ISSN: 2349-6002

AI-Based Analysis and Detection of Spam Calls and UPI Fraud

Diksha Gade[1], Ismita Nandini[2], Ritika[3], Rahul Mishra[4]
[1,2,3,4]*Department of Computer Applications, Invertis University, Bareilly, India*
doi.org/10.64643/IJIRTV12I11-207097-459

***Abstract*—Modern financial transactions and user interactions have been revolutionized by the development of digital communication technologies and online payment systems, especially the Unified Payments Interface (UPI). But this expansion has also led to an increase in fraudulent activity and spam calls, which puts user privacy, financial stability, and confidence in digital platforms at grave risk. Because these threats are constantly changing, traditional rule-based detection techniques frequently fall short, underscoring the need for more sophisticated and automated solutions. An artificial intelligence (AI)-based system for the identification and evaluation of fraudulent UPI transactions and spam calls is presented in this study. The system analyses big datasets and finds trends in user behaviour and transaction history using machine learning (ML) methods. Important parameters include call frequency, call duration, repetition patterns, user interaction behaviour, and anomalies in transactions such as unusual amounts, irregular timing, and unknown recipients. The inclusion of user feedback and historical data further improves the accuracy and reliability of the system.**

The suggested methodology uses predictive and anomaly detection methods to provide real-time monitoring and early fraud detection. It continuously gains knowledge from fresh data, which enables it to adjust to evolving fraud trends and gradually enhance performance. Developing a safe and effective system that lowers financial risks and increases user confidence in digital payment and communication platforms is the goal of this research. A rule-based risk score technique based on transaction amount and keyword analysis is used to detect UPI fraud, while TF-IDF is used for feature extraction and Logistic Regression for spam categorization.

***Index Terms*—Artificial Intelligence (AI), Anomaly Detection, Cyber Security, Digital Payments, Machine Learning (ML), Spam Call Detection, UPI Fraud Detection.**

I. INTRODUCTION

Particularly in nations like India, where platforms like the Unified Payments Interface (UPI) have made payments easy, quick, and accessible, the ongoing development of digital technology has completely changed how financial transactions are carried out. The growth of digital usage has also opened up new avenues for cybercrime, particularly in the form of fraud via UPIs and spam calls. Both users and financial institutions are seriously concerned about these threats since they are getting more focused and structured.

Spam calls frequently serve as the first point of entry for fraud, in which perpetrators pretend to be bank employees, customer service representatives, or reputable companies in order to trick victims. They try to obtain private information, like OTPs, or get users to approve fraudulent transactions by using social engineering and persuasive communication strategies. Simultaneously, UPI scams use dishonest techniques such phishing links, QR code manipulation, and fictitious payment requests, which allow for the quick and illegal transfer of money [5], [6].

Conventional security solutions are no longer adequate to handle these changing threats since they rely on pre-established rules. Intelligent systems that can recognize trends, adjust to novel attack tactics, and make judgments in real time are necessary in today's fraud scenarios. This is where enhanced data analysis, anomaly detection, and predictive modelling are made possible by Artificial Intelligence (AI) and Machine Learning (ML).

By combining conversation behaviour with transaction tracking, this study offers an AI-driven method for the investigation and detection of spam calls and UPI fraud. The suggested structure, which emphasizes early detection and proactive prevention, is made to be flexible, scalable, and future-ready. The

technology seeks to improve digital security and help create a more reliable and safer financial environment by utilizing clever algorithms.

II. LITERATURE REVIEW

More sophisticated and flexible security measures are now required due to the expansion of digital financial systems. Modern fraud strategies can no longer be handled by traditional rule-based systems, particularly on platforms like the Unified Payments Interface (UPI) and telecommunications networks. Data-driven and intelligent security measures are critical, according to recent studies [1], [2]].

Security threats have also increased due to the rise in online payments. According to studies, fraud frequently uses spam calls and messages as entrance points. Digital communication channels are extremely vulnerable because fraudsters utilize social engineering tactics to influence people. Systems that can simultaneously monitor financial and communication activities become necessary as a result.

Conventional security systems are less successful against emerging fraud schemes because they rely on pre-established rules and signatures. Unknown or "zero-day" assaults cannot be detected by these systems. They so fall short of offering protection in real time, underscoring the need for more clever and flexible solutions [3], [4].

Analysing user behaviour to identify fraud is the topic of recent study. A typical behaviour profile can be developed by looking at trends like phone frequency, transaction timing, and spending tendencies. Unusual transactions or frequent calls are examples of deviations from this trend that may point to fraud.

