JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Implementation Paper on UPI Fraud Detection using Machine Learning

[1] Miss. Sayalee S. Bodade, [2] Prof. P.P. Pawade

[1] PG Scholar, [2] Professor

[12] Computer Science & Engineering

[12] P. R. Pote (Patil) College of Engineering & Management,

Amravati, Maharashtra, INDIA

Abstract:-

The UPI fraud detection system are to enhance the security and reliability of digital payment transactions, ultimately safeguarding users from fraudulent activities. Firstly, the paper aims to employ advanced machine learning algorithms and data analytics to analyze transaction patterns and detect anomalies that may indicate potential fraud. Secondly, it seeks to develop a robust system that can identify and mitigate various types of UPI fraud, including phishing, identity theft, and unauthorized transactions. The paper also aims to create a real-time monitoring mechanism to promptly identify suspicious activities and trigger alerts for immediate intervention.

The scope of developing a UPI fraud detection system is vast and holds significant potential in addressing the emerging challenges in the digital payment landscape. Firstly, the paper encompasses the implementation of cutting-edge technologies such as machine learning, artificial intelligence, and data analytics to create a sophisticated fraud detection model. This model will have the capability to analyze massive datasets of UPI transactions in real-time, identifying patterns, anomalies, and trends associated with fraudulent activities.

Keywords:-

Clustering Algorithms, Taxonomy of Clustering Algorithms, Challenges in Clustering Algorithms

I .Introduction

This introduction will provide an overview of the key components and challenges involved in UPI fraud detection using machine learning, highlighting the importance of staying ahead in the ongoing battle against financial fraud in the digital age. With the increasing popularity of digital payment systems like UPI (Unified Payments Interface), there is a growing concern about fraud in these platforms. This paper aims to develop a robust fraud detection system for UPI transactions using machine learning techniques. UPI fraud detection using machine learning is a proactive approach to safeguarding financial transactions by leveraging the power of artificial intelligence. Machine learning algorithms analyze vast volumes of transaction data, patterns, and user behaviors to identify and prevent fraudulent activities in real-time. This technology holds the potential to minimize financial losses, protect user privacy, and enhance the overall security of digital payment ecosystems.

In this era of constant technological evolution, it is crucial for financial institutions, finch companies, and payment service providers to implement advanced machine learning models and algorithms to stay ahead of fraudsters. This approach not only helps in detecting known fraud patterns but also adapts to emerging threats through continuous learning and optimization. The project focuses on the development of a machine learning model that can analyze UPI transaction data in real-time to identify fraudulent activities. The primary objective is to create a system that enhances the security of UPI transactions and reduces financial losses due to fraud.

II. Literature Survey

In fraud detection, we often deal with highly imbalanced datasets. For the chosen dataset (Paysim), we show that our proposed approaches are able to detect fraud transactions with very high accuracy and low false positives – especially for TRANSFER transactions. Fraud detection often involves a tradeoff between correctly detecting fraudulent samples and not misclassifying many non-fraud samples. This is often a design choice/business decision which every digital payments company needs to make. We've dealt with this problem by proposing our class weight based approach. We can further improve our techniques by using algorithms like Decision trees to leverage categorical features associated with accounts/users in Paysim dataset. Paysim dataset can also be interpreted as time series. We can leverage this property to build time series based models using algorithms like CNN. Our current approach deals with entire set of transactions as a whole to train our models. We can create user specific models - which are based on user's previous transactional behavior - and use them to further improve our decision making process. All of these, we believe, can be Very effective in improving our classification quality on this dataset **[1]**

Now a days Digital transactions are rapidly increasing as it results in increasing online

