International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Multi Model Fraud Analytics in Digital Payments: A UPI-Based Approach

Sneha D S[1], Sowmya V[2]

[1,2]R V Institute of Technology and Management, (Affiliated to Visvesvaraya Technological University) Bengaluru, Karnataka, India

Abstract:
The rapid growth of Unified Payments Interface (UPI transactions has made it an important method for transactions in worldwide. As the use of digital payment systems increases, the risk associated with like fraud has also become a serious concern. To tackle this, system uses a several machine learning models like random forest, XGBoost and LSTM to predict the chances of fraud in transactions. To improve the system transparency, the solution uses LIME to provide clear explanations for the system results. The application has a user-friendly interface where users can enter transaction details and can see the results. A voice alert system announces whether the transaction is fraudulent or not and a results email notification is automatically sent to the user based on the prediction.

Keywords: Machine Learning, LIME, Flask App, Voice Alerts, Email Notification, Admin Dashboard, User Management, Finance

1. INTRODUCTION

A. Background

The proliferation of digital payments has changed the financial sector with Unified Payment Interface leading the way in throughout the world. This allows money transfer between bank accounts using mobile devices which encourages cashless transactions. To identify fraud in these transactions is challenging because financial behaviors are constantly changing and diverse. Fraudulent patterns evolve, making static rules inadequate. To address these issues, using machine learning algorithms, presents a promising approach for adapting fraud detection systems.

B. Objectives

The main goal of the research was to design, develop and validate an accurate machine learning model for detecting fraudulent transactions in real-time within UPI ecosystem. An important goal was to create a multi-model, alert system to ensure users are quickly notified of potential security threats through email and voice. Additionally, this research project aims to build a complete administrative side that includes two separate modules: A user side panel to check the transaction by user and get notified. An admin side panel consists of transaction checking, dashboard and user management options. The final goal is to merge the predictive models, alert system, user and admin side option into one unified and validated end-to-end system. This approach will provide a practical and effective solution for improving the security and reliability of digital payments.

C. Scope

- The research's sole focus was on the analysis and detection of fraud transactions within the UPI sys-

tem. Credit card, debit cards and net banking are not included.

- Development of front-end module that enables users to test their own transaction history and can check the results.
- Installation of multi model prediction and alert systems that sends users a voice if user, a disabled person and email notification of results predicted.
- Constructing a secure administrative panel with two distinct areas. Dashboard will display transaction data visualization and user management will allow administrators to view status of user who currently logged in.
- The project makes use of LIME XAI to provide administrators with a feature-based, concise explanation of the model's predictions.

2. LITERATURE REVIEW

In Fiscal Year 2024-25, the Unified Payment Interface (UPI) accounted for almost 83.4% of all retail electronic transactions by volume, demonstrating the rapid expansion of digital payments in India. However, due to the similar development trend, fraud losses increased to Rs. 520 crores during the fiscal year, compelling banks, researchers and regulators to develop more advanced and data-driven counter measures. In order to safeguard UPI rails in real time, the study by Kavitha et al. [1] suggest an ensemble of Hidden Markov Models (HMM), Convolutional Neural Networks (CNN). This paper's methodology within the large corpus of scholarly, commercial and regulatory work on payment fraud detection.

Using machine learning approaches, Akinje and Abdulgalee [2] looked at developing a fraud detection model for Unstructured Supplementary Service Data (USSD). While USSD offers crucial financial services to consumers without smartphones, the authors point out that it is also susceptible to fraud because there are not enough detection models in place to deal with this problem. Their study concentrated on improving model performance by extracting statistical information from the collection of consumer activities in a brief period of time.

According to a literature analysis by Viswanatha V et al. [3] in the paper, online fraud is a major and expanding problem in the digital age, necessitating the development of efficient detection systems. The authors point out those conventional techniques, such human reviews and static rule-based systems, are frequently laborious and unable to keep up with the intricate and quickly changing strategies employed by scammers. Implementing efficient fraud detection systems is hampered by a number of issues, such as idea drift, skewed data distribution and the sheer amount of data.

Ashtiani and Raahemi [4] synthesize studies on the application of data mining and machine learning for financial statement (FFS) fraud detection in their systematic literature review. The authors point out that in comparison to other forms of fraud, FFS causes the most financial losses and the conventional techniques such as manual auditing are frequently expensive, inaccurate and time-consuming. Technique-wise, supervised learning algorithms have been widely preferred with the most widely used strategy being classification approaches.

