International Journal of Innovations & Research Analysis (IJIRA)
(An International Quarterly Multidisciplinary Peer Reviewed Refereed Journal)
e-ISSN :2583-0295, Impact Factor: (Cosmos 7.662 & I2OR 5.105), Volume 06, No. 02(I), April- June, 2026, pp 17-24

A Study of UPI Fraud and Complaint Process against UPI Frauds and its Prevention

Anjali Meena[1*] | Dr. Jyoti Jagwani[2]

[1]Research Scholar, Maharshi Dayanand Saraswati University, Ajmer, Rajasthan, India.
[2]Research Supervisor & Assistant Professor, Sophia college (Autonomous), Maharshi Dayanand Saraswati University, Ajmer, Rajasthan, India.

[*]Corresponding Author: anjalimeenasogan@gmail.com

Citation: Meena, A. & Jagwani, J. (2026). A Study of UPI Fraud and Complaint Process against UPI Frauds and its Prevention. International Journal of Innovations & Research Analysis, 06(02(I)), 17–24.

ABSTRACT

Online payments have made payment methods easier. *The use of* ***UPI has become necessary for*** *business,* ***banks****, hospitals, education****, similarly recharging,*** *buying* ***bus****,* ***train tickets****,* ***paying electricity bills, UPI*** *transactions* ***have become necessaryfor payment of small everyday expenses. As****UPI* ***transactions are increasing, so are*** *UPI* ***frauds. Therefore, it*** *has become necessary to be aware of the frauds that occur in* ***UPI transactions. Under this paper, the awareness of UPI users aboutfraud has been studied****.*

Keywords*: UPI Fraud, Types of UPI frauds, Process of Complaint Against Fraud, Prevention from Fraud.*

Introduction

This research paper explains the types of UPI frauds and the procedure for complaint. UPI fraud avoidancemeasuresand information about the institutions related to the complaint have been made available. and the methods of analysisof UPI fraud. The objective of this paper is to increase the awareness of UPI fraud among the users.

Literature Review

Dr. Yogesh Shukla (2026), The study investigates awareness and adoption of UPI applications among 506 college students in Etawah District, Uttar Pradesh. The study adopts a descriptive and analytical research design and uses primary data collected through structured questionnaires via both online and offline modes. Percentage analysis and frequency distribution techniques were employed for data interpretation. Findings reveal that 90.7% of respondents are aware of UPI apps and 85.6% actively use them. PhonePe (43.3%) is the most preferred application, followed by Google Pay (27.7%). Although 32.8% of respondents reported experiencing online fraud, 85.8% are willing to recommend UPI apps. The study concludes that UPI adoption among college students is significantly high; however, digital security awareness needs strengthening for sustainable financial inclusion.

Jallapuram Sindhu, Ms. Vijaya Sree Swarupa (2024), In this study 5 Algorithms to detection the UPI Fraud and evaluated results based on that. Various modern techniques like artificial neural network. Different machine learning algorithms are compared, including Auto Encoder, Local Outlier Factor, Kmeans Clustering. This project uses various algorithms, and neural network which comprises of techniques for finding optimal solution for the problem and implicitly generating the result of the fraudulent transaction. This algorithm is a heuristic approach used to solve high complexity computational problems.

Melam Nagaraju, Yarramreddy Chandrasena Reddy Dept. of IT, Polavarapu Nagendra Babu et al. (2024, March14), This paper introduces a novel approach utilizing Convolutional Neural Networks (CNNs) for fraud detection. The study focuses on developing machine learning models tailored for recognizing fraudulent transactions and addresses challenges such as imbalanced datasets, feature transformation, and engineering. The proposed CNN-based model exhibits superior accuracy, particularly in handling imbalanced datasets, offering a promising solution compared to traditional algorithms. The research emphasizes the adaptability of CNNs to unconventional data types, such as banking transactions, and showcases their ability to capture intricate fraud patterns. Evaluation metrics include precision, recall, F1-Score, ROC Curve, and AUC, providing a comprehensive assessment of the model's effectiveness.