Payment frauds too. In fact, according to the Reserve Bank of India, comparing March 2022 to March 2019, digital payments have risen in volume and value by 216% and 10%, respectively. People are starting to go all-in with digital transactions, but one can't deny the security issues that loom, and know-how when it comes to online payments. Few years ago, we could have barely seen the online payment, but today UPI payment QR code installed at doorstep. This invited the hoaxers and attackers to develop fraudulent transactions and fool people for some amount of money. Fortunately, the online transactions are monitored and hence could be analyses using the latest tools. In this system, an attempt is made to develop a machine learning model to identify fraudulent transactions in a transaction's dataset. **[2]**

Fraud detection for credit/debit card, loan defaulters and similar types is achievable with the assistance of Machine Learning (ML) algorithms as they are well capable of learning from previous fraud trends or historical data and spot them in current or future transactions. Fraudulent cases are scant in the comparison of non-fraudulent observations, almost in all the datasets. In such cases detecting fraudulent transaction are quite difficult. The most effective way to pre-vent loan default is to identify non-performing loans as soon as possible. Machine learning algorithms are coming into sight as adept at handling such data with enough computing influence. In this paper, the rendering of different machine learning algorithms such as Decision Tree, Random Forest, linear regression, and Gradient Boosting method are compared for detection and prediction of fraud cases using loan fraudulent manifestations. Further model accuracy metric have been performed with confusion matrix and calculation of accuracy, precision, recall and F-1 score along with Receiver Operating Characteristic (ROC) curves **[3]**

Financial fraud, considered as deceptive tactics for gaining financial benefits, has recently become a widespread menace in companies and organizations. Conventional techniques such as manual verifications and inspections are imprecise, costly, and time consuming for identifying such fraudulent activities. With the advent of artificial intelligence, machine-learning-based approaches can be used intelligently to detect fraudulent transactions by analyzing a large number of financial data. Therefore, this paper attempts to present a systematic literature review (SLR) that systematically reviews and synthesizes the existing literature on machine learning (ML)-based fraud detection. Particularly, the review employed the Kitchenhand approach, which uses well-defined protocols to extract and synthesize the relevant articles; it then report the obtained results. Based on the specified search strategies from popular electronic database libraries, several studies have been gathered. After inclusion/exclusion criteria, 93 articles were chosen, synthesized, and analyzed. The review summarizes popular ML techniques used for fraud detection, the most popular fraud type, and evaluation metrics. The reviewed articles showed that support vector machine (SVM) and artificial neural network (ANN) are popular ML algorithms used for fraud detection, and credit card fraud is the most popular fraud type addressed using ML techniques.

The paper finally presents main issues, gaps, and limitations in financial fraud detection areas and suggests possible areas for future research. **[4]**

