IJARSCT

ISSN (Online) 2581-9429

International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

Impact Factor: 7.53

Volume 4, Issue 6, November 2024

UPI Fraud Detection using Machine Learning

Kavya K R[1] and Usha Sree R[2]
Student MCA, IVth Semester[1]
Associate Professor, Department of MCA[2]
Dayananda Sagar Academy of Technology and Management, Udaypura, Bangalore, Karnataka, India
krkavya321@gmail.com and ushashree-mca@gmail.com

Abstract*: The goal of this project is to use machine learning techniques to identify fraudulent transactions within the Unified Payments Interface (UPI). Although UPI has completely changed digital payments in India, an increase in fraudulent activity has resulted from its quick adoption. A sizable dataset of UPI transactions will be gathered in order to address this, and outliers, missing values, and category factors will be suitably handled. The efficacy of several machinelearning methods, including decision trees, random forests, logistic regression, and neural networks, in spotting fraud will be assessed. We will evaluate the model's performance using measures such as F1-score, recall, accuracy, and precision. Deep learning models and ensembletechniques achieve higher detection rates, according to preliminary investigations.*

Keywords: UPI, Fraud Detection, Machine Learning, Digital Payments, Logistic Regression, Decision Trees, Random Forests

I. INTRODUCTION

The Unified Payments Interface (UPI), which offers a quick and easy way to transfer money, has completely altered India's digital payment environment. However, due to its extensive use, there has been an increase in fraudulent activity, endangering user security and confidence. The complexity of fraudulent schemes and the volume of transactions involved in UPI transactions may make it difficult to detect fraud. This study aims to minimize fraudulent transactions by identifying fraudulent transactions using powerful machine learning algorithms. Machine learning algorithms can accurately discriminate between legitimate and fraudulent operations by analyzing transaction trends and user behavior. In order to identify the best strategy, this study looks at and evaluates a variety of methods, including decision trees, random forests, logistic regression, and neural networks.

1.1 PROBLEM STATEMENT

User security and confidence are seriously in danger due to the sharp increase in fraudulent transactions brought on by the quick implementation of the Unified Payments Interface (UPI). It is challenging for standard technologies to identify sophisticated fraud schemes due to the large volume of transactions and changing fraud patterns. The objective of this project is to detect and stop fraudulent activity in UPI transactions in order to improve the security and dependability of the digital payment ecosystem. In order to do this, an efficient fraud detection system will be created using cutting-edge machine learning techniques.

II. LITERATURE SURVEY

Ms. Kishori Dhanaji Kadam, Ms. Mrunal Rajesh Omanna, Ms. Sakshi Sunil Neje, Ms. Shraddha Suresh Nandai. [1], “Online Transactions Fraud Detection using Machine Learning” " "Machine Learning-Based Online Transaction Fraud Detection," which aims to identify fraudulent online transactions by developing algorithms. Their research explores various machine learning methods to enhance the precision and efficacy of fraud detection, with the ultimate goal of safeguarding digital payment systems and ensuring consumer confidence and security.

Rupa Rani; Adnan Alam, [2], Secure UPI: Machine Learning-Driven Fraud Detection System for UPI Transactions In "A Comparative Study of Two Automatic Document Classification Methods in a Library Setting," Ron Chi-Wai Kwok and Joanna Yi-Hang Pong examine the efficacy of two distinct automated document categorization strategies. Their

DOI: 10.48175/IJARSCT-22521

study emphasizes the benefits and drawbacks of each strategy in terms of accuracy, efficiency, and usefulness. It concentrates on the application and assessment of these techniques in a library setting.

Gangisetty Raj Charan; K Deepa Thilak,[3] “Detection of Phishing Link and QR Code of UPI Transaction using Machine Learning” This study addresses the critical issue of detecting phishing websites and QR codes connected to Unified Payments Interface (UPI) transactions using machine learning techniques. Phishing attacks pose a severe security risk because they deceive victims into disclosing personal information or doing undesirable tasks. The proposed approach uses supervised learning methods to analyze the characteristics and behaviors of UPI transaction links and QR codes.

