ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr830

AI-Powered UPI Fraud Detection

Dr. D. Jaya Kumari [1]; Gurram Tejaswi [2]; Nekkanti Durga Sri Jahnavi [3];
Korapati Anusha[4]; Kotakonda Naga Kathyayani [5]; Areti Divya Sri [6]; Medapati Sharmila[7]

Student Scholar, Professor & Hod,
Department of CSE, Sri Vasavi Engineering College(A) Tadepalligudem – 534101.

Publication Date: 2025/04/24

Abstract: A significant step in safeguarding India's digital economy against cyber threats is the implementation of AI-driven fraud detection systems in Unified Payments Interface (UPI) transactions. Real-time transaction analysis is made possible by AI technologies, especially machine learning and deep learning, which aid in identifying anomalous patterns that might point to fraud. In 2023, there will be over 100 billion UPI transactions, increasing the need for sophisticated fraud detection techniques. These systems utilize anomaly detection, behavioral biometrics, and network analysis to monitor user interactions and transaction patterns. AI analyzes keystroke dynamics, mouse movements, and transaction history to differentiate legitimate users from fraudsters. Research shows that Generative AI (GenAI) enhances fraud detection accuracy by continuously assessing behavioral patterns, enabling swift identification of suspicious activities. Additionally, combining AI models like Random Forest, Naïve Bayes, and Support Vector Machines (SVMs) improves detection efficiency while reducing false positives. The flexibility of these AI models is crucial for combating new fraud methods, including deepfake scams and synthetic identity fraud. Additionally, initiatives like the Reserve Bank of India's MuleHunter.ai are instrumental in identifying mule accounts involved in illegal transactions and facilitating real-time fraud monitoring among financial institutions. This joint effort strengthens the security infrastructure while ensuring adherence to regulatory requirements for anti-money laundering and counter-terrorism financing. The growing use of AI-driven solutions to identify UPI fraud signifies a notable change in how financial institutions address security issues in an increasingly digital economy. With 72% of financial institutions in India currently employing or considering Generative AI (GenAI)-based technology for fraud prevention, the sector is experiencing a significant transformation that emphasizes the importance of security alongside user experience. As these technologies evolve, they will be vital in fostering consumer confidence and preserving the integrity of India's digital payment landscape in the face of changing cyber threats.

Keywords*: NLP, UPI, Digital Platforms.*

How to Cite: Dr. D. Jaya Kumari; Gurram Tejaswi; Nekkanti Durga Sri Jahnavi; Korapati Anusha; Kotakonda Naga Kathyayani; Areti Divya Sri; Medapati Sharmila (2025) AI-Powered UPI Fraud Detection. *International Journal of Innovative Science and Research Technology*, 10(4), 1208-1213. https://doi.org/10.38124/ijisrt/25apr830

I. INTRODUCTION

Financial transactions have been transformed by the rise of digital payment systems, especially India's Unified Payments Interface (UPI), which offers efficiency and convenience. Advanced security measures are crucial because of the increased danger of fraud brought about by this quick adoption. By using machine learning algorithms to evaluate enormous transaction databases in real-time and spot trends and abnormalities suggestive of fraudulent activity, AI-driven fraud detection systems have emerged as a vital defense against these dangers. By examining device data, user behavior, and transaction patterns, AI can efficiently differentiate between fraudulent and genuine activity. High false-positive rates are frequently the result of ineffective and error-prone traditional fraud detection techniques, which rely on manual monitoring and strict rule-based systems. On the other hand, AI models are always learning from past data, which enables them to adjust to changing fraud strategies and gradually increase the accuracy of their detections.AI can now monitor user interactions thanks to sophisticated techniques like anomaly detection and behavioral biometrics, which enable it to promptly identify odd activity, such as logins from strange locations or unusual purchasing habits. Furthermore, combining many machine learning models—such as Random Forest, Naïve Bayes, and Support Vector Machines (SVMs)—into a weighted fusion classifier has demonstrated encouraging outcomes in terms of precisely identifying fraudulent transactions while reducing misclassifications. This multi-layered AI system enhances fraud detection accuracy and lowers operational costs for financial institutions by automating fraud prevention processes. Given the high volume