K Padma Kiran & Vedala Naga Sailaja (2025), This study examines the factors influencing the intention to adopt UPI with a focus on add-on services, perceived promotional benefits, and perceived trust with the integration of the Unified Theory of Acceptance and Use of Technology (UTAUT). Employing the survey responses of 416 UPI users, this research applies partial least squares structural equation modeling (PLS-SEM) to validate the hypothesized model developed for this study. The findings revealed that facilitating conditions, performance expectancy, effort expectancy, social influence, perceived promotional benefits, and perceived trust significantly influence the users' intention to adopt UPI, which further influences its usage behavior. Interestingly, add-on services by UPI did not affect the intention of users to adopt UPI, questioning its role in UPI adoption. However, add-on services had a significant impact on performance expectancy and effort expectancy. Additionally, perceived promotional benefits impacted facilitating conditions for UPI usage. Demographic attributes further moderated these relationships: age and occupation significantly moderated the impact of performance expectancy on the intention to adopt UPI, while gender and income did not exhibit any profound moderating effects. The findings offer valuable insights for service providers and policymakers aiming to improve UPI adoption among consumers. Customized strategies considering demographic variations can optimize the platform's accessibility and appeal to a broader audience.

Amit Rohilla (2024), This paper navigates the intricate landscape of financial fraud, addressing its various dimensions and offering a comprehensive strategy to strengthen defences. IN This framework not only clarifies key terms but also informs the subsequent analysis by establishing theoretical underpinnings. The research methodology section delineates the chosen approach, whether qualitative, quantitative, or a mix of both.

Research Methodology

The study is descriptive in nature and secondary data has been used under this study. Secondary data has been collected from commercial websites and newspapers. After reviewing 50 papers, the top 12 papers were selected, and based on them, this paper was prepared. For this paper, only papers from Google Scholar have been reviewed.

UPI Fraud

UPI fraud refers to any type of fraudulent activity that occurs in the context of UPI-based digital transactions. UPI is a popular payment system that allows users to instantly transfer funds between bank accounts via mobile. UPI has made transactions faster and more convenient, making it essential for users to be aware of fraud and scams.

Types of UPI Fraud (Amit Rohilla, 2024)

Phishing	Phishing occurs when fraudsters send fake UPI links via text message, e-mail, or phone call, or ask for sensitive information such as UPI PIN, password, and OTP. Once they find this information, they use it to transfer funds or make purchases without the user's consent. Phishing is a common cybercrime tactic that lures victims into clicking on fake or suspicious links. These links often come in the form of emails or websites that send stolen data, such as login credentials, personal information, or financial details, to fake sites designed to steal them. Phishing also installs malware in the device, giving cybercriminals unauthorized access.
Vishing	This is a type of UPI scam, in which fraudsters use voice calls to tell the user sensitive information like UPI PIN, password, OTP. They cheat by posing as bank officials or representatives of UPI payment providers to win the trust of the user. Spam/wishing calls are a deceptive form of cybercrime. Fraudsters use social engineering to trick victims into disclosing personal or financial information, such as personal information and financial data. They often create fake identities of legitimate entities, such as banks or government agencies. They use tricks like caller ID spoofing and pressure them to take immediate action to gain trust and steal