To increase the efficacy of fraud detection systems, Chauhan et al. [5] evaluate a number of strategies that have been investigated in earlier research in their study on UPI fraud detection. One such technique is anomaly detection and behavioral analysis, which tracks user behavior patterns, navigation and interaction history to spot departures from typical behavior. The authors also point out that suspicious networks suggestive of money laundering or collaboration have been found by mapping the links between various parties in a transaction including users, merchants using graph-based research approaches.

The shift from conventional detection methods to more advanced machine learning algorithms is reviewed by Kadam et al. [6] in their study on online transaction fraud detection. They point out that the usefulness of traditional methods, which are mostly focused on statistical and multi-dimensional analysis, is limited since they frequently fail to identify the underlying patterns in transaction data. Dealing with the unbalanced data where fraudulent cases are greatly outnumbered by valid ones remains a serious difficulty in the profession. The utilization of both labeled and unlabeled data in semi-supervised methods and the ability to effectively handle a large number of transactions.

The substantial expansion and regulatory changes in India's fintech and digital payments sector are contextualized by the literature review conducted by Jagadeesan et al. [7] in their work on UPI fraud detection. Citing Sagar Suresh et al. research, which looks at the effects of significant government programs like Adhaar and the National Payments Corporation of India (NPCI), they point out that these laws have encouraged the growth of fintech industry in tandem with the nation's rapidly rising internet adoption rate. There is also a discussion on how the Reserve Bank of India's goal of a less cash society caused a significant change in India's payment systems.

In the study on UPI-based financial fraud detection, Gupta et al. [8] examine a variety of research that uses different machine learning and deep learning methods to detect fraud transactions, most related to online payments and credit cards. The authors research on data mining methods and classification algorithms with 92-94% accuracy such as logistic regression and decision trees. By citing research that used CNNs to achieve high precision and recall one model achieving 99.9% accuracy for UPI fraud.

A. Identified gaps

The present rule-based fraud detection systems are not flexible enough to recognize changing fraud patterns. Due to high volume and real time nature of UPI transactions, the current system is unable to manage them, therefore, scalable and effective solutions needed. The study presents a novel method uses LSTM networks to analyze sequential UPI transaction data, addressing the dearth of techniques specifically made for detecting UPI fraud. Using cutting-edge AI developments to increase the system's resilience and flexibility in the face if changing fraudulent trends.

2. METHODOLOGY

A. Approach

A dynamic and adaptable Unified Payment Interface transaction fraud detection system is put into place by using multi machine learning models. The main approach is to use an algorithm to precisely detect and stop fraud transactions in real time. The core machine learning engine is integrated with a comprehensive two-module python application that includes an advanced admin panel dedicated to monitoring, model interpretation and user management as well as an interactive user interface for checking of the transactions. Two separate modules for administrator and user makes up the solution's architecture. In addition to offering email and voice alerts, the user module crucially gathers user input on transactions that have been flagged in order to produce high-quality data labels.

In this project, the Random Forest algorithm was employed given its strong reputation and widespread use in fraud detection applications. Additionally, XGBoost and LSTM models were also trained as part of the implemented solution. LSTM, a type of deep learning architecture, was selected for the UPI fraud detection task due to its ability to recognize temporal patterns and capture long-term relationships within sequential data—capabilities that traditional classification algorithms may miss. This makes LSTM particularly well-suited to analysing the inherently sequential nature of financial transaction records.

B. Data Collection

Finding the right data to train our fraud detection system was like searching for the perfect ingredients for a complex recipe. We needed massive amounts of real transaction records - the kind that banks and payment companies deal with every day - but with a crucial twist: each transaction had to come pre-labeled, telling us definitively whether it was legitimate or fraudulent. Our treasure hunt led us to popular data-sharing platforms like GitHub and Kaggle, where researchers and organizations generously share their datasets with the community. These platforms became our goldmine, offering collections containing millions of actual transaction records that previous researchers had already carefully examined and categorized. What made these datasets particularly valuable wasn't just their size - though having millions of examples certainly helped - but their richness. Each transaction came packed with relevant details: payment amounts, merchant information, user behavior patterns, timing data, and dozens of other factors that could potentially signal whether something fishy was going on. Think of it as having access to a massive library of financial stories, where each transaction tells a tale of either normal shopping behavior or suspicious criminal activity. This diverse collection of real-world scenarios became the foundation our machine learning models would learn from, helping them understand the subtle differences between honest customers making purchases and fraudsters trying to game the system.

