International Journal of Advanced Multidisciplinary Research and Educational Development
Volume 2, Issue 2 | March – April 2026 | www.ijamred.com
ISSN: 3107-6513

Machine Learning Approaches for Online Payment Fraud Detection: Challenges and Performance Analysis

Mr. I. GOBI
Faculty, Department of Information Technology, Sri Krishna Adithya College of Arts and Science, Coimbatore, Tamil Nadu, India. 9944331036,gobii@skacas.ac.in
Dhamu D
Student, Department of Information Technology, Sri Krishna Adithya College of Arts and Science, Coimbatore 641042, Tamil Nadu, India.9385702003, dhamuvgp@gmail.com

Abstract -Online payment fraud detection is crucial to safeguarding e-commerce transactions from skilled criminals taking advantage of system vulnerabilities. This framework uses six machine learning algorithms to predict online payment fraud on three datasets: constant, CN7Rule induction, KNN, Tree, Random Forest, Gradient boosting, SVM, Logistic regression, Naive Bayes, Ada boost, neural network, and stochastic gradient descent. My extensive testing has shown that the particular gradient-boosting approach consistently outperforms other algorithms I have investigated. This algorithm's astounding accuracy of 99.7% is astounding. The algorithm became the best-performing framework for online payment fraud detection because of its resilience in a range of testing scenarios. The idea behind the invention is a gradient boosting first-aid solution for electronic fraud.

Keyword- Gradient boosting, E-commerce transactions, Fraud prediction, Accuracy, Resilience, Electronic fraud

.

I. INTRODUCTION

Online payment fraud detection refers to the process of stopping fraud during online transactions. It uses geolocation, transaction monitoring, behavioral analysis, device fingerprinting, and two-factor authentication. Financial institutions can benefit from cooperating with payment service providers, as machine learning and AI algorithms are being dynamically adapted to new fraud [1].

Online payment fraud refers to unethical and illegal acts carried out to deceive an online payment system. Identity theft, payment credentials compromise, phishing & social engineering, lack of security standards with malfunctioning of consumer or merchant systems taking over, international transaction issues as well vulnerabilities related to new technology are among major issues which are on the rise [2].

Machine learning is a growing area of computational techniques that attempts to utilize experience for learning from the environment. Big data is said to be the workhorse of this new era. Machine learning methods have proven to be successful in many fields, including pattern recognition, computer vision, spacecraft engineering, finance, entertainment, computational biology, and biomedical and medical applications [3].

Machine learning is essential in fighting online payment fraud through its automated, data-driven fraud detection and prevention systems. This is how machine learning is used for fraud prevention in online payments [4].

This study's findings prove that we successfully utilized comprehensive algorithms to forecast online payment fraud (cross-validation (10), training (80), and testing (20)). The best approach was gradient boosting Accuracy(0.997). Machine learning can help prevent and detect online payment fraud which we will discuss in the rest of the paper. It can discover trends, evaluate vast quantities of data, and create sound predictions. Machine learning models can identify and highlight suspicious trends by using features like transaction and amount. amount/location/timestamp, user behaviour, and device information. Caprice's final act, a human and tantalite, is essential. The Machine Emin Motel cases dealt with the reliability and relevance of the training data.

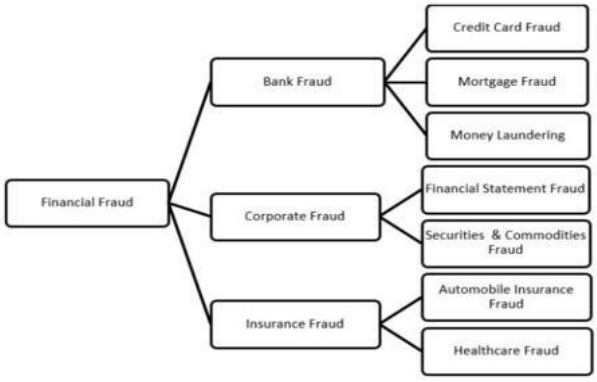


Fig1.Types of Common Fraud

II. RELATED WORK

According to the authors in [5], the model reduced fraud significantly and saved 101,970.52 EGP out of 131,297.83 EGP. The decision tree in the IBM SPSS modeller was used to design it. It achieved an astounding 93.5% precision and 88.45% accuracy. Online and mobile fraud is expected to grow from an estimated $10.7 billion in 2015 to $25.6 billion by the end of the decade, which will have a big impact on the global e-payments industry.