Digital arrest	Digital arrest occurs when a person is stopped or restricted by digital means rather than traditional physical arrest. This often involves fraudsters impersonating government officials so that they can extort money. In this, criminals intimidate the user by telling him that he is involved in a crime and threaten to arrest him. To save the crime, fake arrest warrants and court notices are shown and to avoid crime, it is said to calm the matter by taking money and asking for account information or to transfer money from the account, as soon as someone shares personal information or transfers their money, all the payments disappear from their account and after them. It is found that they are victims of digital fraud.
This challan is fraudulent in the name of Bus and Marriage Bureau.	An e-challan traffic violation notice is sent by the offenders. The APK file is offered as an e-challan app with which there is a link, as soon as you click on that link, all the data reaches the hackers and the money is withdrawn from the account. Apart from this, **a link is sent on WhatsApp for registration in the Marriage Bureau**. Clicking on the link, all the money is transferred to the hackers.
KYC Scam	In KYC scams, cybercriminals exploit identity verification processes to steal real personal information or create illegal access to financial accounts. This can lead to significant financial losses and reputational damage, whether for individuals, businesses, or financial institutions. Common tricks include deceiving people, creating fake documents, and creating false identities.
Malware	It is a software that is used to steal a user's UPI login credentials, payment information, or other sensitive data.
Money Mule accounts	In this type of UPI scam, fraudsters use unsuspecting users as intermediaries to transfer the money obtained through illegal means. They promise commissions or other incentives in exchange for the user using their UPI account to receive or transfer funds.
SIM cloning	SIM cloning is a process in which fraudsters create a duplicate SIM card of the victim's mobile number. They then use this SIM card to access the victim's UPI account and transfer funds without the victim's knowledge.
Cyberbullying	This includes online bullying or threatening to harm someone, cyberbullying and dissemination of content, online harassment.
Cyber Police	There is a form of harassing or bullying someone using electronic communication means such as computer, laptop, phone, etc.
Sending email spoofing	Sending e-mails that look real and with a trusted ID that they know but don't do.
Banking fraud	Receiving money from the depositor's account by posing as a bank or other financial institution.
Job/Employment-Related Fraud	Fraud is done by giving fake advertisements through newspapers or through fake websites
Online Shopping Fraud	They create fake websites or **fake platforms** to fraudulent victims, offer such deals and steal personal and financial information, causing financial losses in the online market.
Financial Fraud from Online Gaming	Online gaming has become a hotspot for cybercriminals, with threats ranging from virtual and account breaches to real-world financial fraud and identity theft. Attackers exploit platforms and gaming apps promising secure returns to players through phishing schemes, malware, and social engineering.
Investment scam	Investment scams **involve fraudulent schemes** that lure investors by promising **incredibly high returns**. These are also often **referred to as** Ponzi schemes, where new investors' money is used to benefit old investors.
Lottery fraud	The user is sent a message to win the lottery amount and the amount credited to your account is immediately sent a link to transfer money to their account, then ask them to send money in exchange for shipping fees or sharing personal information. These scams often take advantage of the expectation of a big win.
Quishing Scam	Quishing scams are on the rise. Scammers lure QR codes with promises or convenience deals to scan but ultimately unauthorize financial transactions. Malicious code can directly redirect users to phishing sites, steeling credentials, or transferring money directly to a scammer's account. Valid scanning codes do not require entering banking details such as MPIN or password.
Search Engine Fraud	Search engine fraud occurs when fraudsters manipulate search results to spread fake contact information, such as information pretending to be legitimate entities. Such individuals are tricked into making unintentional calls that can reveal these sensitive information, such as passwords and account details, leading to financial loss, identity theft, and many other serious consequences.
Social Media Impersonation	Social media impersonation occurs when a person pretends to be another. By creating fake profiles, fraudsters try to win people's trust in order to deceive them.