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr830

of daily transactions and widespread UPI adoption, implementing AI-driven fraud detection is essential. Researchers have developed advanced AI models that accurately detect fraud using real-world transaction data from platforms like Google Pay. The continuous advancement of these AI systems ensures their effectiveness against evolving fraud tactics, strengthening the security and reliability of digital payment systems. As financial institutions continue to integrate AI-driven technologies, they can effectively reduce risks associated with digital payments, strengthen user privacy, and improve transaction security. In conclusion, AI-powered fraud detection is a groundbreaking innovation that plays a crucial role in protecting the integrity of UPI transactions and preserving consumer trust in digital payment systems, especially as cyber threats continue to rise.

II. LITERATURE SURVEY

- This study investigates strategies for preventing fraud that leverage artificial intelligence (AI), with an emphasis on machine learning (ML), deep learning, and natural language processing (NLP). It assesses the effectiveness of supervised learning methods, such as decision trees and neural networks, for pinpointing fraudulent transactions. Furthermore, the research examines unsupervised learning techniques like clustering and anomaly detection to uncover hidden fraud patterns. It also tackles significant challenges, including concerns about data privacy, the need for model transparency, and the ongoing requirement for advancements in fraud detection techniques.

- This research presents a hybrid system for detecting fraud that integrates both rule-based approaches and machine learning techniques. By employing anomaly detection methods, the system detects unusual transaction behaviors in real-time, enhancing security and reducing instances of fraud. Furthermore, the study highlights the importance of examining user behavior to improve the precision of fraud detection. The main goal is to increase user trust in digital payments by guaranteeing secure and reliable UPI transactions.

- This research presents a fraud detection system that utilizes various machine learning algorithms, such as Hidden Markov Models (HMM), Autoencoders, Local Outlier Factor, and K-means clustering. It assesses and contrasts these models, concentrating on their ability to identify fraudulent UPI transactions. The study emphasizes the importance of real-time fraud detection while striving to minimize false positives. Furthermore, it investigates feature engineering methods to enhance the precision of fraud detection.

- This research explores the identification of fraud in online transactions using machine learning methods. It tackles the challenges of real-time fraud detection amidst the large volume of digital transactions. The study highlights the importance of classifying fraud, selecting features, and creating predictive models, applying algorithms like Decision Trees, Random Forest, and Logistic Regression. The suggested framework aims to enhance financial security by providing an adaptable and effective system for detecting fraud.

- This research investigates the detection of UPI fraud through machine learning methods, employing supervised, unsupervised, and semi-supervised learning approaches. The authors advocate for the use of Random Forest in identifying fraudulent activities, highlighting its robust predictive power. The paper also emphasizes the significance of continuous monitoring and adaptive learning techniques for effective fraud prevention.

- This study investigates strategies for preventing fraud that leverage artificial intelligence (AI), with an emphasis on machine learning (ML), deep learning, and natural language processing (NLP). It assesses the effectiveness of supervised learning methods, such as decision trees and neural networks, for pinpointing fraudulent transactions. Furthermore, the research examines unsupervised learning techniques like clustering and anomaly detection to uncover hidden fraud patterns. It also tackles significant challenges, including concerns about data privacy, the need for model transparency, and the ongoing requirement for advancements in fraud detection techniques.

- This research presents a hybrid system for detecting fraud that integrates both rule-based approaches and machine learning techniques. By employing anomaly detection methods, the system detects unusual transaction behaviors in real-time, enhancing security and reducing instances of fraud. Furthermore, the study highlights the importance of examining user behavior to improve the precision of fraud detection. The main goal is to increase user trust in digital payments by guaranteeing secure and reliable UPI transactions.

- This research presents a fraud detection system that utilizes various machine learning algorithms, such as Hidden Markov Models (HMM), Autoencoders, Local Outlier Factor, and K-means clustering. It assesses and contrasts these models, concentrating on their ability to identify fraudulent UPI transactions. The study emphasizes the importance of real-time fraud detection while striving to minimize false positives. Furthermore, it investigates feature engineering methods to enhance the precision of fraud detection.

