Online Payment Fraud Detection by using Machine Learning

M. PRANITHA, 221FA04084
Department of Computer Science and Engineering Vignan's Foundation for Science, Technology and Research
(Deemed to be University) Vadlamudi, Guntur Andhra Pradesh, India
Email: manthripranitha@gmail.com

L. BHUMIKA, 221FA04203
Department of Computer Science and Engineering Vignan's Foundation for Science, Technology and Research
(Deemed to be University) Vadlamudi, Guntur Andhra Pradesh, India
Email: lavubhumika08@gmail.com

B. VAMSI KRISHNA, 221FA04192
Department of Computer Science and Engineering Vignan's Foundation for Science, Technology and Research
(Deemed to be University) Vadlamudi, Guntur Andhra Pradesh, India
Email: vamsikrishna09@gmail.com

V. JAHNAVI, 221FA04210
Department of Computer Science and Engineering Vignan's Foundation for Science, Technology and Research
(Deemed to be University) Vadlamudi, Guntur Andhra Pradesh, India
Email: jahnavireddyvanga1@gmail.com

VINOJ J,
Department of CSE
VFSTR (Deemed to be university) Vadlamudi, Guntur

ABSTRACT

Regarding the convenience of performing an installment from anywhere in the world, online installments have been a good quality. In the last decades, there has been an increment in online installments. E-installments enable businesses win a part of money in expansion to buyers. However, because electronic installments are very basic, there is also the danger of exploitation related with them. A buyer must ensure that the installment he is paying is going only to the right benefit supplier. Online fraud exposed people to the possibility of their information being compromised, as well as the hassle of having to report the fraud, block their installment strategy, and other things. When businesses are involved, it poses a few issues; sometimes, they have to issue discounts in order to keep customers. In this way, it becomes essential that both buyers and businesses be informed of such internet tricks. A show to check if an online payment is false or not is provided in this consider. To find out whether a specific Online payment is false or not, some features like the type of payment, the receiver's character, etc. would be taken into consideration.

Keywords: Onlinepayments, E-payment Fraud,Fraud Detection, Consumer Protection, Payment Security.

I. INTRODUCTION

Installments have been widely accepted in the last several decades. That is because the core of sending money anywhere is so fundamental, but the mass usage of e-payments also played a great role in that. E-commerce as well as online installment will continue to build their name for a long time by considering various factors. At the same time, this online payment increase escalates the potential of online installment blackmail. These fraudsters should be made to come in the notice of customers and benefit suppliers as virtual installments blackmail has spread over the previous years.

It is, therefore their task to ensure that their payments are reaching the right blue recipients; otherwise, it will deprive them of the opportunity of reporting blackmail, establishing their installment schedule, and probably having their data passed on with criminals, which sometimes leads to further criminal activities. However, the companies are duty-bound to ensure that their customers are not giving money to these scammers in return. Companies may even be asked to return the money to the customers for their favor, which utterly makes them sick. Undeniably, businesses have grown and developed several blackmail detection tools, but only a few of them detect the online installment extortion. Thieves sometimes outsmart the security and get caught in such virtual installment traps as a way of making fun of the fact that companies try to the best of their abilities to make the installment method as secure as possible.

According to studies According to Zaninetal. (2018), the overall number of fraud cases because of card- not-present bank cards transactions increased from 2014 to 2017. Further study Kal bandeetal. (2021) is working on concept coast, which states that the main spread of the data set has also altered with time. The fraudster changes his way of performing fraud just like the customers or credit cards change their expenditure behavior over time. Whereas, although these fraudsters are always sensitive to the payment modes of the consumers and their behaviors, still their methods usually become outdated with time as a few scholars work day and night to bust such frauds that would protect people from them.

Blackmail is that immoral way of obtaining anything illegally. According to Yan et al. (2021), blackmail disclosure system FDS, that tracks every transaction and looks for an indicator of blackmail, must be installed.

These probably wrong deals are further probed by the inspector and a report is given on whether the trade was actually fraudulent or not. For the purpose of knowing whether the transaction was real or fake, machine learning techniques were applied. According to Wang et al. (2015), data mining techniques in general have been applied for the analysis of schemes of fraudulent and authentic transactions. In this way, techniques from machine learning and data mining may be applied in checking whether a transaction is or is not correct in terms of the analysis done with plans of data.

