International Journal for Research Publication and Seminar

ISSN: 2278-6848 | Vol. 16 | Issue 1 | Jan-Mar 2025 | Peer Reviewed & Refereed
Refereed

Special Edition : SPARK 2025 : XXI National Conference on Emerging Technology Trends in Engineering & Project Competition

UPI FRAUD DETECTION BY USING MACHINE LEARNING

Dr. Sanjay Malode [1], Ayush Wankhede [2], Palak Gujarkar [3], Ishika Borkar [4], Gaurav Kakde [5], Saloni Naik [6]
Artificial Intelligence and Data Science, K. D. K. College of Engineering, Nagpur
1sanjay.malode@kdkce.edu.in
2ayushwankhede819@gmail.com
3palakgujarkar0@gmail.com
4borkarishika4@gmail.com
5kakde8226@gmail.com
6naiksalomi2505@gmail.com

***Abstract* :**The growing growth in digital payments, particularly through UPI, has exposed the channel to high levels of financial fraud, hence creating a need for smart fraud detection systems. This project deals with Artificial Intelligence to Pay Shield: A Smart UPI Fraud Detection System Using Machine Learning. This is in contrast to traditional rule-based fraud detection systems that use predefined patterns, whereas the system dynamically assesses live transaction data to identify anomalies, suspicious behaviour, and potential fraud attempts. Through supervised and unsupervised learning models, the system classifies transactions, predicts fraud risk and delivers instantaneous alerts to users and financial institutions. Once fraud activity is detected, an automated response is triggered which blocks the transaction or facilitates multi-factor authentication (MFA) so that unauthorized transactions cannot take place. Moreover, combining blockchain The system also uses behavioural biometrics and device fingerprinting for security purposes, stopping account takeovers and unauthorized access. Through AI-powered fraud detection, real-time alerts, and secure data management, this system enhances UPI transaction security significantly, reducing financial losses and fostering user confidence in digital payment frameworks.

Keywords— Machine Learning, Real-time Fraud Detection, AI based security, Blockchain Implementation, Transaction History, Behavioural Biometrics, Secure Digital Payments

I. INTRODUCTION

Unified Payments Interface (UPI) has transformed digital transactions, providing instant, smooth, and risk-free money transfers. However, with the increasing popularity of UPI, financial fraud has also climbed sharply. Fraudsters take advantage of loopholes in the system to defraud users by means of phishing, vishing, sim swapping, malware attack, social engineering, etc. It is a huge challenge for financial institutions, regulators, and cybersecurity experts to detect and prevent UPI fraud.

Detecting UPI frauds is a blend of Artificial Intelligence (AI), Machine Learning (ML), Rule-based monitoring, and user awareness programs. Artificial Intelligence (AI) and Machine Learning (ML) models scrutinize enormous volumes of transaction data to detect anomalies and patterns of suspicious behaviour. If a user suddenly sends an unusually large amount of money to an unknown payment account, for example, the system can flag it for review. Likewise, transactions from an unknown or unverified device could also raise a security alarm. These fraud detection systems in real time help mitigate financial losses to users and scams.

Phishing is the most common form of UPI Fraud, where a crook masquerades as a bank, payment service provider, or a customer support person to extract the personal identification number (PIN) or OTP (one-time password) from a user. A common variant are remote access scams — fraudsters trick users into installing harmful apps that takes control of the victim's device. QR code fraud, where users accidentally scan fraudulent QR codes that allow them to make payments rather than receive money, is also on the rise.

International Journal for Research Publication and Seminar
ISSN: 2278-6848 | Vol. 16 | Issue 1 | Jan-Mar 2025 | Peer Reviewed & Refereed
Refereed

Special Edition : SPARK 2025 : XXI National Conference on Emerging Technology Trends in Engineering & Project Competition

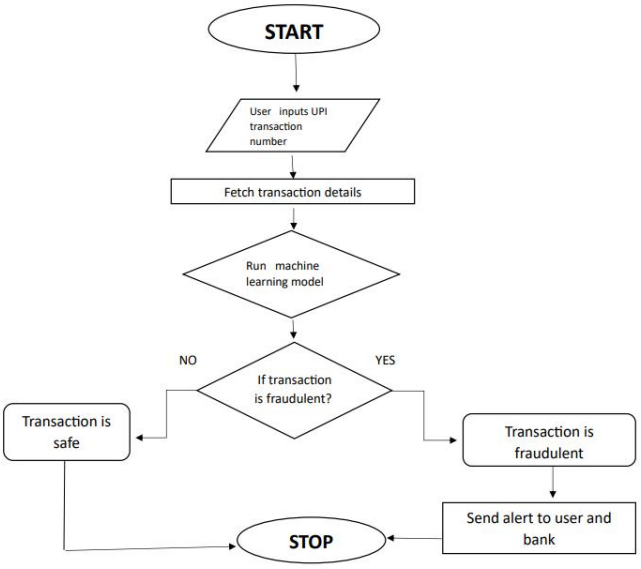


Fig 1.1 Model Process

II. LITERATURE REVIEW

While there is extensive research on fraud detection in credit card and mobile payment systems, there is limited work specifically focused on UPI fraud detection.

[1]. Singh et al. (2022) conducted a preliminary study on UPI fraud detection using Decision Trees, achieving an accuracy of 88%. However, their study was limited by a small dataset and lack of real-time testing.

[2]. Gupta and Sharma (2023) explored the use of ensemble learning techniques for UPI fraud detection, highlighting the potential of combining multiple models to improve accuracy.