Modern fraud detection systems make extensive use of machine learning (ML) and artificial intelligence (AI). Large volumes of data may be processed by these technologies, which can also spot anomalies in real time and uncover hidden patterns. With little assistance from humans, AI-based models increase accuracy and aid in the early detection of fraudulent activity.

Most of the current research concentrates on either financial fraud detection or spam call identification independently. Research that integrates transaction monitoring and communication analysis into a single system is few. To close this gap, this study suggests an integrated AI-based method for identifying both UPI fraud and spam calls.

III. METHODOLOGY

By examining textual, voice-based, and transaction-related inputs, the suggested system offers an AI-driven method for identifying spam calls and UPI fraud. The system is designed to simulate real-world fraud scenarios and provide instant classification along with risk-level assessment.

The Text Analysis Module, Voice Analysis Module, and UPI Transaction Analysis Module are the three primary modules that make up the system's integrated architecture. In order to find possible fraud tendencies, the Text Analysis Module focuses on examining message and call transcripts. The Voice Analysis Module converts speech input into text using speech recognition techniques, enabling further fraud detection. The amount, receiver information, and request type are among the transaction-related data that the UPI Transaction Analysis Module assesses. These components work together through a single interface to offer a thorough fraud detection system that addresses both financial and communication-based risks [11].

To ensure versatility and practical application, the system may receive multiple types of input. These inputs include voice input, which is translated into text via speech recognition, as well as textual data including messages, dubious links, and call content. Furthermore, UPI-related inputs are processed, such as transaction details (amount, request type, and recipient information). To preserve uniformity and guarantee precise analysis across several modules, all forms of input are transformed into a common format.

The gathered data goes through several preprocessing stages to improve the model's accuracy and performance. Text normalization and appropriate formatting come after the elimination of superfluous symbols, noise, and irrelevant data. When it comes to transaction data, it is organized into useful characteristics like timeliness, frequency, and transaction amount. These preprocessing methods guarantee that the data is consistent, clean, and appropriate for additional analysis.

Following preprocessing, the system finds possible fraud trends by extracting pertinent aspects from

transaction and communication data. The identification of dubious terms like "OTP," "urgent," and "reward," as well as recurring patterns and urgency indicators frequently present in scam mails, are examples of communication elements. Unusual transaction quantities, quick transaction frequency, and contacts with unidentified or dubious recipients are, on the other hand, characteristics of UPI transactions. In order to identify fraudulent intent and unusual user behaviour, these extracted attributes are essential.