According to the authors of [6], the model's effectiveness is evaluated by comparing it to the Random Forest and Gradient Boosting Machine methods. Results show how well the Light Gradient Boosting Machine performed; in real datasets, it provided timely feedback and attained a total recall rate of 99%. This illustrates the model's ability to identify credit card fraud.

In [7], the authors described the procedure of identifying payment fraud. Machine learning classifiers like Naïve Bayes, C4.5 decision trees, and Bagging Ensemble Learner are recommended for this purpose. Evaluation metrics including accuracy, recall rate, and precision-recall curve area rate are used to gauge how well these classifiers operate. The dataset, which comprised roughly 297,000 credit card transactions from September 2013 to November 2017, contained 3,293 fraudulent transactions. Machine learning classifiers have exceptional performance, with a precision-recall

curve ratio ranging from 99.9% to 100%. The most effective classifier is C4.5 decision trees, which have an incredible 94.12% accuracy rate in predicting fraudulent transactions.

In [8] the authors explained for these detection methods, assessment criteria include specificity, Accuracy, sensitivity, and precision. Naive Bayes, K-Nearest Neighbour, Support Vector Machine, and logistic regression all had accuracy rates of 97.53%, 97.53%, 94.98%, and 99.51%, respectively. Logistic regression is the best method among these, according to the study's comparison findings. Logistic regression has the best accuracy compared to Naive Bayes, K-Nearest Neighbour, and Support Vector Machine. These findings demonstrate how logistic regression outperforms other techniques for detecting credit card fraud.

The study [9] examines credit card fraud detection using various machine learning algorithms, including naïve Bayes, support vector machines, random forests, decision trees, OneR, and AdaBoost. To provide performance metrics, a dataset is assessed using a range of machine learning techniques, with a focus on accuracy. The study comes to the conclusion that the random forest classifier outperforms every other method that was looked at.

In [10] the authors explained the primary goal of this research is to study machine learning methods. The algorithms used are the Random Forest algorithm and the Ada boost method. Algorithms are built on the results of accuracy, precision, recall, and F1-score. Plotting the ROC curve is based on the confusion matrix. The approach with the highest accuracy, precision, recall, and F1 score is considered the most successful for fraud detection when comparing the Random Forest and Ada boost algorithms.

III. METHODOLOGY

a. Datasets Descriptions

The first dataset comprises 1,048,576 records and 10 characteristics. 80% of the dataset was used for training, and the remaining 20% was used for testing. A detailed explanation of each feature may be found below. Step: A duration of one hour. Type: Describes the type of virtual transaction or its classification. Amount: Describes the method of money exchange in this transaction. NameOrig: Identifies the client who initiated the transaction. OldbalanceOrg: This displays the customer's balance prior to the transaction. After a transaction, NewbalanceOrig displays the customer's balance. NameDest: Indicates the recipient of the transaction. OldbalanceDest: Holds the initial balance of the receiver prior to the transaction. NewbalanceDest: These variables document the recipient's updated balance following the transaction. IsFraud: This shows whether or not the transaction is

b. Used Algorithms

These datasets were loaded into twelve various machine learning techniques, such as Gradient Boosting, K Nearest

Features	Type	Value
step	Numerical	From 1 to 743
Type	Classification	Payment or transfer or debit. etc
amount	Numerical	0 to 92.4 m
nameOrig	Alphanumerical	String
oldbalanceOrg	Numerical	0 to 59.6m
newbalanceOrig	Numerical	0 to 49.6m
nameDest	Alphanumerical	String
oldbalanceDest	Numerical	0 to 356 m
newbalanceDest	Numerical	0 to 356 m
isFraud	Classification	0 or 1

Neighbour (k-NN), and Logistic Regression. Naive Bayes, Random Forest, Decision Tree, Constant, CN7 Rule induction, SVM, Ada boost, neural network, and stochastic gradient descent. Statistics including accuracy, recall, precision, and MCC were produced for each algorithm. After that, the data were plotted and contrasted. Later in the publication, there are results, drawings, and a commentary.