C. Tools and Techniques

The following tools and techniques were used to implement and test the system functionality:

Development Tools and Framework: Because Python is widely used in data science, it was used to construct the system. The UI and API endpoints for interaction were created using the Flask framework. Tailwind CSS, HTML, and Jinja templating were used to create user and administrator interfaces that were responsive and efficient.

Preparing data and using machine learning models: To provide consistency among models, MinMaxScaler was used to normalize all numerical input features. Categorical inputs were properly encoded, and missing values were handled. To increase the accuracy of predictions, a collection of machine learning models was used.

Interpretation of the Model: Local Interpretable Model-Agnostic Explanations, which offer feature-wise contribution for the prediction, were utilized to support and improve explainability.

Database and Email Integration: The MySQL database contains user credentials and transaction information. The database was interfaced with using Flask-MySQLdb. Additionally, users get notifications via SMTP Gmail using Flask-Mail.

Visualization and Access Control: Matplotlib was used to create the visual analytics in dashboard, which shows the number of transactions in both fraud and non-fraud cases. Role-based access is supported by the system, which separates administrators from users.

RESULTS AND DISCUSSION

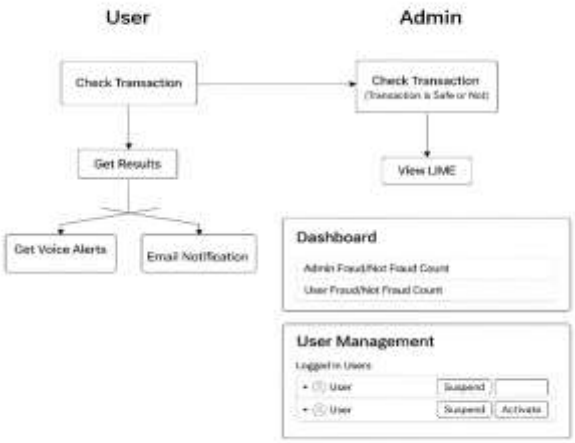

Fig. 4.1 Workflow of fraud detection system

The Fig.4.1 provides the detailed architecture of dynamic fraud detection system.

In the Fig.4.1, the suggested Unified Payment Interface Fraud Detection System's operational architecture is shown in detail. The workflow is divided into two main components: a user module and an admin module, designed to enhance both system clarity and efficiency. This dual-module setup offers a comprehensive solution, equipping administrators with the necessary tools for oversight, analysis, and intervention, while also providing users with greater transparency. The entire process is interactive and operates in real-time—beginning with the entry of transaction data, passing through the machine learning model for evaluation, and culminating with notifications sent to users via email.

User Module: Notification and Interaction

The User Module acts as the primary gateway for everyday users, designed with simplicity and speed in mind to make transaction verification effortless. When someone wants to check if a transaction might be suspicious, they start by inputting the transaction details through an intuitive analysis interface. Behind the scenes, sophisticated machine learning algorithms spring into action, examining the submitted information and cross-referencing it against patterns of fraudulent behavior they've learned from past data. Once this automated review is complete, users receive clear, no-nonsense feedback - the system simply tells them whether their transaction appears legitimate or raises red flags for potential fraud. To ensure security and maintain proper usage records, users need to sign into their accounts before they can begin checking transactions. The system safely stores these login credentials in the database, which helps administrators keep track of platform usage while making future logins smoother for returning users.

This approach transforms what could be a complex fraud detection process into something as straightforward as checking your email - users get the sophisticated analysis they need without having to understand the technical complexity working behind the scenes.

Admin Module: System management and analysis

The admin module gives system administrators a set of strong tools to keep an eye on, assess, and control the platform's security. It mimics the user's capacity to perform transaction checking, but it has more capabilities and offers enhanced results with a higher degree of understanding. The Local-Interpretable Model-Agnostic Explanations (LIME) visualization is accessible through this module, which goes beyond

a straightforward "Fraud/Safe" assessment. When administrators examine which factors most significantly impact the model's decision-making process, they develop a deeper understanding of the reasoning behind transaction alerts. This analysis directly addresses the essential need for transparency and explainability in fraud detection systems.