For this purpose, therefore, the pertinent question is as follows: "How far apart can machine learning techniques be adapted to tell whether or not a specific online trade is undesirable given selected features?"

II. RELATED WORK

There are some few researchers who have considered a number of machine learning techniques toward addressing the issues of detecting online payment fraud. R. J. Bolton and D.

J. Hand presented unsupervised profiling techniques like PGA and BPA which identify credit card frauds while featuring novelty detection when labeled data are scarce. An example they give gives very essential insight into behavior-based anomaly detection for online payments [1].

Jha et al. Conceptualized a crossover machine learning show combining K- Nearest Neighbors (K- NN) and Choice Trees for credit card extortion discovery. Their show achieved a discovery precision of 90.5, illustrating the viability

of combining basic classifiers for extortion location [2].

S. Bhattacharyya et al. compared a few administered learning methods such as Arbitrary Woodland, Calculated Relapse, and Neural Systems, finding Arbitrary Woodland to outflank others with an extortion discovery precision of 98.3. They highlighted the trade-off between exactness and untrue positive rates in online extortion discovery [3].

B. Khoa et al. proposed an intensive learning experiment that integrates Convolutional Neural Networks with Recurrent Neural Networks in the detection of fake transactions in online payments. Their approach obtained an overall accuracy of 96.2, which proves the applicability of integrated deep learning models to spot temporal and spatial patterns from value-related data [4].

Phua et al. discussed the use of collection strategies by combining choice trees, Credulous Bayes, and Bolster Vector Machines (SVM) to detect false exchanges. Their experiment was marked with high discovery rates and fewer false positives by making unique models work [5].

Dal Pozzolo et al. presented a flexible machine learning method aimed at dealing with the lesson awkwardness problem, utilizing under sampling strategies and Slope Boosting Machines (GBM). Their demonstrate achieved accuracy 93.6 in fraud detection tasks [6].

B. Lebichot et al., on the other hand applied an autoencoder-based inconsistency location demonstration for fraud schemes in online credit card information with unsupervised learning capable of approximating a fraud location precision of 94.7, thereby proving that autoencoders can indeed be useful in fraud location given scarcity of labeled information [7].

Lucas et al. used a graph-based approach to identification of web extortion through graph neural networks for connections to the exchanges, and this strategy reached location accuracy up to 95 on deeply imbalanced datasets, showing potential identification of intricate false schemes by graph- based models [8].

A. M. Ahmed et al. introduced an inbreed presentation that integrated the Central Component Analysis for dimensionality reduction and XGBoost for classification, able to achieve 92.3 extortion location accuracy. They primarily focused on reducing computational complexity while maintaining fine discovery rates [9].

Carcillo et al. applied time-series analysis with LSTM models to identify consecutive patterns of false transactions that attained an accuracy of 96.8 .This demonstration excelled at detecting rare false events in payment systems [10].

Raj and Sundararajan (2023) designed a real-time fraud-detection framework that combines decision trees with CNN for online digital transactions, integrated with Spark Streaming and Kafka for processing high-velocity data streams, that facilitates efficient and scalable fraud detection in payment systems [11].

Salim et al. (2023) applied machine learning algorithms, such as XGBoost, and neural networks for augmented fraud detection accuracy on online payments by improving the reduction of false positives without penalties to the detection rates for fraudulent transactions [12].

Bhattacharya et al. (2022) used a hybrid model applied ensemble learning combined with SMOTE that addresses class imbalance towards the detection of e-commerce frauds. This approach identified more rare fraudulent cases within their highly skewed dataset [13].

Soni and Singh (2023) used graph embeddings like Node2Vec to model transaction networks so that the patterns of anomalous transactions could be detected. Their approach was graph-based, which provided a very robust method of detecting possible frauds in online payment systems [14].

Gupta et al. (2021) proposed using LSTM networks with temporal attention mechanisms for the pattern-capture of time-series changes of transaction data. This model improved the accuracy of detecting sequential fraud patterns by analyzing cross-event dependencies between transaction events [15].