- This research explores the identification of fraud in online transactions using machine learning methods. It tackles the challenges of real-time fraud detection amidst the large volume of digital transactions. The study highlights the

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr830

importance of classifying fraud, selecting features, and creating predictive models, applying algorithms like Decision Trees, Random Forest, and Logistic Regression. The suggested framework aims to enhance financial security by providing an adaptable and effective system for detecting fraud.

III. EXISTING SYSTEM

The existing UPI fraud detection system relies on fixed rule-based methods, which struggle to keep up with evolving fraudulent activities. These systems often generate false alarms or fail to detect new types of fraud. With the increasing number of UPI transactions, traditional methods become less effective as they cannot adapt to changing fraud patterns. Additionally, they do not fully utilize the vast transaction data available. Machine learning offers a better solution by analyzing past transactions and identifying unusual patterns. It continuously learns from new data, improving accuracy and adaptability. Combining models like Random Forest, Naive Bayes, and Support Vector Machines can enhance fraud detection while reducing errors. Real-time behavioral analysis further strengthens security by monitoring user interactions. Adopting AI-driven fraud detection can minimize financial losses and improve transaction safety.

IV. PROPOSED SYSTEM

The proposed system aims to collect our college's feedback process for placements. It recognizes the vital role of placements in guiding students career paths and industry making. By analyzing data from successful and rejected students, it analayses pinpoint strengths and weakness, which enable focused improvements. The system introduces a dynamic feedback form for company HR, to fill out. This data will redirect visual representations of performance. The goal is to empower the college management to address specific lagging topics effectively, ultimately optimizing the placement outcomes. So that with this Project i.e, Placement feedback form analysis grabbing data from HR on how the student performed in every aspect ,how he taken interview with confidence levels. Finally with the input given by HR by filling the form, a graph or chart will be generated after successful analysis which gives a clear look by visualization. As this is a feedback form with numerical rating , Linear regression algorithm is used to predict overall form. For generating entire drive data regarding feedback is positive, negative or neutral, We are going for sentimental analysis Logistic regression which can deal large dataset and provide best result for overall strength.

V. METHODOLOGY

- *Natural Language Processing (NLP):*

NLP is applied to interpret and process textual data from UPI-related messages. It performs various tasks like breaking down the text into tokens, converting it to lowercase, and removing punctuation to clean and organize the content. These steps help highlight important information within the messages, allowing the system to more effectively identify signs of fraudulent activity.

- *Stopword Removal using NLTK:*

The NLTK library is utilized for stopword removal, eliminating frequently occurring but non-essential words like "is," "at," and "on" from transaction messages. This process minimizes unnecessary data, allowing the system to focus on critical keywords, thereby enhancing the accuracy of the fraud detection model.

- *URL Detection and Analysis:*

If a message includes a URL, the system extracts and examines it to identify potential threats. It looks for indicators such as incorrectly spelled domains, the presence of IP addresses instead of standard domain names, excessively long URLs, or the use of URL shorteners. Additionally, the system cross-checks these links with well-known security databases like Google Safe Browsing and PhishTank to verify their legitimacy.

- *Machine Learning Classification:*

Machine learning models like Random Forest, Ada boost, and Support K Nearest Neighbours (KNN) are trained using historical transaction and message data. By analyzing past instances of fraudulent and legitimate activities, these models can identify patterns that indicate potential fraud. This approach enhances detection efficiency and accuracy, allowing the system to quickly classify new messages or URLs as either safe or suspicious.

- *Real-Time Alert System:*

When the system identifies suspicious activity, it promptly notifies users and relevant financial institutions in real-time. This enables swift action to prevent potential financial losses, such as halting the transaction or alerting the user about a possible fraud attempt