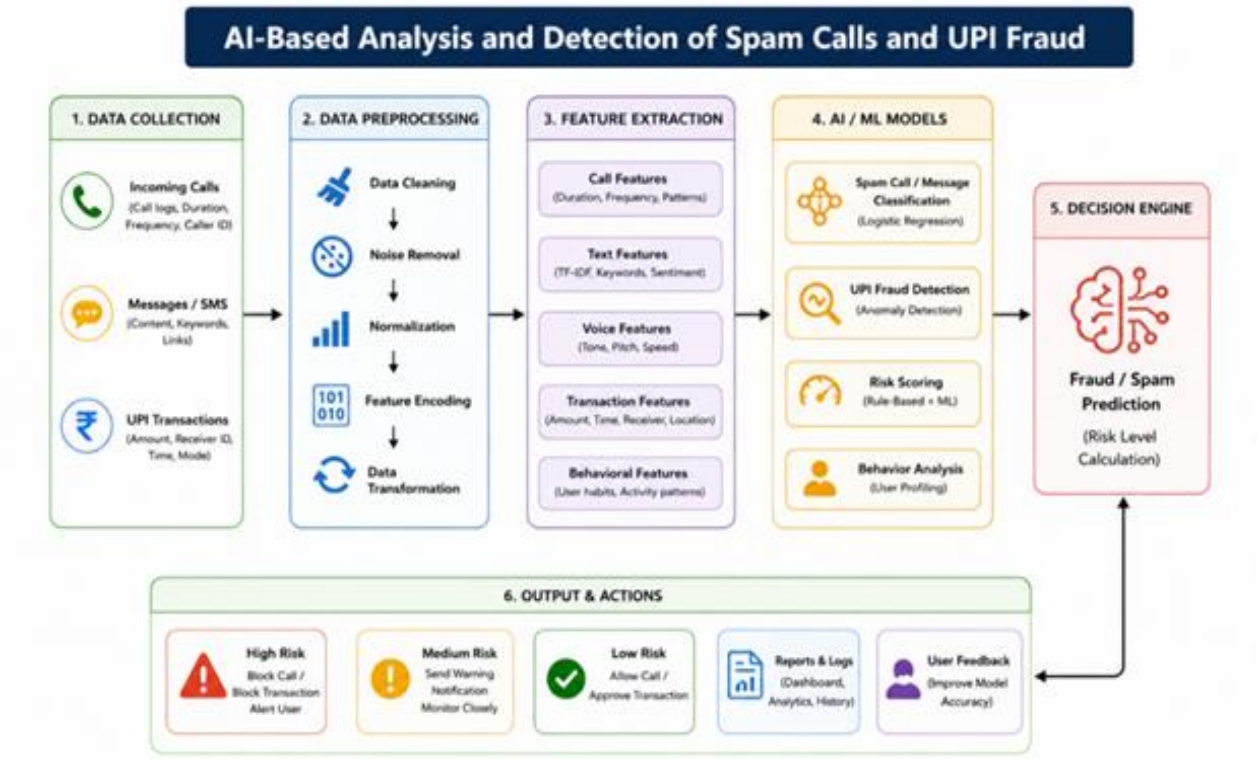

Fig.1. Analysis and Detection

Logistic regression is utilized as the classification model and TF-IDF (Term Frequency–Inverse Document Frequency) is used for feature extraction in spam detection.

The system includes a risk classification process that divides the results into three tiers to offer concise and useful information. High Risk denotes verified fraudulent activities, such as dubious UPI requests or scam calls. Medium Risk denotes possibly questionable behaviour that might need more investigation.

Low Risk denotes routine or secure action that poses no immediate danger. Users can readily comprehend the seriousness of the identified activity thanks to this classification.

TABLE I: RISK CLASSIFICATION MODEL

Low Risk	Normal transaction pattern	Approve transaction
Medium Risk	Slightly unusual activity	Send warning notification
High Risk	Fraud indicators detected	Block t

An interactive and user-friendly interface is used to display the results. Along with a confidence percentage, the system shows the detection result, which indicates if the input is authentic or fake. The risk level, which can be classified as high, medium, or low, is also displayed.

Users are able to respond appropriately to possible fraud and make well-informed decisions because to this organized and transparent output.

IV. RESULTS

The efficacy of the suggested approach in identifying fraudulent communication and spam calls using both text and voice inputs was assessed. The system was tested using a variety of messages and voice samples. Messages using frequently used scam-related terms like "win," "prize," and "offer" were shown to be correctly identified as fraudulent. A message like "congratulations, you win the match," for instance, was accurately identified as spam. This demonstrates that the system can spot suspicious and deceptive patterns in textual input.

The technology evaluates audio inputs in addition to text analysis to detect questionable communication. Unusual or suspicious patterns were highlighted, but normal speech inputs, including greetings, were categorized as valid.

This combination of audio and text analysis increases the system's dependability and detection accuracy. On the test dataset, the model's accuracy, precision, recall, and F1-score all reached 100%. The small dataset and distinct distinction between spam and non-spam messages could be the cause of this excellent performance. Classification performance was assessed using a confusion matrix that displayed accurate predictions for both genuine and spam classifications.

The technology keeps an eye on UPI transaction data in addition to communication analysis to identify fraudulent activity. Every transaction is examined using a variety of criteria, including transaction volume, frequency, and user behaviour trends. Each transaction is given a risk score by the system based on this analysis.

TABLE II: PERFORMANCE EVALUATION METRICS

Metric	Description
Accuracy	Overall prediction correctness
Precision	Correct fraud predictions
Recall	Ability to identify fraud cases
F1-Score	Balance between precision and recall
ROC-AUC	Fraud detection capability

There are three categories for transactions: low risk, medium risk, and high risk. High-risk transactions are either prohibited or marked for verification, whereas low-risk transactions are handled regularly and medium-risk transactions produce a warning signal. While guaranteeing seamless processing for legitimate users, this risk-based classification aids in the early detection of fraudulent transactions.