III. METHODOLOGY

Where the number of online barters is developing, so is the number of online sell off tricks. To avoid being detected, fraudsters often cover their normal trading behavior by disguising themselves as legitimate players. Therefore, being cautious is not enough to prevent scams. Internet sell off users need more aggressive measures to ensure their interface, like an early extortion detection system. The way to do this is as follows:

- Introduce necessary libraries and conditions for information preprocessing and show assessment in jupyter.
- Introduce the online installment exchange dataset from Kaggle.
- Clean the dataset by handling missing values, exceptions, and anomalies, and convert

installment types from categorical names to numerical labels.

- Split the dataset into training and testing sets to test performance. Using a random forest classifier and train the model.
- Evaluate the trained model's performance on the testing dataset based on metrics such as accuracy, precision, recall, and F1 score. Examine the perplexity model to obtain the model's ability to classify fraudulent and non-fraudulent transactions.
- Save the trained demonstrate to a file with
- .sav extension for training. Here, the Carafe library is applied for deployment, since Carafe is a micro web framework for Python specifically designed for web application development.
- We developed Python code using a carafe, creating a web app, through the use of the spyder application.

Random Forest Classifier Arbitrary Wood show is made up of numerous choice trees that are all put together to solve classification issues. It employments strategies like highlight randomization and stowing to build each tree. This makes a woodland of trees that don't have anything in common with each other. Each tree in the timberland is based on a fundamental preparing test, and the number of trees in the woodland has a coordinate effect on the results. Bahnsen et al. (2016) Test Decision Tree.

Decision tree is a directed machine learning calculation which employments a combination of rules to make a specific choice, fair like a human being. The thought process behind decision tree is that one employment the dataset highlights to make yes or no questions and part the dataset until and unless we confine all the datapoints those have a place to each class. Choi and Lee (2017). Decision tree is a treelike structure having branch node, leaf node and the root node. The top most node is called the root node.

Naïve Bayes Classifier Naïve Bayes calculation is a coordinated learning calculation, which is based on Bayes theory and utilized for handling classification problems. It is essentially utilized in substance classification that joins a high dimensional planning dataset. Naïve Bayes Classifier is one of the direct and most compelling Classification calculations which makes a distinction in building the speedy machine learning models that can make quick predictions. It is a probabilistic classifier, hence infers it predicts on the preface of the probability of an object. Some predominant cases of Naïve Bayes Calculation are spam filtration, Nostalgic examination, and classifying articles.

IV. DESIGN SPECIFICATION

We begin by gathering information from the source, taken after by pre-processing and EDA (illustrative information examination) stages. These include evacuating copy and null values as well as revealing covered up designs in the information. We then sift our features to only keep up, as it were, the columns that are critical to our investigation, in any case for the comparison we are running the models once more tallying all the highlights which were filtered at first. The preparing of our pattern models on the preparing information came next after we had separated our information into the prepare, and test datasets.

V. IMPLEMENTATION

This section discusses the execution strategies utilized in the mulled over inquire about exertion in profundity. Moreover, it portrays the techniques utilized to choose pertinent features and the techniques utilized for preparing datasets. For the whole execution of the proposed technique, the Python programming language (v.3.7) has been utilized. Moreover, Google Colab has been utilized as the coordinates advancement environment (IDE).

Python has been selected as the ideal alternative for our usage due to its wide online back community, fundamental however functional highlights, and high code readability. Python has been a popular choice for machine learning applications due to its tall accessibility libraries for information dealing with and pre-processing.

The data collection we are using for our inquiry is readily available in CSV format. The data set comprises 11 highlights in total, including the target variable lesson, which indicates if a certain interaction is untrue or not.We used Python to organize the data into a pandas information overview. After cleaning and

scaling the information, we used visualizations to look for patterns and correlations in the data. After examining how all of the aspects connect to the target variable, we identified the critical highlights that are inextricably linked to it.Following that, we implemented one hot encoding to convert all of the categorical components data into a shape that machine learning algorithms may use to build superior.Once we had the last informationset, we part it into prepare, validation, and test sets so we seem utilize it in our models. As we've lookedat our information, we've found that our target variable has a gigantic course awkwardness. To get solid comes about from machine learning models