SMS, Email and Call Scams	SMS, email, and call scams are used by fraudsters to deceive victims with fake offers. They use their logos and fake IDs to impersonate trusted NBFCs (non-banking financial companies), as well as ask for advance payments using fake letterheads or requests. Fraudsters disappear once the payment is made.
Debit and Credit Card Fraud	Debit and credit card fraud occurs when the card details are stolen without the user's consent or by doing unwanted activity in the ATM, data or debit, credit card and the user is defrauded.
Cyber Slavery	Cyber slavery involves the exploitation of individuals through digital platforms, where they are forced or manipulated to work without compensation. It imposes human trafficking and forced labor. It uses the internet and digital devices specifically for exploitation.
SIM swapping	SIM swapping is a fraud in which fraudsters trick the user's mobile operator into transferring the user's phone number to their SIM card, so that all the user's calls and messages go to them and they commit fraud by accessing banks, social media and other accounts, it gives them access to calls, texts, and two-factor authentication codes. This leads to identity theft, account hacking, and financial fraud. It is also called SIM jacking or port-out scam. It is often coaxed into revealing personal details by offering upgrades to network staff or through benefits.
Juice jacking	There is a cybersecurity risk associated with compromised public **USB charging stations**. Hackers misuse USB ports to charge and transfer data, allowing them to steal sensitive information from your device.
Deepfake Cybercrime	**Cybercriminals** create fake videos or audio clips using advanced AI **(**Artificial Intelligence), which manipulate the actual footage or recording. These spread quickly through fake media, social media, messaging apps, and email. Its goal is often to target public figures, celebrities, or people in power. The purpose of criminals is to deceive, manipulate, or spread misinformation to people. Criminals also use social engineering techniques to make deepfakes real, posing risks to individuals and organizations.
Remote Access Fraud	This fraud occurs when cybercriminals impersonate trustworthy entities (such as technical support services, banks, or government authorities). They **lure individuals into gaining unauthorized access through screen-sharing** apps. Once accessed, they can steal data, take control of accounts, and carry out fraudulent transactions.
Safe Browsing	**Safe browsing involves using practices and tools to protect yourself from** online threats such as phishing, malware, and identity theft while surfing the internet. This ensures secure interactions with websites and reduces cyber risks.
Ransomware	Ransomware is a type **of malicious software** that locks the victim's files, making them unable to use. The attackers demand a ransom in exchange for unlocking the file. The attackers then **spread the ransomware through phishing emails,** malicious software downloads, and security flaws. It spreads rapidly to individuals and organizations, causing significant data loss and financial damage.

Key Institutions to Prevent Online Fraud in India (Amit Rohilla,2024)

Institutions	
The Reserve Bank of India RBI is the regulator of the digital payment system.	• Enforcing KYC/CKYC Rules • Mandatory 2-Factor Authentication (OTP, PIN) • Customer Protection Guidelines in Digital Payments • Issuing Fraud Reporting and Refund Rules to Banks
Home Ministry – I4C (Indian Cyber Crime Coordination Centre)	**Objective:** Prevention of Cybercrimes • **National Cyber Crime Reporting Portal** (cybercrime.gov.in) • 1930 Helpline Number (Digital Fraud Reporting) • Cyber Police Training • Coordination between States
CERT-In (Computer Emergency Response Team – India) **Role:** Cybersecurity Agency	**Functions:** • Warning of Cyber Attacks • Phishing & Malware Alerts • Safety guidelines for banks and fintech companies • Mandatory data breach reporting
SEBI (Securities and Exchange Board of India)	**Digital Investment Fraud Prevention** • Warning on Fake Investment Apps/Links • Online Trading Fraud Monitoring • Investor Awareness Program

Department of Telecommunications (DoT)	• Fake SIM/SIM Call/Call/Call Ban on SMS • SMS Header and URL Blocking • Spam control in tandem with TRAI
6. State Cyber Cell /Cyber Cell, Cyber Police	• Online fraud investigation at the local level • Digital Evidence Collection • Freeze fraud account
Functions to be performed by NPCI (National Payments Corporation of India)	NPCI operates systems like UPI, RuPay, IMPS, FASTag, AEPS **in India**. Provide data of digital payments and payments banks.
TRAI	• **Fake Calls & Fraud SMS** • **TRAI has directed telecom companies to:** ▪ **Fake customer care calls** ▪ **Fraud SMS (KYC update, account block, etc.) should be blocked.** • **TRAI implemented DLT (Distributed Ledger Technology) to:** ▪ **Bank/UPI SMS can be sent only with registered sender ID** • **Fake bank SMS is caught** ▪ **On receiving repeated complaints:** ○ **Fraud calling numbers** ○ **Bulk scam** ○ **SIMs are blocked or deactivated** **TRAI protects UPI not directly, but by closing the path of UPI fraud (Fake Call, SMS, Spam).**