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr830

VI. RESULTS

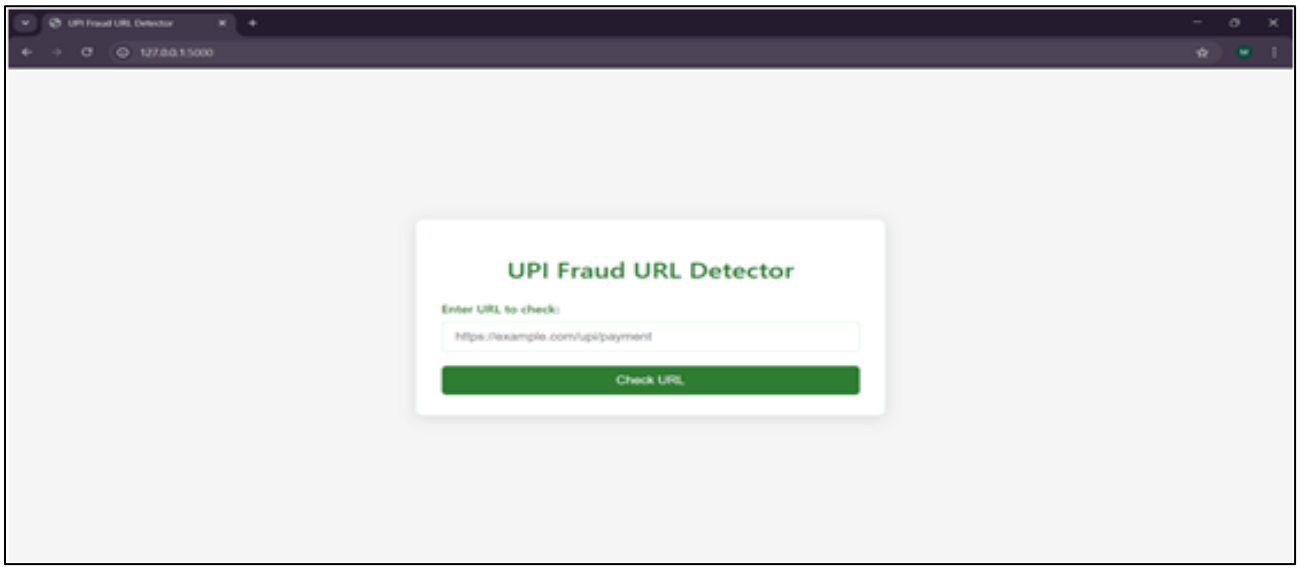

Fig 1: Web Page to Detect

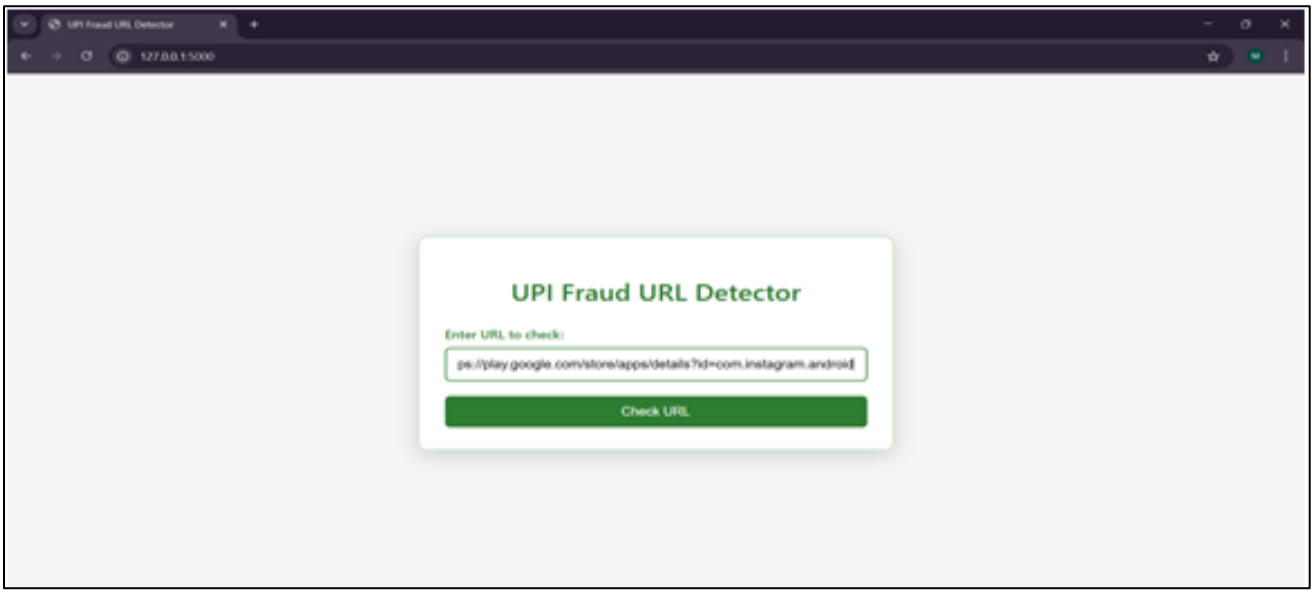

Fig 2 : Giving URL to Check

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr830

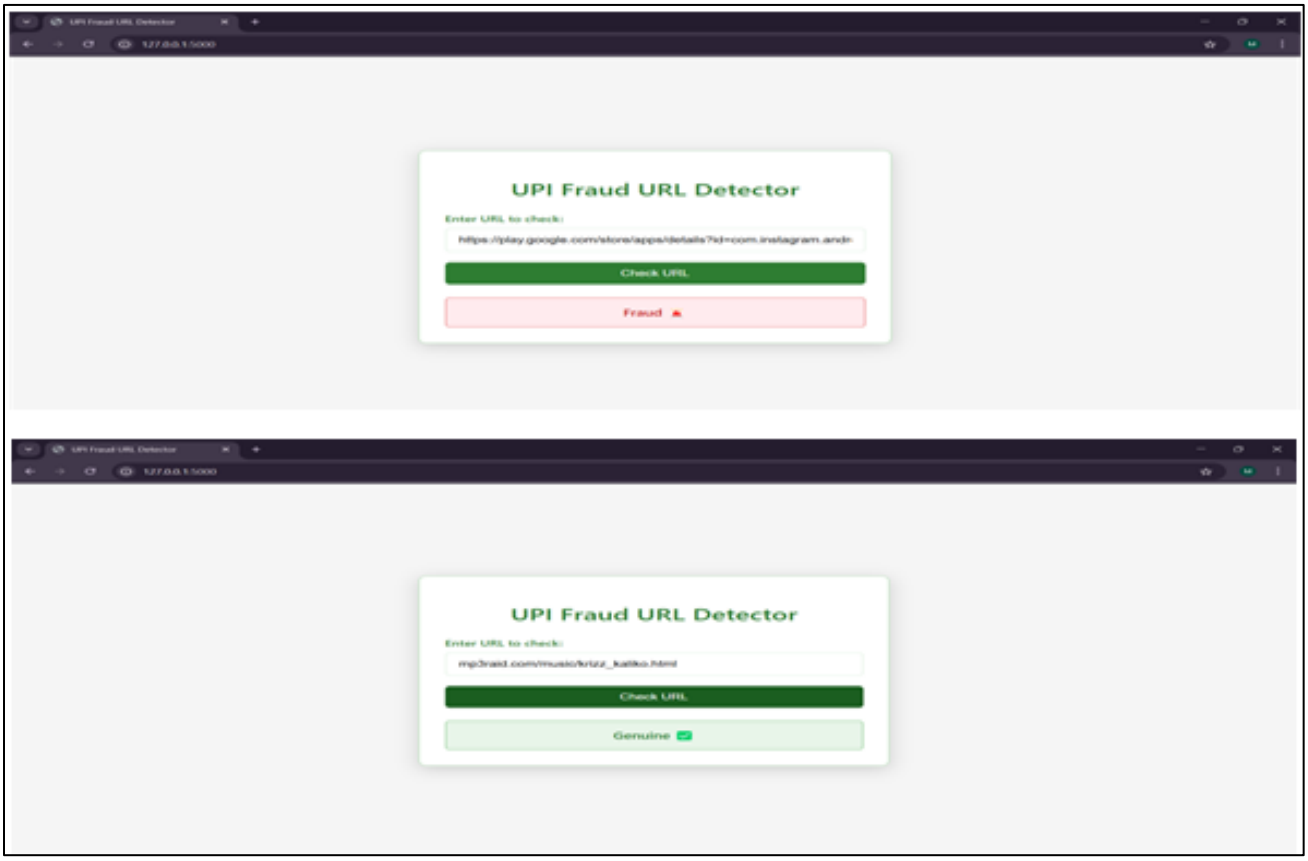

Fig 3: Result Analysis

VII. CONCLUSION

AI-powered fraud detection has significantly enhanced the security of Unified Payments Interface (UPI) transactions. As UPI usage grows, financial institutions face mounting challenges in fraud detection and prevention. Traditional rule-based methods, reliant on manual oversight, produce high false-positive rates and fail to adapt to evolving fraud tactics. In contrast, AI-driven solutions, leveraging machine learning and deep learning, offer a real-time, adaptive approach that improves accuracy and efficiency in fraud prevention. Through the examination of transaction trends, user interactions, and device information, AI models are capable of accurately distinguishing between genuine and fraudulent activities, thereby improving detection precision and reducing false positives. Sophisticated methods like anomaly detection, behavioral biometrics, and network analysis allow AI systems to evolve continuously, thereby increasing their efficacy in combating intricate fraud tactics, including deepfake scams and synthetic identity fraud. Furthermore, the incorporation of various AI models—such as Random Forest, Naïve Bayes, and Support Vector Machines (SVMs)—into hybrid fraud