1. Gradient Boosting: Several real-world applications have shown the remarkable efficacy of a potent family of machine-learning algorithms known as gradient boosting machines. They are very adaptable to the particular needs of the application and can be learnt in reference to different loss functions, for instance [12].
2-(k-NN): One of the most well-known, straightforward, and fundamental algorithms in data mining and machine learning is k-nearest neighbour (KNN). Nevertheless, KNN's capacity for prediction is restricted; that is, if an instance in the training data set does not fall into any of the specified classifications, KNN cannot accurately forecast it [13].

3. Logistic regression is a statistically-based binary classification technique. It uses a linear model [14]. Hence, it is used to perform regression on a group of variables [15]. It is a normally used technique for predicting patterns in data with unambiguous or numeric attributes [14]. It uses a series of input vectors and a dependent response variable to calculate probability using a logarithm. Probability lies among the specific class.

4. Random forest: Random forest classification is a popular machine learning method for building prediction models in many research settings. Prediction modelling often seeks to boost efficiency and reduce the workload involved with data collection by reducing the number of variables needed to make a forecast. For random forest classification settings, a number of variable selection strategies are possible. On the other hand, there is a dearth of research that suggests the optimal strategy for particular types of datasets [17].

5. Neural networks: Although neural networks are good at self-learning, self-adapting, and generalising, they have a low rate of convergence and are prone to becoming trapped in a local minimum. [18] Input variables are modelled as a layer of vertices in the network, as seen in figure 3. Each

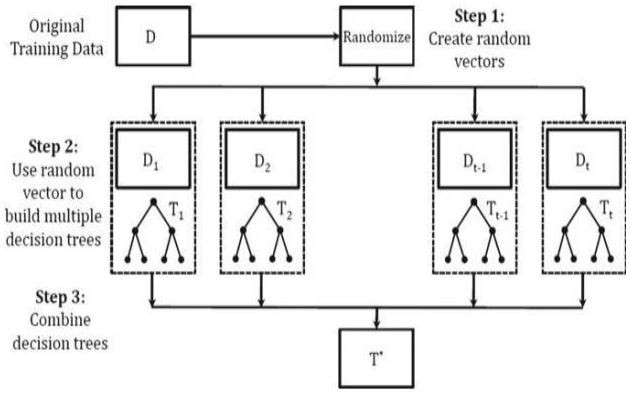


Fig .2 Representation of random forest

c. Performance Metrics

Accuracy, a performance indicator, counts the percentage of examples in a dataset that are properly classified out of all the instances. F1 score aggregates recall and precision into a single number when there is an imbalance between the classes in a binary classification problem; it is especially helpful. Recall is a performance statistic used in classification tasks, sometimes referred to as sensitivity or true positive rate. Precision is a performance metric in machine learning and statistics that measures how well a model generates accurate predictions. It is the proportion of correctly predicted true positives to the total of correctly predicted false positives.

$$\text{Accuracy} = (TN + TP)/(TN + TP + FN + \boldsymbol{RP})$$

$$\text{Precision} = TP/TP + FP$$

connection in the graph is then given a weight distribution. Additionally, the distance from the input nodes is reflected by the placement of the other vertices into distinct layers [19].

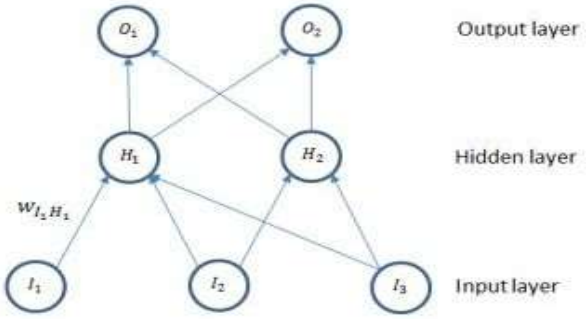


Fig .3 a simple neural network [20].