Measures to Avoid UPI Fraud

UPI Fraud Prevention Measures	• **2-Factor Authentication (PIN + Mobile Binding)** • Device and Mobile Number Verification • Transaction Limit per Day • Real-time monitoring of suspicious transactions
UPI Auto-Disable & Cooling Period	• Cooling period of 24–48 hours **for changing a new mobile/device.** • Temporary Block on Suspicious Behavior
Fraud Risk Management (FRM) System	• Fraud pattern detection with AI/Rule-based systems • Repeatedly Block on Failed PIN Attempts • Identity of Suspicious Merchant/User
Awareness & User Safety Initiatives	• "**Share PIN = Fraud**" campaign • Warning messages in apps • NPCI+Banks + Awareness by UPI Apps
Guidelines for Banks and Apps	• Security Standards for Third Party Apps (Google Pay, PhonePe, Paytm) • Data Encryption and Log Monitoring • Grievance Redressal Timeline
Dispute Resolution Mechanism	• UPI Complaint System • TAT (Turn Around Time) • Refund Process Instructions to Banks

UPI Fraud Detection Method

Methods	Profit	Loss
Rule-Based Detection Method • Alert on pre-determined rules • Example: • Repeated transactions in a very short period of time • Log in with a new device • Sudden payment of a large amount	• Simple and fast • Rule-based systems, which are often rigid and easily circumvented by sophisticated fraud tactics**, (Sindhu & Shree Swarupam, 2024)**	• **Can't catch new fraud patterns**

User Behavioral Analysis Method • Comparison with common user habits • Checked: ▪ Payment time ▪ Location ▪ Amount Pattern	• **Real-time detection** • **Accurate**	• **Initial data needed**
Device & Location Fingerprinting • Mobile Device ID • IP Address / GPS • SIM & OS Details	• **Helpful in identifying fake users**	• **Privacy concern**
Machine Learning (ML) Based Detection (Machine learning based) • **Algorithms:** ▪ **Logistic Regression** ▪ **Decision Tree** ▪ **Random Forest** ▪ **SVM** • **Learning from Historical Data**	Random Forest algorithm which is strong and can deal with big data creates an ensemble of many decision trees and aggregates their prediction to achieve higher accuracy of 96% and lower overfitting. The model achieved a precision of 97%, recall of 91%, and an F1-score of 93%, indicating its strong capability to accurately detect fraudulent transactions while minimizing false positives and false negatives. Results of experiments reveal that the model is capable of identifying fraudulent transactions with high accuracy and recall. The system includes user friendly interface that gives real time fraud detection, transactional monitoring and fraud alerts. With the use of machine learning in digital payment security this project offers a trustworthy means to prevent UPI fraud and enjoy secure financial transactions**. (Sethi et al 2025)**	
AI & Deep Learning Method • **Neural Networks** • **Pattern recognition** • **Real-time risk scoring**	• Very effective Large-scale systems के लिए best • The machine learning model provided a more dynamic solution capable of adapting to evolving fraud techniques. • UPI transactions based on transaction behaviour and user patterns. The machine learning model was successful in identifying patterns associated with fraudulent transactions. Through feature engineering, the system developed a deep understanding of behaviours, such as transaction frequency, transaction value, and user location, that could signal potential fraud. **(Sindhu & Shree Swarupam, 2024)**	• **High infrastructure requirement**

OTP & Multi-Factor Authentication (MFA) • OTP • Biometric (Fingerprint/Face ID) • PIN verification	• **This is a Strong security layer**	• **User convenience is a little less.**
Transaction Velocity Monitoring • Identification of transactions happening very quickly	**Small Multiple Payouts = Red Flag**	
Blacklist & Whitelist Method • **Blacklist**: Suspicious Accounts/Accounts number • **Whitelist: Trusted merchants**	**Easy and effective**	**Limited range**
HMM (Hidden **Markov Model)**	• An HMM is initially trained for a card holder. If a UPI transaction is not accepted by the trained HMM. It is considered to be fraudulent. People can use UPIs for online transactions as it provides an efficient and easy-to-use facility. **(Sindhu & Shree Swarupam, 2024)**	
CNNs	• The CNN-based model exhibits superior accuracy, particularly in handling imbalanced datasets, offering a promising solution compared to traditional algorithms. (**MELAM NAGARAJU et al. 2024**)	
UTAUT Modal	• The UTAUT MODEL measure, performance expectancy, effort expectancy, social influence, perceived promotional benefits, and perceived	

Conclusion

After reviewing so much literature, it can be said that the level of digital fraud has increased significantly, for which there are many methods to prevent it, but still, fraud is increasing. It is essential for people to have information not only about digital awareness but also about the complaint process and institutions that protect against digital fraud.