Beyond its analytical capabilities, the administrative module encompasses two fundamental management features:

Comprehensive Dashboard Interface: The dashboard functions as a sophisticated monitoring hub that oversees all transaction flows within the system. Administrators can observe real-time patterns in both fraudulent attempts and legitimate business activities, creating a comprehensive view of system performance. What makes this dashboard really useful is how it can tell the difference between security checks that happen automatically (because the system is programmed to do them) and those that start when users actually report something suspicious. This helps administrators understand what new threats are popping up and see how different people are using the security features.

Keeping an Eye on Users: The user management section lets administrators see what's happening with users on the platform in real time. They can check who's currently online and logged in, which helps them quickly spot and respond to any security problems. If something looks suspicious, administrators can temporarily block a user's access or give access back to someone who was previously locked out. This hands-on approach to managing users helps keep everything secure while making sure people can still use the system smoothly.

When you put all these features together, they create a solid control centre for administrators - one that keeps things secure without making it complicated or frustrating for users to get their work done.

The below figures show the example of how the system works to real-time data

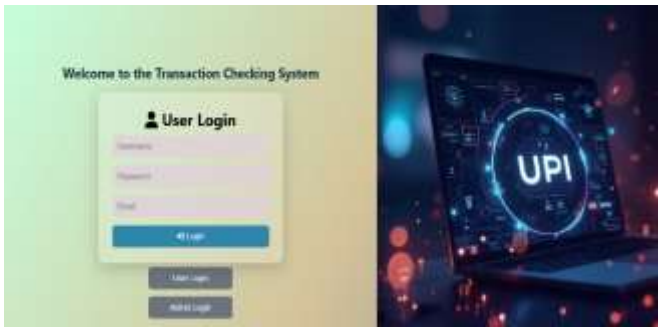

Fig.4.2 Login page for admin and user

Fig.4.3 User side transaction checking form with input details

Fig.4.4 Result of transaction checked will appear in user mail

Fig.4.5 Visual representation of fraud counts

Fig.4.6 User management in admin side with active and suspend button

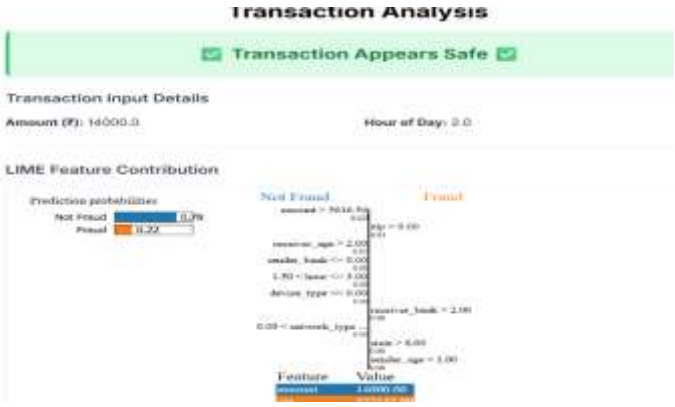

Fig.4.7 Admin can view the results checked by themselves with LIME

Table 4.1.1 Comparison of scores

Model	Accuracy (%)	Precision	Recall	F1-Score	ROC AUC
Random Forest	99	0.99	0.99	0.99	0.994
XGBoost	60	0.61	0.60	0.60	0.650
LSTM	56	0.56	0.56	0.56	0.584

INTERPRETATION OF RESULTS

The proposed fraud detection system performed well in identifying potentially fraudulent transactions by combining machine learning models with interpretability techniques. Realistic transaction data that includes amount, transaction hour, send and receiver age, device types was used to test the system work. LSTM, Random Forest and XGBoost were three different models used to assess each transaction. The likelihood that a transaction was fraud was determined by each of these models separately. A consensus-based method was applied and if at least one of the models exceeds the predetermined threshold value, fraud was reported. This preserved overall robustness. The results were processed and fed into the LIME model, which provided various predictions along with explanations that highlighted the key factors the model considered when making decisions.

The system breaks down its decisions by looking at individual cases, making it easier for administrators to spot unusual patterns or understand confusing results. When it detects fraud, it immediately sends out both email and phone alerts so people know about potential problems before they get worse. The dashboard shows everything openly, letting administrators dig into specific transaction details whenever they need to. What makes this work well is using several different analysis methods together. This approach cuts down on both false alarms and missed fraud since machine learning deals with likelihoods rather than yes-or-no answers. Looking at the data in Table 4.1.1, the Random Forest model performed exceptionally well, hitting 99% on accuracy, precision, and recall - way better than any other model tested. The LSTM model, however, only managed 56% accuracy, which was much lower than expected.