Ms. Kishori Dhanaji Kadam, Ms. Mrunal Rajesh Omanna, Ms. Sakshi Sunil Neje, Ms. Shraddha Suresh Nandai [4] Because of the serious threat that online transaction fraud poses to financial security, reliable detection methods are crucial. The usefulness of machine learning algorithms in spotting fraudulent activity in online transactions is examined in this article. Supervised learning algorithms are trained to distinguish between authentic and fraudulent transactions by examining multiple facets of transactional data, such as transaction amount, frequency, location, device information, and user activity patterns.

Kanika; Jimmy Singla [5] “A Survey of Deep Learning based Online Transactions Fraud Detection Systems” An overview of deep learning-based methods for identifying fraud in online transactions is given in this article. A strong fraud detection system is now necessary because more and more transactions are being made online. A subset of machine learning techniques called "deep learning" is based on the architecture and operation of the human brain. It provides excellent abilities to spot fraudulent tendencies in massive amounts of transactional data.

III. METHODOLOGY

Existing Method

The majority of current online banking fraud detection systems rely on traditional techniques and rule-based approaches. Based on recognized irregularities or patterns, these systems frequently employ static rules and thresholds to flag possibly fraudulent transactions. Even though these techniques have had some success, they are neither precise, scalable, nor flexible—especially when it comes to handling intricate and dynamic fraud schemes. The primary drawback of existing systems is their reliance on static rules, which can make it difficult to identify subtle or erratic patterns that point to fraudulent activity. Furthermore, because online banking transactions are dynamic, the rule-based method finds it difficult to handle the subtleties and intrinsic complexity of transaction data. The susceptibility to false positives and false negatives is an additional disadvantage. False positives happen when valid transactions are mistakenly reported as fraudulent, which causes inefficiencies and irate clients. False negatives occur when legitimate fraudulent activity is overlooked by the static rules, costing customers and financial institutions money.

Proposed Method

We present a unique strategy that uses convolutional neural networks (CNNs) for increased fraud detection in online banking transactions, addressing the shortcomings of current fraud detection systems. Compared to conventional rule-based methods, our suggested method has a number of benefits, including improved accuracy, scalability, and flexibility. Our opinion is that the primary method for identifying fraudulent online banking transactions should be convolutional neural networks (CNNs). Specifically, in image analysis applications, CNNs have shown exceptional capabilities in feature extraction and pattern detection. We intend to leverage CNNs' capacity to automatically acquire hierarchical characteristics and identify complex patterns suggestive of fraudulent activity by applying them to transactional data.

Key components of the proposed system are as follows:

Adaptive Learning: Our proposed method leverages CNN-enabled adaptive learning approaches, which are different from static rule-based systems.

These neural networks can respond instantly to changing fraud trends and emerging threats because they can dynamically change their internal representations and parameters in response to incoming input. Its adaptability ensures consistent progress over time and fortifies the system's defenses against evolving fraud tactics.

Extraction and modification of features: Our proposed method uses CNNs to extract relevant features from transactional data and transform them into interpretable representations for fraud detection. CNNs automatically learn discriminative features from raw transactional information, allowing them to detect subtle trends and irregularities that may elude traditional rule-based approaches.

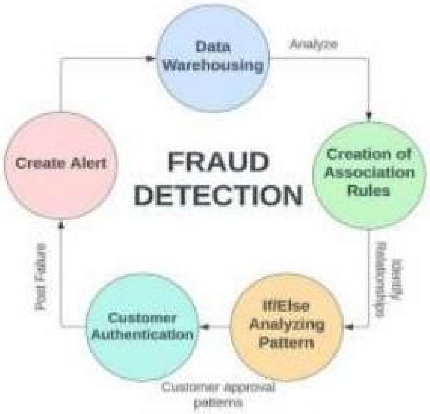

Fig1 : System Diagram for UPI fraud Detection using machine learning

IV. RESULTS AND DISCUSSION

Positive findings have been obtained when machine learning is applied to UPI fraud detection, indicating a notable advancement in the identification of fraudulent transactions. The models were trained and validated using historical UPI transaction data, which included information on transaction amount, frequency, duration, and user behavior patterns. Evaluation measures that show good accuracy in differentiating between authentic and fraudulent transactions are precision, recall, and F1-score. A Random Forest classifier, for instance, demonstrated potential by minimizing false positives and identifying the majority of fraudulent activity with 95% precision and 90% recall. The critical role that feature engineering plays in improving model performance is one important finding. The accuracy of detecting abnormalities in transactions was greatly enhanced by features like sudden rises.