6. Naïve Bayes is an attribute-free supervised learning technique. The Bayes theorem serves as the foundation. based on the kind of distribution. Naïve Bayes is an attribute-free supervised learning technique. The Bayes theorem serves as the foundation. The following algorithms are available depending on the type of distribution: Three distributions: Gaussian, Multinomial, and Bernoulli. This study uses the Bernoulli distribution to detect fraudulent transactions. [21]

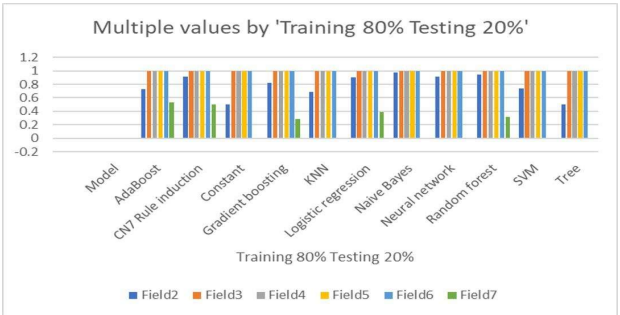
$$c|x) = \frac{P(x \mid c)P(c)}{P(x)}$$

$$\text{Recall} = TP/TP + FN$$

$$\text{Specificity} = (TN/TN + FP)$$

$$MCC = \frac{TP \times TN - FP \times FN}{\sqrt{(TP+FP)(TP+FN)(TN+FP)(TN+FN)}}$$

IV. EXPERIMENTAL RESULTS



The data was collected using Gradient Boosting, AdaBoost, Naïve Bayes, Neural Network, SVM, CN7 Rule

induction, Logistic Regression, Random Forest, Stochastic Gradient Descent, k-nearest Neighbour, Tree, and Constant.

STATISTICS OF ALGORITHMS WITH 10 K-FOLD

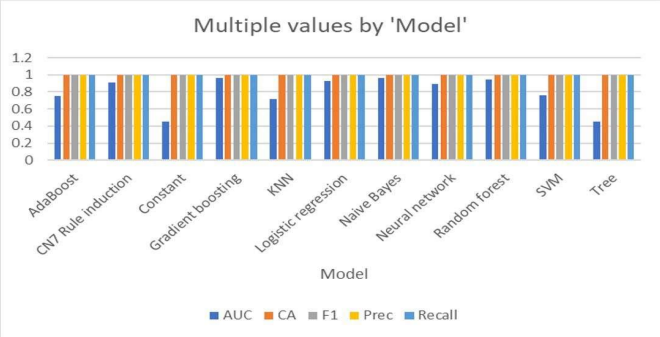


Fig.4 First dataset performance chart with data split

With an incredible 0.967, Gradient Boosting leads the field in machine learning accuracy. Naive Bayes comes in second with a respectable 0.962. The Constant and Tree classifiers, on the other hand, perform the worst, each achieving a lower accuracy rate of 0.455.

With an accuracy of 0.971, Naive Bayes is the best-performing model, followed by Random Forest with 0.948. The least accurate model is t decision tree, which has an accuracy rating of 0.500.

V. CONCLUSION

Machine learning is an effective method for detecting and combating online payment fraud. It can process massive amounts of data, discover trends, and make accurate forecasts. Machine-learning algorithms can detect suspicious trends and flag fraudulent transactions quickly by analysing features such as transaction amounts, locations, timestamps, user activity, and device information. However, they can produce false positives or negatives, thus it is critical to combine human experience with machine learning. Machine learning models' effectiveness is determined by the quality and relevancy of their training data.