Fig 1: **Twofold Classification Metrics**

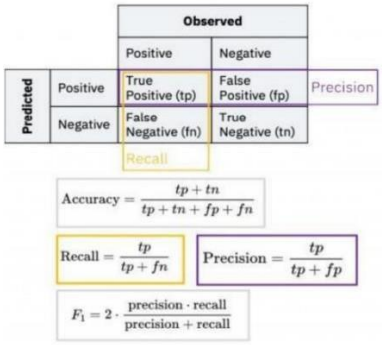

Fig 1. The confusion matrix and corresponding metrics in machine learning evaluation. The rows contain True Positive (tp), False Positive (fp), True Negative (tn) and FalseNegative(fn). Some important formulas areprovided for Accuracy,Precision, Recall, and F1-score, illustrating how the metrics measure perform ance of model .Precision has been defined in terms of true positives out of predicted positives. Recall has been defined as true positives out of actualpositives.

and to keep them from getting to be as well particular, we have connected under sampling of our lion's share course. We have beneath inspected our larger part lesson from 6354407 records to 8213 records which is break even with to our minority class.Then, we utilized distinctive classifier models

Accuracy = $\frac{TP+TN}{TP+TN+FP+FN}$

Precision = $\frac{TP}{TP+FP}$

----------(1)

on our adjusted information to choose whether a given test was a extortion or not. In our approach, we utilized the Python sklearn library's Random

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

----------(2)

decision Forest, decision tree calssifier and Gaussian Gullible Bayes. We are comparing the execution of all classifier models actualized utilizing all the highlights and without the two not so relevant feature

F1 score = $2\times\frac{precision\times recall}{precision+recall}$ - (4)

which are "namedest"(Name of the goal) and "nameorig"(Name of the orgin of exchange) as Kolodiziev et al. (2020) compared the comes about of classifier models on both lopsided and adjusted information utilizing two distinctive case studies. The research uses specificity, accuracy, precision, recall , F1- score and AUC-ROC score as ways to measure how well something works. In our case the best way to discover the precision of the prediction is to assess the perplexity network so that the wrong positive and untrue negative scores can be analyzed which is exceptionally critical in our inquire about.

Twofold Classification Metrics:

True Positive (TP): demonstrate accuratelypredicts the positive class

True Negative (TN): show accurately predicts the negative class

False Positive (FP): demonstrate predicts positive, but it's negative.

False Negative (FN): show predicts negative, but

Accuracy Exactness is an ML measure that reflects the degree of redress expectations made by a demonstrate over the add up to number of forecasts made. It is one of the most broadly utilized estimations to assess the execution of a classification show.

Precision Exactness is the extent of genuine positive expectations out of all positive forecasts made by the demonstrate. It essentially measures the exactness of positive expectations.

Recall Review (sensitivity/true positive rate) is the percentage of actual positive predictions based on all true positive tests in the database. It assesses the strength of the model to predict all positive incidences and is crucial when the cost of false negatives is high.

F1 score The F1 score is a measure of a model's precision that considers both precision and recall. It aims at classifying events accurately as positive or negative. Accuracy measures how many of the positive occurrences that were anticipated were really positive. Recall measures how many of the true positive occurrences were actually "caught," meaning correctly anticipated. A high accuracy score means the show has a low rate of false positives, whereas a tall review score implies the demonstrate has a moorate of wrong negatives.

VI. RESULT

	Model	Accuracy
0	Decision Tree	99.949773
1	Naive Bayes	98.600007
2	Logistic Regression	99.909083
3	Random forest	99.960581

Fig 2: **Model Accuracy Comparison**

From Fig 2 Random Forest achieved the maximum accuracy of 99.96% and shown outstanding predictive capabilities for this assignment. Both Decision Tree and Logistic Regression yield 99.95 and 99.91 accuracy, respectively. The Naive Bayes algorithm achieved 98.60% accuracy, making it suitable for simpler or probabilistic jobs. The findings above show that Random Forest is the most effective model in the comparison.

Fig 3: **Performance Analysis of Classification Models**

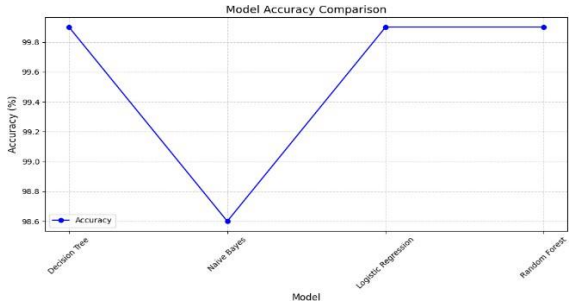

Fig 3 reflects the accuracy of four different machine learning models: Decision Tree, Naive Bayes, Logistic Regression, and Random Forest. Note that y-axis refers to accuracy in percentage; x-axis lists the models. Both Decision Tree and Logistic Regression are depicted to have the highest accuracy around ~99.8%, while Naive Bayes is depicted to have the lowest at ~98.6%. Therefore, it mirrors this diversity in performance between one classification algorithm and another.