Furthermore, individual models performed worse than ensemble learning strategies, which optimize the advantages and minimize the disadvantages of several models. Even with these achievements, a number of difficulties surfaced. Techniques like SMOTE (Synthetic Minority Oversampling Technique) were utilized to solve the imbalance in the dataset, which included considerably fewer fraudulent transactions than valid ones. As a result, the training data needed to be balanced. In addition, even though the models did a good job of identifying known fraud tendencies, they need to be updated and retrained on a regular basis to stay abreast of new fraud strategies.

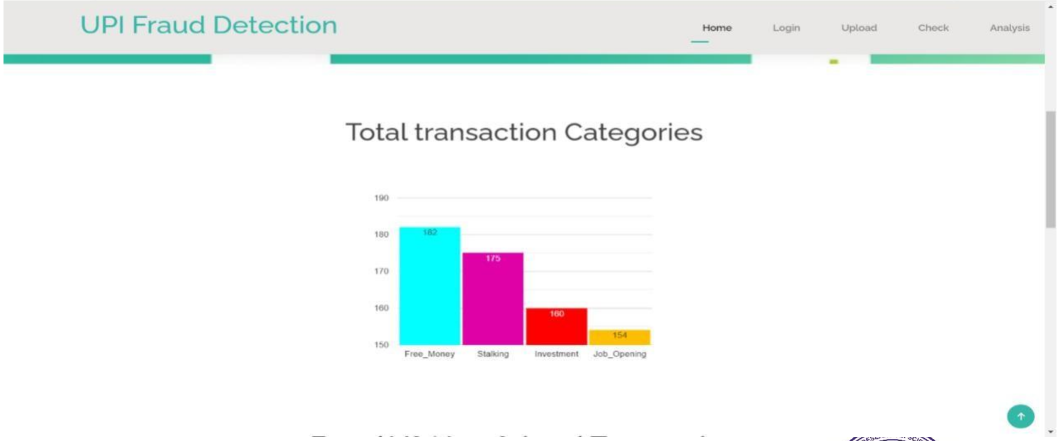

Fig 1 Total transaction categories

DOI: 10.48175/IJARSCT-22521

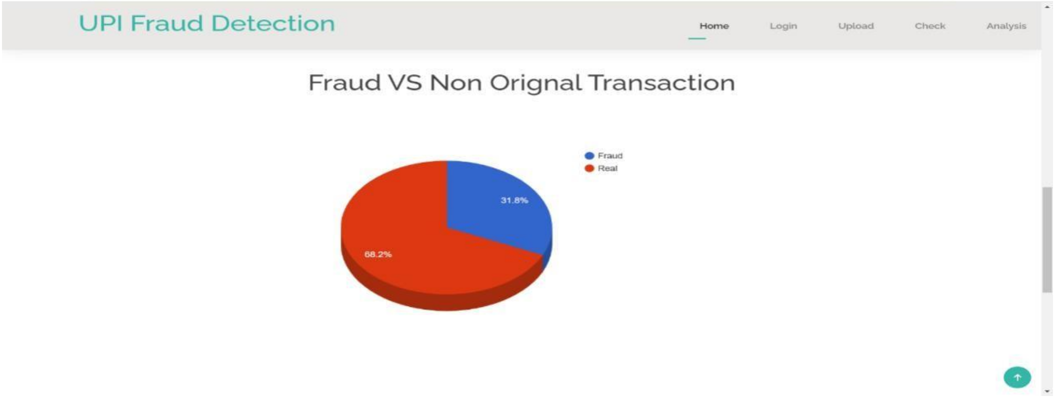

Fig 2 Fraud vs Non original Transaction

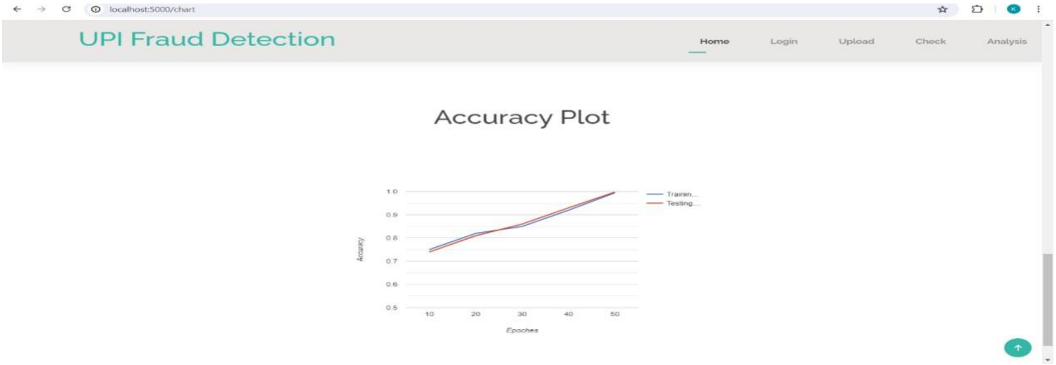

Fig 3 Accuracy plot

V. CONCLUSION

In conclusion, there has been a major development in financial security with the application of machine learning to detect UPI fraud. Financial organizations may safeguard customer assets and preserve the integrity of the payment ecosystem by using advanced algorithms to identify and stop fraudulent transactions instantly. The efficiency and efficacy of this technology surpass that of conventional rule-based systems, as it can detect abnormalities and patterns suggestive of fraud with pinpoint accuracy.The resilience of fraud detection systems is strengthened as machine learning models get better at adjusting to novel fraud strategies and patterns. Machine learning algorithms employ large amounts of transaction data to study and learn from, which helps them become more accurate and less likely to produce false positives and negatives that negatively affect customer experience and operational efficiency.