VI. REFERENCES

[1] 8ir5Sakharova, I. (2012, June). Payment card fraud: Challenges and solutions. In 2012 IEEE international conference on intelligence and security informatics (pp. 227-234). IEEE

[2] Almazroi, A. A., & Ayub, N. (2023). Online Payment Fraud Detection Model Using Machine Learning Techniques. IEEE Access, 11, 137188-137203

[3] El Naqa, I., & Murphy, M. J. (2015). What is machine learning? (pp. 3-11). Springer International Publishing.

[4] Minastireanu, E. A., & Mesnita, G. (2019). An Analysis of the Most Used Machine Learning Algorithms for Online Fraud Detection. Informatica Economica, 23(1).

[5] Nasr, M. H., Farrag, M. H., & Nasr, M. M. (2022). A Proposed Fraud Detection Model based on e-Payments Attributes a Case Study in Egyptian e-Payment Gateway. International Journal of Advanced Computer Science and Applications, 13(5).

[6] Fang, Y., Zhang, Y., & Huang, C. (2019). Credit Card Fraud Detection Based on Machine Learning. Computers, Materials & Continua, 61(1).

[7] Mijwil, M. M., & Salem, I. E. (2020). Credit card fraud detection in payment using machine learning classifiers. Asian Journal of Computer and Information Systems (ISSN: 2321–5658), 8(4).

[8] Adepoju, O., Wosowei, J., & Jaiman, H. (2019, October). Comparative evaluation of credit card fraud detection using machine 1earning techniques. In 2019 Global Conference for Advancement in Technology (GCAT) (pp. 1-6). IEEE.

[9] Isabella, S. J., Srinivasan, S., & Suseendran, G. (2020). An efficient study of fraud detection system using Ml techniques. Intelligent Computing and Innovation on Data Science, 59.

[10] Pumsirirat, A., & Liu, Y. (2018). Credit card fraud detection using deep learning based on auto-encoder and restricted boltzmann machine. International Journal of advanced computer science and applications, 9(1).

[11] Corballis, M. C., & Nagourney, B. A. (1978). Latency to categorize disoriented alphanumeric characters as letters or digits. Canadian Journal of Psychology/Revue canadienne de psychologie, 32(3), 186.

[12] Natekin, A., & Knoll, A. (2013). Gradient boosting machines, a tutorial. Frontiers in neurorobotics, 7, 21.

[13] Asim, M., & Zakria, M. (2020). Advanced kNN: A Mature Machine Learning Series. arXiv preprint arXiv:2003.00415.

[14] Ngai, E. W., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X. (2011). The application of data mining techniques in financial fr aud detection: A classification framework and an academic review of literature. Decision support systems, 50(3), 559-569.

[15] Nusinovici, S., Tham, Y. C., Yan, M. Y. C., Ting, D. S. W., Li, J., Sabanayagam, C., ... & Cheng, C. Y. (2020). Logistic regr ession was as good as machine learning for predicting major chronic diseases. Journal of clinical epidemiology, 122, 56-69.

[16] Ravisankar, P., Ravi, V., Rao, G. R., & Bose, I. (2011). Detection of financial statement fraud and feature selection using d ata mining techniques. Decision support systems, 50(2), 491-500.

[17] Speiser, J. L., Miller, M. E., Tooze, J., & Ip, E. (2019). A comparison of random forest variable selection methods for class ification prediction modeling. Expert systems with applications, 134, 93-101.

[18] Ding, S., Su, C., & Yu, J. (2011). An optimizing BP neural network algorithm based on genetic algorithm. Artificial intelligence review, 36, 153-162.

[19] Kirkos, E., Spathis, C., & Manolopoulos, Y. (2007). Data mining techniques for the detection of fraudulent financial statements. Expert systems with

ISSN: **3107-6513**

applications, 32(4), 995-1003.

[20] West, J., & Bhattacharya, M. (2016). Intelligent financial fraud detection: a comprehensive review. Computers & security, 57, 47-66.

[21] Chen, S., Webb, G. I., Liu, L., & Ma, X. (2020). A novel selective naïve Bayes algorithm. Knowledge-Based Systems, 192, 10536