References

1. Swaraj, A., & Bohara, A., (2024). A Comprehensive Study on Security Measures and Consumer Awareness with Special Reference to UPI in India, Library Progress International, 44(3).
2. Kumar., & Rani, N., (2025). Optimized Machine Learning and Deep Learning Approaches for Effective Detection of Fraud in Unified Payments Interface (UPI) Transactions International. *Journal on Science and Technology (IJSAT)*, 16(4). Website: www.ijsat.org Email: editor@ijsat.org.
3. MELAM NAGARAJU, Yarramreddy Chandrasena Reddy Dept. of IT, Polavarapu Nagendra Babu Venkata Sai Pavan Ravipati, V. Lakshmi Chaitanya et al. (2024 March 13) UPI Fraud Detection Using Convolutional Neural Networks (CNN),Research *Square,V1, 1-16. ISSN 2693-5015 (online)* https://doi.org/10.21203/rs.3.rs-4088962/v1
4. SAINI, A. (2025). SECURITY AND FRAUD PREVENTION IN ELECTRONIC PAYMENT SYSTEMS: UNDERSTANDING USER BEHAVIOUR. *TPM–Testing, Psychometrics, Methodology in Applied Psychology*, *32*(S6 (2025): Posted 15 September), 727-739.
https://tpmap.org/submission/index.php/tpm/article/view/1833/1464

5. Shukla, Y. (2026). Assessing Awareness and Adoption of UPI Apps Among College Students of Etawah District. *AIJFR-Advanced International Journal for Research*, *7*(1).
https://www.aijfr.com/papers/2026/1/3636.pdf

6. Kiran, D. S., Sanjay, S., & KR, S. N. (2025). ENHANCED UPI FRAUD DETECTION. *International Journal of Information Technology, Research and Applications*, *4*(Special Issue), 9-24.
https://www.ijitra.com/index.php/ijitra/article/download/180/87

7. Sethi, B., Mhatre, S., Yadav, S., Das, S., & Jadhav, V. (2025, October). Machine Learning-Based UPI Fraud Detection: A Comprehensive Approach Using Random Forest. In *Proceedings of the MULTINOVA: First International Conference on Artificial Intelligence in Engineering, Healthcare and Sciences (ICAIEHS-2025)* (p. 462). Springer Nature.
https://www.atlantis-press.com/article/126016569.pdf

8. Unified Payment Interface Fraud Detection Using AI, ML, and Blockchain Technology Author - Suyog Brahmadeo Patil

9. Rohilla, A., (2024, May). Strengthening Financial Resilience: A Holistic Approach to Combatting Fraud. *Indian Journal of Economics and Finance (IJEF)*, *Published by Lattice Science Publication* (LSP), 4(1), http://doi.org/10.54105/ijef.A2566.04010524

10. Journal Website: www.ijef.latticescipub.com

11. Padma Kiran, K., Assessing Unified Payments Interface (UPI) adoption and usage through the interplay of UTAUT factors. *HUMANITIES AND SOCIAL SCIENCES COMMUNICATIONS ARTICLE,* 1-12.https://doi.org/10.1057/s41599-025-05313-w

12. Sindhu,J.,Swarupam, V.S.., (2024, October 3). UPI FRAUD DETECTION USING MACHINE LEARNING ALGORITHMS. *International Journal of Engineering Research and Science & Technology*, *20*(4), 57-67. https://ijerst.org/index.php/ijerst/article/view/446

13. Bhiku Bhoite, D., “A Study on Factors Influencing on The Adoption of E-Wallets While Using Digital Currency for Business Resilience and Sustainability in Satara Region” NBN Sinhgad School of Management Studies, Ambegaon (Bk.), Pune, India dashrathbhoite@gmail.com.

❑❑❑