III. System Diagram

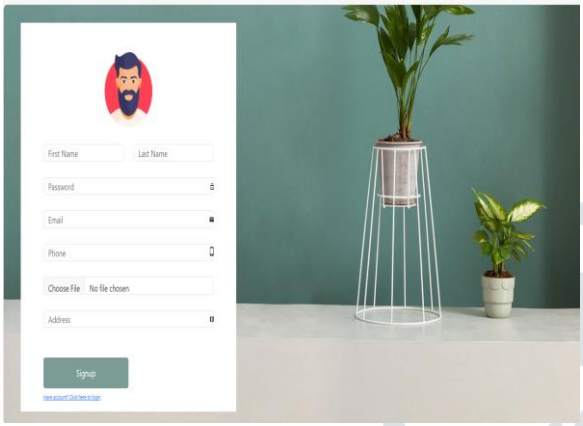

Fig: Home page

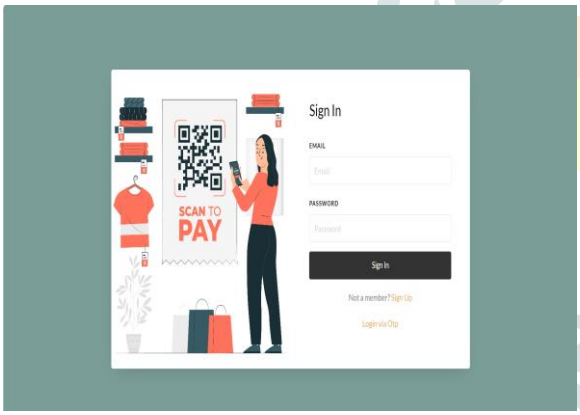

Fig: Sign-Up Page

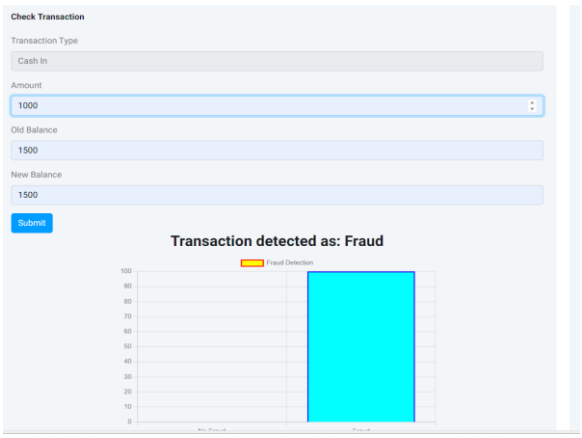

Fig: Fraud Detection

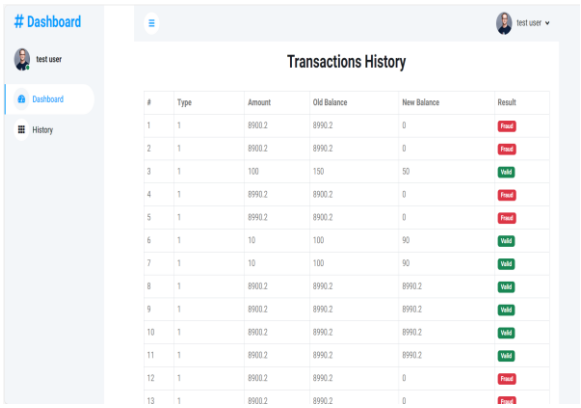

Fig: Transaction History

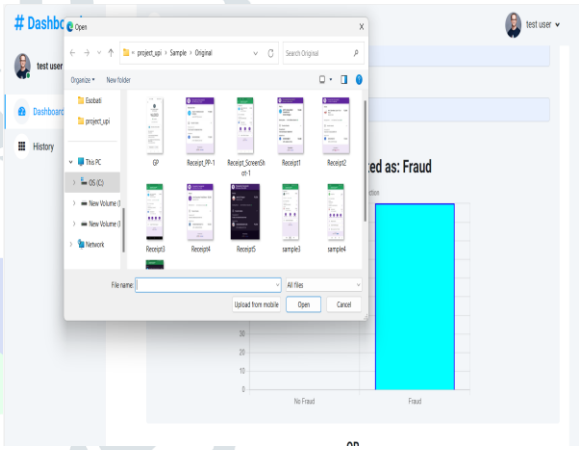

Fig: Payment Receipt Upload

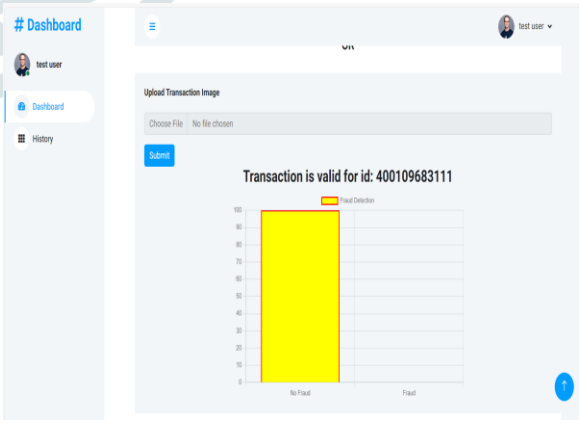

Fig: Results for Transaction Receipt

IV. Working Methodology

Data Cleaning: Some preprocessing of the data was necessary. Our chosen method could not handle all comments from the datasets without failing. Since the data files were read line by line, newlines () within the comments had to be removed. Certain emoji's couldn't be properly encoded in our chosen file format (UTF8) so those emoji characters had to be deleted. This did not affect the results whatsoever since the word preprocessing and tokenization we implemented through Scikit-learn (Count Vectorizer) only considers alphanumeric characters for words with the parameters we used [39]. Regex and character replacing were used to make all datasets adhere to the same format.