Regarding the collaborative model approach - different algorithms complement each other effectively. When one model misses something, another often catches it. This combined methodology handles uncertainty more effectively than single-method approaches. The dashboard allows administrators to track each step in the process, supporting accountability when reviewing flagged transactions. Internal metrics show that voice alerts generate faster response times compared to email-only notifications. People typically respond more quickly to phone calls when potential financial issues are involved. The Random Forest results are logical given how these algorithms process multiple data points simultaneously, compared to the sequential processing approach of LSTM model, it can identify sequential pattern.

The decision to include LSTM in the analysis was deliberate - since UPI transactions are inherently sequential, LSTM networks are designed to capture temporal dependencies in this type of time-based data. The LSTM model should theoretically excel at transaction-based fraud detection because it's designed to learn from sequences of data, which is exactly what we have with transaction patterns. A few things probably made the LSTM model not work so great here. Maybe the data didn't have enough of those sequence patterns LSTMs are good at spotting. There was that classic problem where most transactions were legit. Made it tough for the model to really learn what fraud looks like. They probably should have tried more setups with the LSTM. Different training approaches, maybe bigger datasets showing how transactions play out over time. Those deep learning models eat up tons of data points anyway. Even

though LSTMs did not shine here, the takeaway still matters. Random Forest's clearly the winner for this specific dataset as things stand. But that doesn't mean we should write off deep learning stuff like LSTMs. With better data prep and some tuning, they might crush it next round. For now, Random Forest is our go-to solution, but LSTM and similar deep learning models deserve consideration for future implementations when we have access to more comprehensive datasets.

The high-performance potential of LSTM networks in fraud detection tasks might be unlocked in the future with improved feature engineering or larger sequential datasets or with hybrid model training.

CONCLUSION

This research developed a robust fraud detection system that combines multiple machine learning models, creating a framework that is both effective and easy to interpret for identifying fraudulent UPI transactions. By integrating different models, the system can detect various fraud patterns, whether they appear in time-based sequences or within structured transaction data. What makes this approach special is how we merged the results from all these models and used smart threshold settings to make the system more sensitive to suspicious behavior while staying flexible enough to adapt to new fraud tactics. We also made sure the system explains its decisions clearly - when it flags a transaction as potentially fraudulent, it tells you exactly why, which is absolutely crucial when you're dealing with people's money. The real-world impact is pretty significant. Bank staff and financial teams now have a much better toolkit for spotting sketchy transactions, and they actually understand what red flags to look for in fraudulent activity patterns. Instead of just playing defense and catching fraud after it happens, the system actively monitors transactions and immediately alerts the team when something doesn't look right. Plus, it breaks down each transaction's risk profile in detail, so decision-makers know exactly what they're dealing with and can act fast when needed.

What makes this particularly valuable is how user-friendly the interface has become. Instead of complicated dashboards that need a lot of training, the system shows information in a clear way for both technical and non-technical staff. Users actually want to engage with the platform because it's simple and doesn't overwhelm them with extra complexity. This is especially important for digital payment systems like UPI, which millions of people use every day. The solution keeps up with growing transaction volumes, maintains steady performance under stress, and most importantly, reveals to users how it comes to its conclusions instead of acting like a mysterious black box. This approach builds trust between financial institutions and their customers while offering the strong protection that modern digital payments require.

A. SIGNIFICANCE OF WORK

This research tackles a significant problem that impacts millions of people who use digital payment systems daily. As UPI and similar platforms manage increasingly large transaction volumes, traditional fraud detection methods struggle to keep pace with the advanced techniques criminals develop. The work contributes in several meaningful ways to both academia and the financial technology industry. First, it shows that you can maintain transparency without sacrificing accuracy in building AI systems for fraud detection. Many current solutions treat explainability as an afterthought. However, this research shows that interpretable models can perform just as well as black-box methods. When you look at the real-world impact, this approach could help banks avoid losing millions to fraudulent transactions each year. At the same time, fewer genuine customers would have their legitimate purchases wrongly rejected - something that's incredibly frustrating when you're just trying to buy groceries or pay a bill. We've all been there -