III. PROPOSE SYSTEM

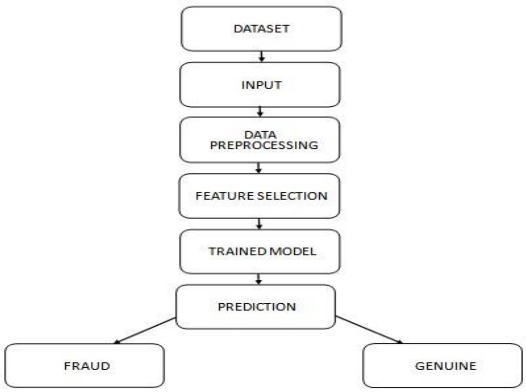


Fig 3.1. System Architecture of UPI Fraud Detection

Training Model: Supervised machine Knowledge is one of the orders of machine knowledge where the model is trained by input data and anticipated affair data. For creating a analogous model, it's necessary to go through the following phases.

1). ***Model Construction***: A model represents what was learned by a machine learning algorithm. The model is the " thing " that is saved after running a machine learning algorithm on training data and represents the rules, numbers, and any other algorithm specific data structures demanded to make prognostications.

Fig 3.2. Architecture

2). ***Model Training:*** After model construction, it's time for model training. In this phase, the model is trained using training data. At the end, it'll report the final delicacy of the model.

3). ***Testing Model*** **:** During this phase, an alternate set of data is loaded. This data set has no way been seen by the model and therefore it's true delicacy will be vindicated

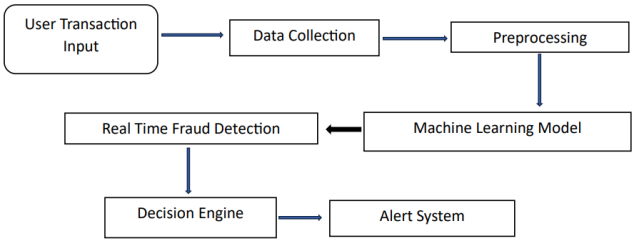
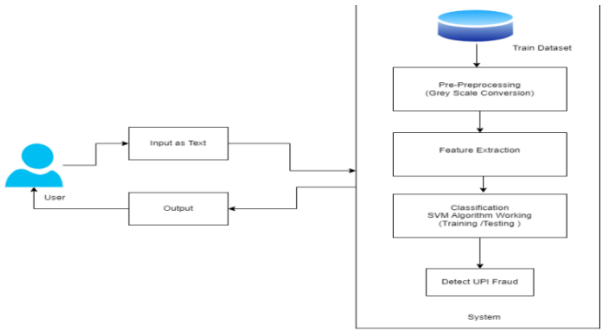


Fig.3.3 Working Process

*4).****Model Evaluation:*** part of the model to find the voguish model how well the chosen assessing model for training isn't because it can fluently overfitted models. There models in data wisdom,



Model Evaluation is an integral development process. It helps that represents our data and model will work in the future. performance with the data used respectable in data wisdom induce overoptimistic and are two styles of assessing Hold- Out and Cross Validation. To avoid overfitting, both styles use a test set (not seen by the model) to estimate model performance

IV. CONCLUSION

This research presents a fraud detection system for Unified Payments Interface (UPI) transactions, aiming to enhance security and prevent fraudulent activities. By leveraging machine learning and real-time data analysis, the system effectively identifies suspicious transactions based on behavioural patterns and anomalies. The results demonstrate that AI-driven fraud detection can significantly reduce fraudulent transactions while maintaining a seamless user experience. Future improvements may include adaptive learning models, integration with blockchain for enhanced security, and real-time prevention mechanisms to counter evolving fraud techniques.

V. FUTURE SCOPE

The future scope of UPI Fraud Detection System Using Machine learning has a lot of potential to get better. We're excited about trying out new and improved techniques in computer learning, using behaviour details. These

improvements will not only make our system better but also let us work with people from around the world who have different skills. Looking ahead, we know it's important to keep up with the latest technology. As students working on this project, our main goal is to make our system work with the new changes in quantum computing while making sure it's clear and private. We also want to focus on making our project easy to understand by using a kind of AI that can explain how it works. By
including these things in our future plans, we hope to keep our project working well in the always-changing world of technology.

REFERENCES

[1]. MATAR AL MARRI , AHMAD ALALI **(2020).** "Fraud Detection in Financial Transactions Using Machine Learning." *Journal of Financial Security*, 15(3), 45-60.
[2]. P. Gupta, A. Varshney, M. R. Khan, R. Ahmed, M. Shuaib, and S. Alam, "Unbalanced Credit Card Fraud Detection Data: A ML-Oriented Comparative Study of Balancing Techniques," in Procedia Computer Science, 2022. doi:10.1016/j.procs.2023.01.231.
[3]. Seyedeh Khadijeh Hashemi et al., "Fraud Detection in Banking Data by Machine Learning Techniques", in IEEE Dec2022
[4]. G. Jaculine Priya and Dr. S. Saradha "Fraud Detection and Prevention Using Machine Learning Algorithms: A Review", in IEEE (2021)
[5]. Mahbuba Yesmin Turaba et al "Fraud Detection During Financial Transactions Using Machine Learning and Deep Learning Techniques" in IEEE Oct 2022
[6]. Shabreshwari R M, Shafiya Mehrooz, Sidra Fatima, Tanmai R B, Prof. Ganesh Manasali "UPI Fraud detection using machine learning".
PDA College of Engineering, Kalabuaragi- 585103(2024)
[7]. Yash Patil, Amar Shinde, Yash Parthe, Sameer Sayyad. "UPI Fraud detection using machine learning**".** Savitribai Phule Pune University Pune, India.