Training: All classifiers were trained on the training datasets with a test train split of 80/20 percent. This enabled us to see the accuracy of the classifiers on the training datasets. The same random state was used between the classifiers to make sure that the training is reproducible between the classifiers. Text feature extraction was done using the bag-of-words model using the Count Vectorizer in Scikit-learn. As mentioned in section 2.5 Sentiment Analysis, this a popular approach to feature extraction.

Classifiers: All used classifiers were used with the standard parameters in Scikit-learn except for logistic regression where the max parameter was increased from the default value of 100 to 1000. This was done since the logistic regression classifier reached the maximum allowed iterations before the optimal solution to the classifying problem was found. Classifiers were selected based on what is suitable for text and social media sentiment analysis and what has been used in previous work in the field. Naive Bayes classifiers such as multinomial and complement naive Bayes are common for use in text classification due to being fast and simple to implement [18]. Stochastic gradient descent classifier was recommended for use on tweets by Bifet and Frank [32]. Since YouTube comments are also part of social media and tend to be of short length, like tweets, we believe this to be appropriate for this study. Support vector machines are used since they are effective at a variety of traditional text categorization tasks and generally outperform naive Bayes classifiers [18], [40]. Logistic regression is another classifier commonly used in sentiment analysis [41]. The International Workshop on Semantic Evaluation (SemEval) had between 2013 - 2018 a task about sentiment analysis on Twitter. Several years this task included variations of classifying the tweet on a scale from positive or negative. SVM- and logistic regression-based classifiers were used by several teams attempting the task of classifying tweets on a scale from positive to negative [42].

Prediction: Four formulas for making the prediction were tested. This will be explained below. Prediction 1 / the base prediction assumes that only the number of comments classified as positive and negative contributes to the like proportion. The formula for the base prediction is given below: predicted like proportion = Npositive Npositive + Nnegative where Npositive & Nnegative are the number of comments classified as positive and negative respectively. A consequence of this formula for the base prediction is that the videos whose comments are only labeled as neutral had to be excluded since the denominator

would be 0. This causes the size of the testing dataset to vary by small amounts between the classifiers for the base prediction. The following three predictions consider neutral comments to some extent. Any factor for the neutral comments could be used in the numerator of the predicted like proportion but we have only considered those cases we believe make reasonable assumptions. Prediction 2 assumes that all comments labeled as neutral contribute to dislikes. The predicted like proportion for prediction 2 is given below: predicted like proportion = Npositive Npositive + Nneutral + Nnegative where Npositive, Nneutral &Nnegative are the number of comments classified as positive, neutral and negative respectively. Prediction 3 assumes that half of the neutral comments contribute to likes and that half of the neutral comments contribute to dislikes. The predicted like proportion for prediction 3 is given below: predicted like proportion = Npositive + 0.5 · Nneutral Npositive + Nneutral + Nnegative where Npositive, Nneutral &Nnegative are the number of comments classified as positive, neutral and negative respectively. Prediction 4 assumes that all neutral comments contribute to likes. The formula is given below: predicted like proportion = Npositive + Nneutral Npositive + Nneutral + Nnegative where Npositive, Neutral &Negative are the number of comments classified as positive, neutral and negative respectively.

Evaluation: The accuracy of all classifiers on the training dataset was calculated. Knowing the actual and predicted like proportions on the YouTube trending dataset, the Pearson correlation, the p-value for the Pearson correlation, mean absolute error, and standard deviation of differences were calculated. This way the performance of the four different predictions and using all configurations of classifiers and training datasets could be compared

Result Interpretation

Result analysis is a critical phase in building a UPI fraud detection system as it assesses the effectiveness and performance of the implemented solution.