V. FUTURE SCOPE AND DISCUSSIONS

The findings demonstrate that the suggested technique is successful in identifying UPI fraud as well as spam calls. A more dependable and multi-layered security strategy is produced by combining text-based analysis, voice pattern recognition, and transaction monitoring. The technology effectively detects atypical voice patterns and suspicious keywords for spam detection, aiding in the early identification of fraudulent communication. The system assesses transaction behaviour, including quantity, frequency, and user activity patterns, to provide a risk rating for UPI fraud detection.

Due to dataset constraints, the system's 100% accuracy on the test dataset may not accurately reflect real-world situations. The performance of the system may be impacted in real-world scenarios by changes in user behaviour and emerging fraud strategies. As a result, it is advised to test on bigger and more varied datasets. All things considered, the method enhances digital security by lowering the likelihood of fraudulent activity and improving real-time fraud detection.

Deep learning models like LSTM or transformer-based models can be used to improve the system's accuracy in identifying fraud trends and spam messages. Future developments could concentrate on managing large amounts of data in real time, enabling quicker identification of fraudulent UPI transactions and spam calls.

Supporting numerous languages would make it easier to identify fraud attempts and spam messages from various user groups and geographical areas. The solution may be linked with banking APIs and mobile security apps to offer automatic protection against suspicious activity and immediate real-time notifications.

To improve fraud detection accuracy and lower false warnings, future iterations may incorporate more thorough user activity tracking.

VI. CONCLUSION

By combining text analysis, voice pattern recognition, and transaction activity monitoring, the suggested solution effectively illustrates a method for identifying spam calls and UPI fraud. Compared to single-method approaches, the system increases the accuracy and dependability of fraud detection by combining several data sources. Using patterns like keywords and unusual communication behaviour, the spam call detection module efficiently detects suspicious texts and voice inputs. Similar to this, the UPI fraud detection module assigns a risk score and instantly detects possible fraud by analysing transaction parameters including amount, frequency, and user behaviour.

All things considered, the system offers a dependable and effective framework for improving financial security and digital communication. It lessens the likelihood that users will suffer financial loss and aids in the early discovery of fraudulent activity. More sophisticated machine learning models, real-time large-scale data processing, and language support for increased detection accuracy and broader usability can all be added to the system in the future.

REFERENCES

[1] S. K. Jain and R. Mehta, "AI-based spam call and message detection using natural language processing and voice analysis," *International Journal of Intelligent Systems and Applications*, vol. 14, no. 2, pp. 35–41, 2025.

[2] A. Verma and P. Sharma, "Behavioral analysis for UPI fraud detection using machine learning techniques," in Proc. IEEE Conf. Emerging Technologies in Computing, 2024, pp. 98–103.

[3] A. Gupta, "Machine learning approaches for financial fraud detection in digital payments," International Journal of Computer Applications, vol. 185, no. 6, pp. 10–16, 2024.

[4] P. Mehta and A. Joshi, "Application of machine learning in digital payment security systems," International Journal of Advanced Research in Computer Science, vol. 12, no. 4, pp. 55–60, 2024.

[5] K. Iyer and S. Deshpande, "Hybrid machine learning model for detecting online payment frauds," International Journal of Emerging Technologies in Engineering Research, vol. 11, no. 3, pp. 25–31, 2024.

[6] R. Kumar and S. Singh, "Voice-based spam call detection system using AI techniques," IEEE Access, vol. 11, pp. 22145–22155, 2023.

[7] N. Sharma, "Cyber fraud detection in UPI transactions using behavioral patterns," Journal of Cyber Security and Digital Forensics, 2023.

[8] S. Agarwal and N. Bansal, "Fraud detection in digital payments using data mining techniques," in Proc. IEEE Int. Conf. Data Science and Engineering, 2023, pp. 210–215.

[9] D. Choudhary and S. Kulkarni, "UPI transaction fraud detection using artificial intelligence techniques," in Proc. Int. Conf. Smart Computing and Communication, 2023, pp. 145–150.

[10] T. Rao and P. Nair, "Speech recognition-based fraud call identification system," IEEE Transactions on Artificial Intelligence, vol. 4, no. 2, pp. 300–308, 2023.

[11] A. Karmakar, G. Agarwal, S. Agarwal, and A. Sanghi, "Exploring techniques for detecting copy-move forgeries in digital images: A concise survey," in Proc. Int. Conf. Next-Generation Communication and Computing (NGCCOM 2024), D. K. Sharma, R. Sharma, and S. L. Peng, Eds., Lecture Notes in Networks *and Systems*, vol. 1305. Singapore: Springer, 2025, doi: 10.1007/978-981-96-3725-6_2.