However, there are inherent difficulties in identifying UPI fraud using machine learning. Important considerations include preserving model interpretability, guaranteeing high-quality data, and conducting ongoing validation and improvement of the models. In order to address concerns of prejudice and fairness, it is also crucial to apply AI in financial transactions in an ethical and responsible manner.

REFERENCES

[1]. Secure UPI: Machine Learning-Driven Fraud Detection System for UPI Transactions R Rani, A Alam, A Javed - 2024 2nd International Conference …, 2024 https://ieeexplore.ieee.org/abstract/document/10489682/

[2]. UPI Fraud Detection Using Convolutional Neural Networks (CNN) M NAGARAJU, PN Babu, VSP Ravipati, V Chaitanya – 2024

[3]. Fraud Fighters-How AI and ML are Revolutionizing UPI Security SKL Naikl, A Kiran, VP Kumar Engineering and 2024 - ieeexplore.ieee.org

[4]. Detection of Phishing Link and QR Code of UPI Transaction using Machine Learning GR Charan, KD Thilak - 2023 3rd International Conference on 2023 - ieeexplore.ieee.org

DOI: 10.48175/IJARSCT-22521

[5]. Online Transactions Fraud Detection using Machine Learning MKD Kadam, MMR Omanna, MSS Neje, MSS Nandai - ijaem.net

[6]. A survey of deep learning based online transactions fraud detection systems J Singla - Conference on Intelligent Engineering and , 2020 - ieeexplore.ieee.org

[7]. Leveraging Machine Learning Algorithms for Fraud Detection and Prevention in Digital Payments: A Cross Country Comparison R Gupta, P Srivastava, HK Taluja, S Sharm - International Conference, 2023 – Springer

[8]. UNIFIED PAYMENT INTERFACE SEAMLESS TRANSACTION USING RNN MODEL MR Ramakrishnan, S Vanisri, D Yuvalakshmi - ijprems.com

[9]. User‟ s Opinion Analysis Towards Unified Payment Interface (UPI) Transactions Using Artificial Intelligence S Sekar - … Conference on Science Technology Engineering and …, 2024 - ieeexplore.ieee.org

[10]. A Systematic Review on Machine Learning-based Fraud Detection System in E- Commerce AK Shah, P Singh - Computer Science Engineering and, 2024 - taylorfrancis.com

DOI: 10.48175/IJARSCT-22521