your card gets declined at checkout, and when you call the bank, they can't give you a straight answer about why it happened. This research changes that dynamic by providing clear explanations without compromising the security measures that protect your account. What makes this methodology particularly effective is how it marries two different technological approaches. Neural networks excel at spotting subtle patterns that humans might miss, while traditional machine learning offers the kind of transparent decision-making that both regulators and everyday customers can understand and trust. Perhaps most significantly, this work demonstrates that we don't have to choose between powerful AI systems and ethical responsibility. Too often, companies build complex algorithms first and worry about transparency later - if at all. This research proves you can bake accountability and clear explanations right into the system from day one. Whenever automated systems make decisions that affect people's financial well-being - whether that's loan approvals, insurance claims, or investment advice - we need this kind of responsible approach. This research provides a practical roadmap for building AI systems that are both effective and trustworthy in situations where the stakes really matter for ordinary people.

COMPARISON WITH EXISTING RESEARCH

Individual machine learning models like Decision Trees, Logistic Regression have been the main focus of previous research on UPI or digital payment fraud detection. Although these methods have demonstrated respectable results in identifying established fraud trends, they have frequently fall short in managing changing fraud tactics or offering model transparency. The use of deep learning models to identify patterns in transactions has been researched in recent studies. But they are viewed as black box systems, the majority of the determined model have poor interpretability. To improve the robustness and adaptability of the system, the current work presents an approach that utilizes multiple machine learning algorithm and deep learning technique. Furthermore, our system addresses the growing need for interpretable AI in delicate fields like finance by integrating XAI and explain individual forecasts, in contrast to many previous models. Moreover, a large number of existed research are only created as offline prototypes. By providing a deployable flask-based interface, facilitates real-time transaction prediction, visualization, user and admin dashboards and email and voice alerts. This research project bridges the gap between real-world implementation and research problems, advancing the state of art.

SCOPE FOR FURURE RESEACH

The landscape of contemporary banking has changed dramatically with the increasing use of digital payment methods, which provides remarkable efficiency and ease, especially through platforms like Unified Payments Interface (UPI). The future improvements can lead to more advanced and efficient system of the payment platform. Future studies ought to concentrate more on semi-supervised, bio-inspired and metaheuristic algorithms as well as unsupervised techniques like anomaly detection and clustering. The general robustness and integrity of transaction data can be improved by incorporating state-of-the-art technology like blockchain into UPI fraud detection systems. Examining why some classifiers, such as SVM and logistic regression perform badly in particular situations is a specialized subject for the scope of research. Also, addressing of challenges pertaining to resource optimization and scaling one of the needed advancement studies. For systems to adjust to changing fraud strategies and emerging security threats, they must be continuously enhanced and upgraded.

REFERENCES

1. J. Kavitha, G et al. “Fraud Detection in UPI Transactions Using ML”, 2024, EPRA International Journal of Research and Development (IJRD), pp.142-146.
2. Ayorinde O. Akinje, Fuad Abdulgalee,” Fraudulent Detection Model Using Machine Learning Techniques for Unstructured Supplementary Service Data”, 2021, International Journal of Innovative Computing, pp.51-60.
3. Viswanatha V et al. “Online Fraud Detection Using Machine Learning Approach”, 2023, International Journal of Engineering and Management Research, pp.45-57.
4. Matin N. Ashtiani, Bijan Raahemi “Intelligent Fraud Detection in Financial Statements Using Machine Learning and Data Mining: A Systematic Literature Review”,2022, IEEE Access, pp.72504-72525.
5. Vinay Chauhan, Amit Kumar, Prashant Mann “UPI fraud detection using ML”, 2024, Journal of Emerging Technologies and Innovative Research (JETIR), pp.53-59.
6. Kishori Dhanaji Kadam et al. “Online Transaction Fraud Detection Using Machine Learning”,2023, International Journal of Advances in Engineering and Management (IJAEM), pp.545-548.
7. S. Jagadeesan et al. “UPI Fraud Detection Using Machine Learning” ,2025, Challenges in Information, Communication and Computing Technology, pp.755-760.
8. Vaishali Gupta et al. “UPI Based Financial Fraud Detection Using Deep Learning Approach”,2024, International Conference on Advances in Computing Research on Science Engineering and Technology (ACROSET), pp.1-6.