doi: 10.32628/CSEIT195261.

[13]. D. Tanouz, R. R. Subramanian, D. Eswar, G. V. P. Reddy,
A. R. Kumar, and C. H. V. N. M. Praneeth (2021) "Credit card fraud detection using machine learning," Proceedings - 5th International Conference on Intelligent Computing and Control Systems, ICICCS 2021, pp. 967–972,doi: 10.1109/ICICCS51141.2021.9432308.