Accuracy Assessment:

Evaluate the overall accuracy of the UPI fraud detection system by comparing the total number of correctly identified fraudulent and non-fraudulent transactions against the total number of transactions processed. This provides a high-level understanding of the system's efficacy.

Precision and Recall:

Calculate precision and recall to understand the trade-off between false positives and false negatives. Precision measures the accuracy of positive predictions, while recall measures the system's ability to capture all actual positives. Striking a balance between these metrics is crucial for a reliable fraud detection system.

False Positive Rate:

Analyze the false positive rate, which indicates the proportion of legitimate transactions incorrectly flagged as fraudulent. A low false positive rate is essential to minimize disruptions for genuine users while maintaining effective fraud detection.

Receiver Operating Characteristic (ROC) Curve:

Plot an ROC curve to visualize the trade-off between true positive rate and false positive rate at various thresholds. The area under the ROC curve (AUC) provides a comprehensive measure of the model's performance, with a higher AUC indicating better overall performance.

Confusion Matrix Analysis:

Break down the results using a confusion matrix to understand the number of true positives, true negatives, false positives, and false negatives. This detailed analysis helps in identifying specific areas for improvement and fine-tuning the model.

V. Conclusion

As we progress into an increasingly digitized world, the importance of securing digital payment systems cannot be overstated. The implementation paper on UPI fraud detection serves as a proactive measure to mitigate risks, protect users, and foster the widespread adoption of digital transactions. Hence, we concluded UPI fraud detection using machine learniing which is current landscape demands innovative solutions, and the development of a UPI fraud detection system aligns with the imperative to create a secure and trustworthy environment for financial transactions

VI. Acknowledgement

First and foremost, I would like to express my sincere gratitude to my **Prof. P. P. Pawade** who has in the literal sense, guided and supervised me. I am indebted with a deep sense of gratitude for the constant inspiration and valuable guidance throughout the work

Reference

[1] Aditya Oza “Fraud Detection using Machine Learning” - https://github.com/aadityaoza/CS-229-project.

[2] Ms. Kishori Dhanaji Kadam, Ms. Mrunal Rajesh Omanna, Ms. Sakshi Sunil Neje, Ms. Shraddha Suresh Nandai. “Online Transactions Fraud Detection using Machine Learning” Volume 5, Issue 6 June 2023, pp: 545-548 www.ijaem.net

[3] M. Valavan and S. Rita “Predictive-Analysis-based Machine Learning Model for Fraud Detection withBoosting Classifiers” Computer Systems Science & Engineerin

[4] Abdulalem Ali 1,,Shukor Abd Razak 1,2,ORCID,Siti Hajar Othman 1ORCID,Taiseer Abdalla Elfadil Eisa 3,Arafat Al-Dhaqm 1,ORCID,Maged Nasser 4ORCID,Tusneem Elhassan 1,Hashim Elshafie 5 andAbdu Saif 6ORCID “Financial Fraud Detection Based on Machine Learning: A Systematic Literature Review” **https://doi.org/10.3390/app12199637**.

[**5].** Jain AK, Murty MN, Flynn PJ (1999) Data clustering: a review. ACM Comput Surv (CSUR) 31(3):264–323.

[**6].** Roberts SJ (1997) Parametric and non-parametric unsupervised cluster analysis. Pattern Recognit 30(2):261–272.

[7]. Gan G, Ma C, Wu J (2007) Data clustering: theory, algorithms, and applications, vol 20. Siam, Philadelphia.

[8]. Madhulatha TS (2012) An overview on clustering methods. arXiv preprint arXiv:1205.1117.

[**9].** Pearson K (1894) Contributions to the mathematical theory of evolution. Philos Trans R Soc Lond A 185:71–110