detection frameworks enhances the accuracy, scalability, and operational efficiency in identifying fraudulent transactions. The implementation of AI-based fraud prevention is essential for the growing digital payment landscape in India, where services such as Google Pay and PhonePe handle billions of transactions each day. By leveraging actual transaction data, AI algorithms enhance the precision of fraud detection, thereby fostering consumer confidence in UPI transactions. Furthermore, programs like the Reserve Bank of India's MuleHunter.ai bolster real-time fraud surveillance by pinpointing mule accounts associated with illegal activities. As financial institutions increasingly adopt AI-based fraud detection, they can significantly reduce digital payment risks, strengthen user privacy, and improve transaction security. Moving forward, continued advancements in AI and machine learning models will be essential to combat emerging cyber threats and maintain the integrity of India's digital payment infrastructure. The ongoing evolution of AI-driven fraud detection technologies will not only safeguard financial transactions but also foster greater consumer confidence, reinforcing India's position as a global leader in digital payments.

REFERENCES

[1]. Jagadeesan, S., K. S. Arjun, G. Dhanika, G. Karthikeyan, and K. Deepika. "UPI fraud detection using machine learning." In Challenges in Information, Communication and Computing Technology, pp. 755-760. CRC Press, 2025.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25apr830

[2]. Bello, Oluwabusayo Adijat, and Komolafe Olufemi. "Artificial intelligence in fraud prevention: Exploring techniques and applications challenges and opportunities." Computer science & IT research journal 5, no. 6 (2024): 1505-1520.
[3]. Gupta, Yash, Nitesh Saxena, and Krishan Kumar. "UPI Fraud Detection Using Machine Learning."
[4]. Sindhu, Jallapuram, and Ms Vijaya Sree Swarupa. "UPI FRAUD DETECTION USING MACHINE LEARNING ALGORITHMS." International Journal of Engineering Research and Science & Technology 20, no. 4 (2024): 57-67.
[5]. Dhanwani, D. C., Aniruddh Tonpewar, Devashish Ikhar, Komal Ladole, and Suyog Mahant. "Online Fraud Detection System."
[6]. Edburg, B. Franklin, K. Umadevi, M. Vidya, and PM Ramesh Kumar. "Role of UPI Application Usage and Mitigation of Payment Transaction Frauds: An Empirical Study." MDIM JOURNAL OF MANAGEMENT REVIEW AND 7 (2024).
[7]. Rajakrishnan Manivel, Dr D., and J. S. Harsika. "USER'S BEHAVIOUR TOWARDS UPI TRANSACTIONS OF COMMERCIAL BANKS IN COIMBATORE CITY."
[8]. NAGARAJU, MELAM, Polavarapu Nagendra Babu, Venkata Sai Pavan Ravipati, and Velpula Chaitanya. "UPI fraud detection using convolutional neural networks (CNN)." (2024).
[9]. Soni, Sanskar, Shweta Kanojiya, Siddharth Yadav, Rajendra Arakh, and Richa Shukla. "Online Payment Fraud Detection System Using Convolution Neural Network."
[10]. Gupta, Pankaj. "Leveraging machine learning and artificial intelligence for fraud prevention." SSRG International Journal of Computer Science and Engineering 10, no. 5 (2023): 47-52.