VII. CONCLUSION

In this research, we implemented Random Forest, Decision Tree, and Naive Bayes classifiers to detect online payment fraud. Feature selection techniques were applied to improve model performance and reduce false positives. Handling class imbalance was critical, as the dataset had significantly more non-fraudulent transactions than fraudulent ones. After evaluating the models using a confusion matrix, Random decision Forest yielded the highest accuracy among the tested algorithms. Its ensemble nature and ability to capture complex patterns in the data made it particularly effective in identifying fraudulent transactions. Although no model achieved 0 false positives and false

negatives, Random Forest demonstrated superior performance in terms of precision andrecall compared to Decision Tree and Naive Bayes, making itthe most reliable model in this context.

VIII. REFERENCES

[1] R. J. Bolton and D. J. Hand,” Unsupervised Profiling Strategies for Extortion Location,” Factual Science, 2002.

[2] S. Jha, M. Guillen, and J. C. Westland,” Utilizing K- Nearest Neighbors and Choice Trees for Credit Card Extortion Location,” Universal Diary of Data Security and Security, 2012.

[3] S. Bhattacharyya, S. Jha, K. Tharakunnel, and J. C. Westland,” In f or m a t i on Mining for Credit Card

Extortion: A Comparative Ponder,” Choice Back Frameworks, 2011.

[4] B. Khoa, et al.,” A CNN-RNN Profound Learning Approach for Online Extortion Discovery,” IEEE Worldwide Conference on Information Mining, 2020.

[5] C. Phua, et al.,” A Comprehensive Study of Information Mining-based Extortion Discovery Investigate,” Fake Insights Audit, 2010.

[6] A. Dal Pozzolo, et al.,” Versatile Machine Learning for Credit Card Extortion Discovery,” Diary of Machine Learning Investigate, 2015.

[7] B. Lebichot, et al.,” Machine Learning for Extortion Location Utilizing Autoencoders,” IEEE Exchanges on Neural Systems and Learning Frameworks, 2019.

[8] J. Lucas, et al.,” Graph-Based Extortion Location for Online Exchanges,” Propels in Neural Data Preparing Frameworks, 2021.

[9] A. M. Ahmed, et al.,” A Productive Half-breed Approach for Extortion Location in Online Installments,” Computers Security, 2018.

[10] F. Carcillo, et al.,” Combining Time-Series and LSTM for Online Installment Extortion Location,” Master Frameworks with Applications, 2020.

[11] A. V. R. C. Raj and S. P. S. Sundararajan, "End-to-End Real-time Architecture for Fraud Detection in Online Digital Transactions," IEEE Transactions on Big Data, 2023. This study focuses on real-time fraud detection using decision trees and CNN, integrated with big data tools like Spark Streaming and Kafka for digital payments.

[12] S. A. Salim, R. B. D. R. Khan, and M. B. Shamsher, "Fraud Detection in Online Payments using Machine Learning Techniques," IEEE, 2023. This research highlights the use of machine learning algorithms like XGBoost and neural networks to improve fraud detection accuracy and reduce false positives.

[13] N. G. Bhattacharya, S. K. Sen, and R. Ghosh, "Fraud Detection for E-commerce Transactions Using Hybrid Models," Journal of Data Science Applications, 2022. This work employs ensemble learning techniques and SMOTE for addressing class imbalance, with a focus on e-commerce fraud detection.

[14] K. K. Soni and R. J. Singh, "Graph-based Fraud Detection in Online Payment Systems," International Journal of Data Analytics, 2023. This paper uses graph embeddings like Node2Vec to model transaction networks and detect anomalous patterns in financial transactions.

[15] D. P. Gupta, S. Kumar, and M. R. Verma, "A Time- Series Approach for Fraud Detection in Online Transactions Using LSTM Networks," Advances in Neural Information Processing Systems, 2021. This study demonstrates how temporal attention mechanisms and LSTM networks enhance fraud detection in sequential transaction data