iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** XII **Month of publication:** December 2023

DOI: https://doi.org/10.22214/ijraset.2023.57551

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue XII Dec 2023- Available at www.ijraset.com

Review Paper on UPI Fraud Detection Using Machine Learning

Miss. Sayalee S. Bodade[1], Prof. P.P. Pawade[2]
[1]*UG Scholar,* [2] *Professor, Computer Science & Engineering, P. R. Pote (Patil) College of Engineering & Management, Amravati, Maharashtra, INDIA*

Abstract: ***With the rapid growth of digital transactions, the Unified Payments Interface (UPI) has emerged as a popular and convenient method for financial transactions in the modern era. However, the increasing reliance on digital platforms has also led to a rise in fraudulent activities. This paper proposes a robust UPI fraud detection system employing advanced machine learning techniques to enhance the security of digital transactions. The proposed system leverages a diverse set of features, including transactional patterns, user behaviour, and device information, to create a comprehensive model for fraud detection. Machine learning algorithms, such as supervised learning classifiers and anomaly detection techniques, are employed to analyse historical transaction data and identify patterns indicative of fraudulent activities. The model is trained on a labelled dataset that includes both genuine and fraudulent transactions, ensuring its ability to distinguish between normal and suspicious behaviour***
Keywords: Transaction, Payment, UPI, Attackers, Fraudulent, Hoaxers, Money, Dataset. Random forest; decision tree; logistic regression; machine Learning; gradient boosting method; confusion matrix

I. INTRODUCTION

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. 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 project aims to develop a robust fraud detection system for UPI transactions using machine learning techniques. 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 payment 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

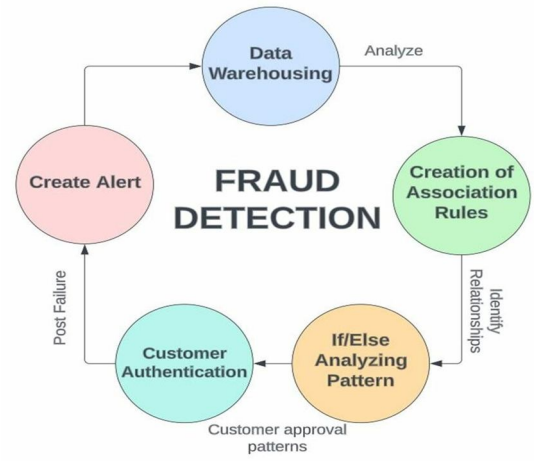


Fig: System Diagram for UPI fraud Detection using machine learning

IV. CONCLUSION

In this paper we conclude machine learning techniques for UPI fraud detection proves to be a robust and effective solution in enhancing the security and reliability of digital payment systems. The utilization of advanced algorithms, such as anomaly detection and pattern recognition, empowers financial institutions and service providers to stay one step ahead of fraudulent activities. Through continuous learning and adaptation, machine learning models can evolve to recognize emerging patterns and tactics employed by fraudsters, thereby minimizing false positives and improving the overall accuracy of fraud detection systems.

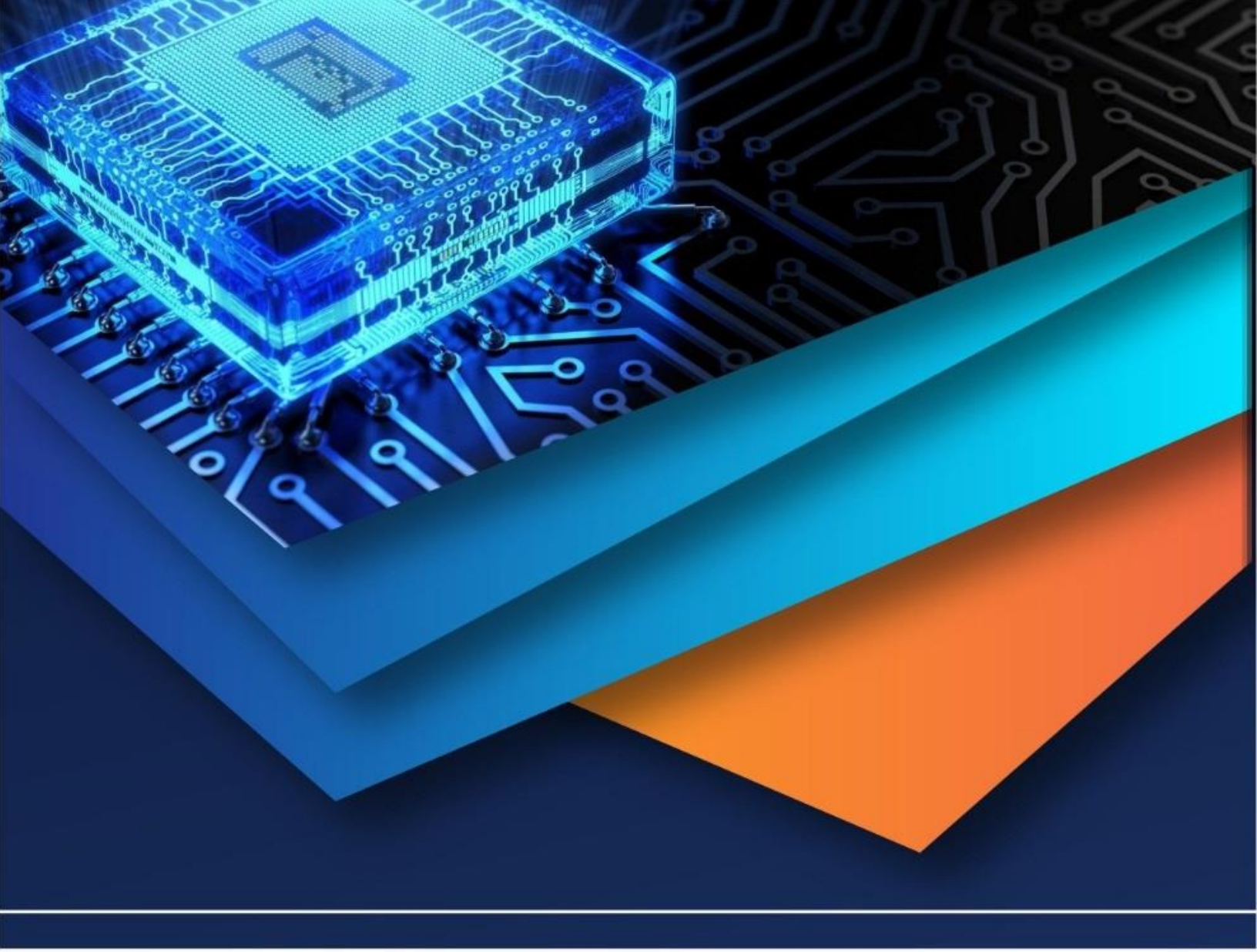
The ability to analyze vast amounts of transactional data in real-time enables swift identification of suspicious activities, preventing unauthorized access and ensuring the integrity of UPI transactions.

V. 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

REFERENCES

[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] PayPal Inc. Quarterly results https://www.paypal.com/stories/us/paypalreports-third-quarter-2018-results
[6] A Model for Rule Based Fraud Detection in Telecommunications - Rajani, Padmavathamma - IJERT – 2012
[7] HTTP Attack detection using n−gram analysis - A. Oza, R.Low, M.Stamp - Computers and Security Journal - September 2014
[8] Scikit learn - machine learning library http://scikit-learn.org
[9] Paysim - Synthetic Financial Datasets for Fraud Detection https://www.kaggle.com/ntnu-testimon/paysim1



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY