"An Analytical Study of FinTech Frauds in India: Types, Trends, and Ecosystem Vulnerabilities"

Yamini Lohani, Mittal School of Business, Lovely Professional University, Phagwara, India,
yaminilohani66@gmail.com

Mentor- **Dr Vishal Goyal**

ABSTRACT

Financial technology (FinTech) has reshaped the delivery of financial services in India. UPI, digital payment, Internet banking, card-based payment, and App-based services have gained in usage. Although the wider access has resulted in improved speed and convenience, it has also made users and institutions more prone to digital financial frauds. This study on fin tech frauds in India aims to fulfil three objectives. First, to identify and classify the major types of fin tech frauds. Second, to analyse the historical trend and year wise pattern on the basis of available secondary data. Third, to find out the various vulnerabilities in the eco system for frauds.

This research is descriptive and analytical in nature and based on secondary data. Using a structured review of selected literature and payment-system indicators, as well as domestic payment fraud statistics, contained in the uploaded dataset. The analysis categorises FinTech frauds into four broadly: social engineering frauds; technical frauds; identity-related frauds; and transaction or platform-related frauds. The trend analysis indicates that there has been a substantial increase in the domestic payment fraud volume, fraud value and fraud intensity during the available period concurrent with the significant growth in payment systems especially UPI and source infrastructure. The study finds that fraud vulnerability is not just a user problem. Rather, it is the result of interacting weaknesses at the user, platform, institutional, and regulatory levels.

The investigation suggests that FinTech fraud in India is more an ecosystem problem than a mere technological misuse problem. According to the study which was published as an article by Digital Finance Outlook 2022, Faster Institutional Response, Stronger Awareness System, Enhanced Interface Safeguards and Coordinated Regulatory Evolving are essential for the Safer Digital Financial Growth. Moreover, the explosion of digital finance has increased exposure surface for fraud.

Keywords: FinTech fraud, India, UPI fraud, digital payments, e-banking fraud, fraud trends, ecosystem vulnerabilities, digital finance.

CHAPTER 1: INTRODUCTION

FinTech fraud is when people defraud others or commit fraudulent activities using technology-enabled financial services. These include digital payments, UPI, internet banking, mobile wallets, cards, digital lending platforms, and other online systems. The last ten years have seen a boost in India's digital finance sector, which has changed people's habits in making payments, taking loans, etc. Although this expansion has made things more convenient and faster, and has improved financial inclusion, it has created new opportunities for cybercriminals and fraudsters.

Fintech fraud is considered a form of cybercrime and digital fraud. Fraud includes phishing, vishing, identity theft, account takeover, fake loan app, QR-code, UPI fraud, card fraud etc. Frauds use loopholes in technology, user awareness, platform security, and enforcement of regulation. In India, there has been widespread adoption of smartphones, digital payment apps and app-based financial services that will lead to increasing scale and complexities of such frauds.

FinTech fraud is studied because it harms not only the consumer but also the banks, NBFCs, FinTech firms, payment service providers, and the trust in the digital financial ecosystem as a whole. So, it is necessary to know the categories,

trends, causes and regulatory responses of these FinTech frauds in India to enhance cyber security, consumer protection and the safe development of FinTech sector.

The classifications of FinTech frauds for the study may be broadly categories as followed.

1. Social engineering frauds.

These frauds utilise psychological manipulation, not direct technical intrusion. The scammer deceives the victim in order to obtain OTP, PIN, password, card details or consent for payment.

2. Technical scams.

These frauds use technical flaws, hacked devices or software vulnerabilities.

3. Identity Thefts.

Activity like the misuse, theft, fabrication, or unauthorised use of personal identity and KYC data.

4. Frauds Relating to Transaction and Platform

Such activity takes place through Financial Transaction Systems and Financial Platforms.

1.1 Background of FinTech Fraud in India

FinTech is making payments, banking, lending faster, easier and accessible in India. As a result, the delivery of financial services is getting impacted. These days, we rely on services like UPI, mobile wallets, internet banking, payment gateways, cards, and app-based lending. These days, people are using digital finance not only to carry out large transactions but also for everyday tasks like paying shopkeepers, recharging mobile phones, paying school fees, receiving money and availing short-term credit. Nonetheless, fast, easy and low-friction plus wide accessibility features of Fintech have enhanced forgery chances in the system. digital finance fraud is when scammers trick users through deception, use technology for fraudulent gains, and misuse digital financial systems. FinTech fraud is a highly pertinent area of study in India, as the rapid adoption of digital finance in the country has been taking place after the pandemic, and the occurrence of fraud now threatens not just the safety of finances but also public trust in the digital economy.

FinTech fraud allows the perpetrator to design frauds that can target a wide genre. It is a sort of fraud, which has become prevalent across payment systems, e-banking channels, and digital lending platforms. It usually combines social engineering with different weaknesses in app design, institutional response, and user awareness. Thus, the problem is greater than isolated case of cheating. The digital financial ecosystem's broader functioning is closely related to it. Understanding how fraud works across interconnected financial pathways, how patterns have changed over time, and why vulnerabilities continue to persist despite technological advances and regulatory safeguards are key to a study of FinTech fraud in India.

Conceptual Position of FinTech Fraud

The largest category of cybercrime, i.e., cybercrime is the use of computer, communication system, network or internet to commit any unlawful act. Fraud is a narrower category that involves deception for wrongful gain within a larger category. Deception through online platforms like mobile, apps, internet banking, payment apps, social media, emails, telecom channels, etc. is generally termed as cyber fraud. Fintech fraud is an even narrower category of digital fraud. It encompasses fraud relating to technology-enabled financial services, such as UPI, mobile wallets, cards, internet banking, payment gateways, and digital onboardings like digital lending and other app-based financial services. According to concepts, this relationship can therefore be explained: Cybercrime → Fraud → Digital Fraud → FinTech Fraud. This hierarchy is significant as it indicates that all FinTech frauds are digital frauds, but not all digital frauds are FinTech frauds.

For this study, the conceptual distinction is necessary because the India fraud environment includes many digital wrongs which do not directly involve fin-tech systems. Cart fraud in e-commerce spectrum may peg it as the digital fraud

category. But it can only be classified under FinTech fraud when it deals with digital financial products like payment, app-based financial service systems. On the contrary, scams that include fake phone calls for UPI collect requests or QR code scams, card not present fraud, fake loan app fraud etc. fall within the purview of FinTech fraud. Reword (30 words.

This distinction assists in setting the limits of the research and ensuring the investigation remains focused on fraud related to financial technology systems and not on digital wrong-doing in general.

Difference Between Digital Fraud and FinTech Fraud

Digital fraud is an umbrella term that includes all kinds of scams carried out via digital means. Anything that misleads people online can be considered cyber fraud. It includes fake websites, social media fraud or impersonation, account compromise, scam messages or anything misleading in the digital space. Digital fraud primarily involves one major activity, which is the use of digital means to deceive. FinTech fraud is, however, a more exact category because it references systems and digital financial services. It relates to movement of money, financial accounts, digital payment instruments, internet banking or digital credit platforms and app-based finance. Put differently, the underlying system or platform is the one that has a financial nature.

This difference can be explained easily. A product listing that is fake and designed for cheating a buyer digitally constitutes cyber fraud, but not necessarily FinTech frauds. Conversely, when a fraud involves UPI payment request, a bank call seeking to capture OTP, a phishing link seeking internet banking credential, misuse of card details, or a banking lending app. On the contrary, this is a FinTech fraud as it exploits the digital financial infrastructure. The importance of this difference for the present research is that the study does not cover all digital frauds. It focuses on frauds that occur through payment systems, banks, lending apps and other related Indian financial platforms instead.

Broad Classification of FinTech Frauds in India

As per the study, FinTech frauds in India may be broadly classified into four major types: social engineering frauds, technical frauds, identity frauds and transaction or platform-based frauds. This classification is useful as it confines the frauds not only by the mechanism through which the fraudster succeeds but also by the channel through which it occurs. The four categories have already been identified in the draft along with the common Indian fraud scenarios such as phishing, vishing, QR-code fraud, SIM-swap fraud, account takeover, fake KYC updates, fake loan apps, and mule account.

Frauds using social engineering are reliant on psychological manipulation rather than technical infiltration. In these situations, the fraudster misleads the victim into providing ID or card details, making a payments or approving a payment. Common types of scams include phishing, vishing, smishing, impersonation fraud, fake customer-care calls, and refund scams. In contrast, technical frauds are more reliant on device compromise, software misuse, or security weaknesses. The scams are based on malware, remote-access apps, SIM swap scams, account takeover, credential theft, and device breaches. Crimes related to the wrongful use, theft, creation or appropriation of identity and KYC-related information due to misuse of Aadhaar, PAN, mobile numbers or fake-document based onboarding. Lastly, financial transaction systems and financial platforms directly cause transaction and platform-based frauds, which include UPI scams, QR-code fraud, card fraud, internet banking fraud, card-not-present fraud, fake loan-app fraud, and routing of stolen funds through mule accounts.

Seeing social engineering as a cross-cutting mechanism is a useful way to understand this classification. Fraudsters may contact victims through calls, SMS messages, WhatsApp, or fake support identities, to drive a sense of urgency, fear, trust or confusion. Such manipulations can easily be employed in UPI fraud, e-banking fraud or digital lending fraud. The categories mentioned are analytically distinct, however, in practice, many fraud events overlap human manipulation, technical compromise, and platform misuse. FinTech fraud in India cannot be addressed effectively through a narrow approach that focuses only on products.

1.2 Complexity in FinTech Frauds

Fraud in the FinTech sphere in India is difficult to tackle because it does not arise from one method, one channel, or one type of offender. This includes frauds by the use of UPI and QR codes and social engineering attacks like phishing and vishing. Further frauds take place through account take over, malware-based banking fraud, mule accounts to transfer stolen money and fraud risk in app-based digital lending (Debnath and Chakraborty 2025; Mishra and Singh 2025; Ali and Marisetty 2023).

Another layer of complexity is added by the technology stack and design choices inside payment apps, as well as in the underlying payment infrastructure. An analysis of UPI-based payment apps by security researchers highlights that the large-scale deployment of such applications must give due consideration to design and implementation flaws, as small loopholes would become large-scale problems once millions of users come on-board (Kumar et al., 2020).

Cybercrime is unauthorized activity in a computer system or the internet against the law. As per Indian Reporting Framework, cybercrime data are compiled from offences under Information Technology Act, relevant sections of Indian Penal Code and Special and Local Laws. According to the NCRB, the revised proforma was utilised from the year 2014 onwards for data collection.

Fraud is an act of deception for wrongful gain. When this kind of deception takes place through online platforms, mobile devices, payment applications, internet banking, social media, telecom channels, etc., it is termed digital fraud. FinTech frauds are a subset of digital frauds. Fraud associated with technology-enabled financial services like UPI, mobile wallets, internet banking, payment gateways, cards, digital lending apps, app-based financial platforms is called cyber fraud.

Consequently, the relation can be expressed as.

Cybercrime → Fraud → Digital Fraud → FinTech Fraud.

This is a critical distinction as all FinTech frauds are digital frauds, but all digital frauds are not FinTech frauds. Fraudulent practices involving the misuse of financial technology systems, digital payment instruments, digital onboarding, and/or financial service platforms are termed as FinTech frauds.

1.3 Technology as a Game Changer in Fraud and Fraud-Prevention

FinTech fraud is a story of technology enabling fraudsters and institutions using technology to counter fraud with technology. Fraudsters can now scale their social engineering attacks with impunity, or use spoofed identities and phishing links to defraud victims. Similarly, the speed of real-time payments reduces the chance of catching fraudsters. Phishing and vishing studies explain that fraudsters rely on manipulation and impersonation to invoke immediate user action (Debnath & Chakraborty, 2025).

In India, the proliferation of smartphones, cheap internet, UPI, app-based banking, and digital lending has increased access to financial services, but it has also increased the surface for fraud. The cybercrime chapter of NCRB for 2015 stated that there were 11592 cybercrime cases, up from 9622 in 2014. It described that cybercrime is one of the classes of offence that is increasing rapidly.

According to Indian banking regulator Reserve Bank of India (RBI), it is becoming evident... Appendix Table IV.7 of the Trend and Progress of Banking in India 2023-24 states that RBI reports 845 card/internet fraud cases in 2014-15 and 29,082 cases in 2023-24; for 2024-25 (till Sep. 2024) it reports 13,133 card/internet fraud cases. The Reserve Bank of India also warns that reporting dates are used to record frauds, and, therefore, some frauds may have occurred earlier than the reporting year.

Growing scale and changing form show the increasing cyber-enabled financial fraud in India. The types of frauds that happened earlier were mostly related to cards and basic internet banking. However, recent fraud patterns are increasingly showing up in UPI, impersonation scams, QR-code fraud and others. In others are mobile-based remote-access

manipulation, fake loan apps, account takeover, and mule-account usage. In the Indian context, it is necessary to conduct a systematic study of FinTech frauds.

1.4 Bridging Gaps in Research and Practice

There is often a divide between what researchers recommend and what users actually use when becoming a fraud victim. Research offers systems such as improving consumer awareness, designing better security controls, strengthening reporting processes and data-driven monitoring. As an illustration, a consumer preparedness study that defines preparedness as knowledge, protective actions and responsiveness demonstrates how fraud prevention is not just 'knowing' the risk but also building habits and response actions (Lonkar et al., 2024).

1.5 Strategic Importance of This Research

This research is strategically important because FinTech fraud is a public trust problem, not just a private loss. When individuals experience fraud and lose money without getting timely recovery assistance, their usage of digital may decline. Such behaviour can impede financial inclusion and undermine trust in systems that are designed to make finances easier. According to regulatory frameworks (RBI, 2024).

CHAPTER: 2 LITERATURE REVIEW

Kumar, Kishore, Lu and Prakash (2020) studied how attackers can exploit the UPI ecosystem by examining the interfacing between a payment app and the UPI protocol. The "sample" in their work is primarily technical: they reverse-engineered seven popular UPI apps and evaluated authentication and protocol design choices rather than surveying a large population. The duration is not framed as a time-bound field study, but as a systematic security analysis phase. The main factors include protocol flows, authentication steps, application behaviours, and threat scenarios.

Santhosh and Parvatikar (2024), investigate the growing incidents of UPI and digital-payment frauds and suggest improving transaction integrity and traceability by employing AI-based anomaly detection along with blockchain enabled smart-contract mechanisms. They don't typically use surveys and their work is more conceptual and solution-oriented. So, sample size and duration are not important in the traditional empirical meaning. The importance of the study is shown in key fraud indicators like phishing, skimming and account takeover. Technological controls are also highlighted as a means to prevent fraud. This literature is important for understanding the fraud risks associated with digital payment systems and the application of advanced technological tools for mitigation.

Priya, Ahmed and Alam (2020), on Indian banking sector, fraud data in the banking system should be collected, shared and used through an institutional process instead of a loss after the event ad response. Their work doesn't rely on field research that is survey-based but documentary and process-led. The significance of the study lies in its treatment of fraud management as an information and governance issue. Data has shown that effective fraud prevention is not only dependent on detection, but also how fraud-related information is recorded, integrated, and used to respond institutionally. The current study is particularly useful to the present research as it suggests the need for systematic fraud registration in consideration of evidence.

Sharma and Singh (2024) highlighted cyber fraud risk in the digital payment ecosystem of India. The authors stated, how regulatory responses and delayed reporting skew the 'true' year-wise picture. Because their work is mainly doctrinal/descriptive instead of a field experiment, the sample size does not apply and the duration is based on the regulatory and secondary sources from which they derive. Four key variables are fraud categories in digital payments, delay in reporting, regulatory control and impact.

Debnath and Chakraborty (2023) Phishing and vishing attacks are two evolving threats in the Financial Technology workplace. Their study is particularly useful because it demonstrates that many frauds are not due to direct technical breach, but rather to social engineering through fear, urgency, trust manipulation and impersonation. The work is descriptive and analytical rather than empirical in the sense of conducting survey-based research. Further, it uses reported incidents and interpretive discussion to explain how these attacks work. This study is very relevant to the present one as

it explains why social engineering should be considered a crosscutting fraud mechanism across payment fraud, e-banking fraud, among other FinTech-related frauds.

Ramesh, Wang, Sambasivan, and Kameswaran 2022, Study in qualitative terms the instant loan platforms in India, focusing on the power relations between platform and users and issues of accountability. Based on 29 semi-structured interviews, their study demonstrates how users' access practices, recovery strategies, and algorithmic control can put financially stressed users in a vulnerable situation. The significance of this study is that fraud and harm in digital lending cannot always be grasped using only technical security models. Instead, harmful outcomes are shaped by platform governance, weak accountability, and user vulnerability. The fact makes the study very pertinent to the ecosystem-vulnerability dimension of the present essay.

Ali and Marisetty (2023) The objective is to check whether FinTech lending apps in India are harmful by analyzing a sample of 2.19 million user reviews for approximately 110 apps in the Google Play ecosystem. In their work users' experience is compared across periods (pre-COVID and COVID). They identify the recurrent themes of harassment, privacy concerns, overcharging, and other indicators of consumer harm. A large-scale text analysis and quantitative modelling is used to detect patterns in complaints. This is particularly important for the present study because it shows that forms of fraud and harm related to lending reflect not an isolated but are persistent in repeated scale in user experience data, thereby broadening the scope of FinTech fraud beyond payment and banking frauds.

Afzal, Ansari, Ahmad, Shahid and Shoeb (2024) The study of the relationship between cybersecurity awareness and users intention to continue using e-banking. According to 428 surveys, the study is cross-sectional and largely focuses on cybersecurity knowledge, awareness, behavioural protection and technology-acceptance related factors, and more. The authors utilized covariance-based SEM to validate that awareness and protective behaviour have a significant impact on confidence in e-banking channels. This study is relevant because it connects fraud risk not only to technical threats but also to user awareness and behavioural preparedness thereby enhances user-vulnerability dimension of the present research.

Mishra and Singh (2025), Phishing, SIM swapping, malware-based attacks, identity theft, and social-engineering-based frauds are a few e-banking frauds in India that need a critical analysis. Their work is based more on secondary discussion of cases and regulatory issues rather than the primary data obtained by means of empirical fieldwork. The study is useful because it identifies recurrence of frauds in e-banking and highlights the importance of real-time reporting, stronger grievance redressal and better coordination between customer-side precautions and institutional controls. This literature directly aids the present study in elucidating how e-banking frauds operate and why they continue to be relevant within the wider FinTech fraud environment.

Lonkar, Dharmadhikari, Dharurkar, Patil and Phadke (2024), Examine consumer readiness regarding digital payment frauds in India. The authors of the study identify preparedness as a multidimensional concept consisting of awareness, protection practices, and responsiveness, after a fraud. After analysing the study data from, a sample of 372 consumers using PLS-SEM, preparedness should be viewed as a capability that can be developed through education, precautionary behaviour and clear posts-fraud response actions, reporting, freezing and escalation. Keep it up! Your answer is too short, try to write more relevant.

Rohilla (2024) gives an overview of the legal issues concerning the electronic payment systems in India, the role of regulators, consumer protection and dispute resolution. Sample size and duration are not applicable. Key variables include legal provisions, liability allocation, compliance requirements and enforcement gaps. Fraud analysis relies on legal interpretation as well as policy review. Recommendations often stress clearer liability rules, better compliance monitoring, and faster dispute resolution processes to restore confidence when fraud occurs.

Aziz and Dowling (2019) create a larger structure for the application of machine learning and artificial intelligence in risk management. Though the research is not specific to India and does not study FinTech fraud exclusively, it is conceptually useful as it illustrates how data-driven models can aid risk detection, monitoring and decision-making in uncertainty. The framework emphasizes challenges regarding risk signals, model performance, interpretability, and operational challenges. As already stated the present paper is more a methodological reference for fraud detection and risk-management logic than a direct source on the nature of Indian FinTech frauds.

Research Questions

- What are the different types of FinTech frauds that are commonly reported in India?
- How can these FinTech frauds be classified into clear categories (UPI/digital payments, e-banking, and digital lending/loan apps)?
- How have FinTech fraud incidents in India changed over the years, and what year-wise patterns can be observed?

Research Gap

The literature on FinTech fraud in India reviewed here provides useful insights; however, it is fragmented when examined with regard to the three objectives of the present study. Many existing studies focus on either UPI and digital payments, e-banking, or digital lending, which fail to integrate the three domains into a larger FinTech fraud framework. Another limitation is being overly focused on identifying fraud risks, awareness issues or technological vulnerabilities rather than explaining the year-on-year changes in frauds and fraud patterns. According to literature, definition of fraud varies significantly between studies. Some studies look at unauthorized appropriation of financial incentive. Others, however, take a much wider focus on well-being of entire platform. This results in matters such as psychological harassment, misuse of private information and exploitative practices to recover loss. Comparing studies is made difficult by the diversity of technical security analysis, surveys, app-review mining, legal analysis, etc., they use. The current study attempts to combine growth classification, trend interpretation and ecosystem-vulnerability mapping into one India-centric analytical framework for the aforementioned limitations.

The literature often splits on product type, which is one of the largest gaps. Most studies that focus on payment stayed within the UPI and digital space. Kumar, Kishore, Lu and Prakash (2020)'s UPI security work helps understand security design weaknesses and application-level risks in technical depth and is a valuable addition. However, this particular kind of technical work does not correlate automatically with what the digital lending studies are showing. Difficulties in the lending-app area aren't just a case of technical loopholes. Difficulties in governance of the platform, users' vulnerability, and patterns of harm observed at scale in users' experience. According to Ali and Marisetty (2023), there are about 2.19 million Indian reviews for lending-apps in the dataset and that fraud-related negative experiences closely appear in pattern and not some isolated complaints. Ramesh et al. (2022) provide another perspective on power imbalance and accountability gap, this time focusing on how these shape the outcomes for financially stressed users.

Another gap is how many papers clarify the problem, but do not go on to build a strong bridge between awareness and security design. Many studies identify problems and make suggestions such as "better security" or "more awareness". These suggestions are certainly not wrong. However, they tend to be vague. Debnath and Chakraborty (20225) state that finally, this days devastating phishing and vishing scams manage to get work done with fear umpiring, urgency creating and trust manipulating. According to Mishra and Singh (2025), cybercriminals execute different kinds of frauds on customers such as phishing, SIM swapping, malware and social engineering attacks. Also, the weaknesses of the consumers in response to the e-bank frauds are discussed. In short, the major thefts of the modern age do less to break technology and far more to break decision-making. Meanwhile, studies focused on preparedness Lonkar, Dharmadhikari, Dharurkar, Patil and Phadke (2024) measure preparedness in 372 consumers and break it into three factors that are awareness, protection and responsiveness.

There is a third gap around year-on-year trends, which is one of your objectives. A small part of the 20-paper set does not really support a strong "trend chapter" in the sense of what is changing year on year and why. A lot of papers mention that fraud is increasing while adoption is increasing. However, they do not show detailed year-wise pattern logic. It is not always the researchers' fault; often open and reliable datasets are hard to come by. As a result there is a gap. Technical security studies such as Kumar et al. (2020) focus on design vulnerabilities rather than time series movement. Further, ML-based fraud-detection papers such as Shruthi M K et al. (2025) and Kavitha et al. (2024) propose a method of detection. But they do not connect the design of the model to how fraud patterns change historically over the years. While studies, such as Ali and Marisetty (2023) and Lekshmi et al. (2025), on the review of lending apps may compare periods (for instance, pre-COVID versus COVID) and demonstrate how themes within complaints evolve through time, these insights are not fully translated into a trend map at the national level which differentiates payment fraud, e-banking

fraud and digital lending abuse under one storyline. So the research gap here is the absence of a well-accepted method of evidence blending for credible year-wise pattern analysis.

Certain papers say fraud is mainly unauthorized or deceptive financial loss. Other papers expand the meaning to cover platform harm, invasion of privacy, coercive recovery tactics, and exploitation. A technical paper on payment security and research on harm from lending have been compared. The difference is stark. Fraud in the lending ecosystem is often experienced as misleading, illegal lending, harassing, or misuse of permissions. Fraud experience may not fit into banking fraud reporting categories always. In the paper loan-app misery, Saritha (2023) argues that potentially harmful effects may be systemic, in that, they occur even when users agree to the terms at the hardware or software stage.

A different gap consists of the fact that the methods used in the 20 papers are radically different and not always "speaking the same language." Some are technical security studies, such as Kumar et al. (2020). According (to Ali and Marisetty, 2023; Lekshmi and others, 2025. To app reviews text mining is used on a large scale. According to Milana, Sarawagi, and Das, a legal or doctrinal (Mishra & Singh, 2025; Rohilla, 2024). All techniques are useful, and each measures different things. This makes it difficult to integrate their findings into one complete picture. Surveys measure awareness but may not keep pace with rapid scams. Review mining helps capture harmful signals but risks conflating fraud and discontent. Security analysis shows design gaps but may not show user behavior. In legal research, it is said what one must do, but it does not show how fraud occurs in actual user flows.

The existing research on FinTech frauds in India is valuable, but it remains fragmented when viewed from an ecosystem perspective. Most studies examine fraud within a single product space—such as UPI and digital payments, e-banking channels, or digital lending and loan apps—without building a unified framework that connects fraud mechanisms across these linked financial pathways. In addition, the literature does not consistently provide strong year-wise or historical pattern explanations, largely because many studies are not designed around time-series evidence and because open, standardized datasets are limited. Another gap lies in the absence of a common definition and classification of "FinTech fraud," as some works focus mainly on unauthorized financial loss while others include platform harm such as privacy misuse, harassment, or exploitative practices, making comparisons and aggregation difficult. Finally, many papers recommend broad actions like improving awareness or strengthening security, but fewer studies clearly map where the fraud chain breaks across stakeholders (users, apps, banks, telecom systems, platforms, and regulators) and who should take responsibility for fixing specific weak points through targeted interventions.

Research Objectives

Objective 1: Identify and categorize the main types of FinTech frauds reported in India.

Under this objective, the research will give an account of the major types of FinTech frauds reported in India and classify them. The research would deal with the frauds happening in UPIs and digital payments, e-banking channels and digital lending or loan-apps. It will look at the common methods used by the fraudsters such as phishing, vishing, fraud Customer-care calls, QR-code scam, collect-request scam, SIM-swap fraud, malware, fake loan app, misused identity, account takeover, etc. In order to achieve the objective, the study will review the notable literature and extract the type of fraud, channel, and modus operandi from each article. The frauds, then, will be further consolidated into wider heads such as social engineering frauds, technical frauds, identity-related frauds and transaction or platform-related frauds. This classification aims to link the type of fraud, with the channel through which it perpetrated, and the means with which it performed successful.

Objective 2: To analyze the historical trends and year-wise patterns of various FinTech fraud incidents in India.

The study will look at how FinTech fraud incidents in India have changed over time, and what are the year-wise patterns that can be identified from available secondary evidence. The research will examine whether the growing use of digital payments, internet banking, cards, and app-based lending has led to an increased number of frauds. In this context, the research will utilize the available official and other secondary sources for the non-governments to trace trend indicators for the last several years. The statistics would include data on cybercrime cases, card and internet fraud and other categorically available evidence regarding UPI frauds, phishing-based payment frauds, QR-code frauds, loan-app frauds and identity-based misuse. The study will arrange this evidence in a structured year-wise manner to enable the systematic

interpretation of changes in scale, concentration and pattern. The goal here is to throw some light on the trend of FinTech fraud in India, relating it with the growth of a digital financial ecosystem.

Objective 3: To explore the key vulnerabilities within the FinTech ecosystem that may lead to the risk of FinTech frauds.

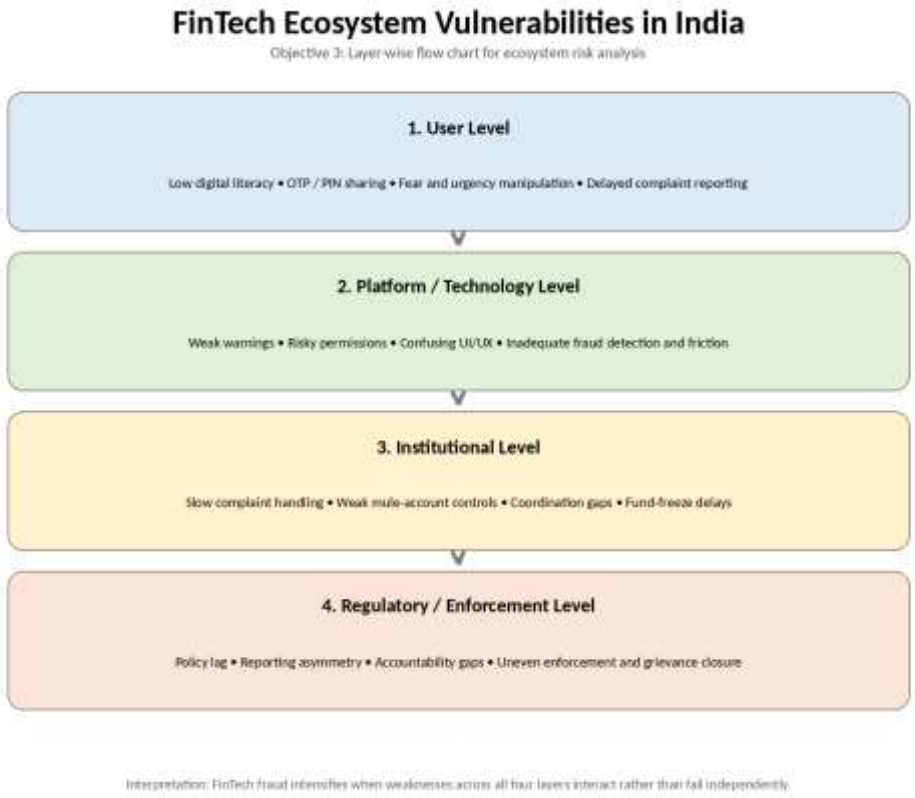


Figure 1 objective 3 flow chart

The research will determine the key weaknesses in FinTech's ecosystem that lead to fraud and allow it to continue under this objective. The study will analyse the FinTech fraud as an ecosystem rather than a disruption of technology. So, the goal of the study is mapping vulnerabilities at four interconnected levels: user level, platform or technology level, institutional level, and regulatory or enforcement level. At the user level, the study will investigate issues low awareness, unsafe credential sharing, weak response habits, and delayed reporting. It will examine interface confusion, weak warnings, risky permissions, design flaws and poor fraud detection at platform and technology level. It will look into complaint-handling delays and weak mule-account controls at the institution level, as well as poor escalation mechanisms and coordination failures. It aims to assess reporting gaps, accountability problems, delayed responses and difficulties in responding to the rapidly changing modus operandi of frauds at the level of regulation and enforcement. The aim is to create a layered map of vulnerabilities illustrating how different weaknesses combine to contribute FinTech fraud risk in India.

Scope of Study

This study continues to focus primarily on FinTech frauds reported in India but takes a sufficient overview of the major FinTech touch points where frauds have often been covered in literature. Digital space of Finance which covers 3 main FinTech sectors- (i) payment systems which cover UPI and payment apps, (ii) e-banking channels which include internet banking and mobile banking, and (iii) Digital Lending and instant loan apps. The selection was intentional and based on evidence. That is, evidence in the research papers themselves shows that fraud and harm are visible across all three. Also, users view them as part of one inter-connected financial life.

In terms of digital payments, UPI Security and Payment App studies cover the types of risks that fall within scope. According to Kumar et al. (2020), it is necessary to study the underlying protocol and how the apps implement the

security flows. This is because weaknesses can arise due to design assumption, authentication behaviour or implementation raid. Essentially, fraud methods covered here include those related to payment applications, authentication misuse, transaction manipulation, and user-authorised scams that are facilitated by the speed of settlement and confusing prompts for users.

The e-banking literature highlights the fraud types and behavioral risk that is within e-banking. Afzal et al. (2024) focus on the connection of cybersecurity awareness and protective behaviour with users' intention and confidence in using e-banking services shows how risk of fraud. Papers written in the "critical analysis" style on e-banking frauds deal with phishing, SIM swapping, malware, and social engineering frauds among others. These are quite common frauds cropping up in the same ecosystem. The reason why these frauds continue to remain relevant is simply that they are used to breach or distract users.

So, what does this fraud analysis cover? This fraud analysis considers the fraud mechanisms and user-side and bank-side factors that can make fraud more likely to succeed. Within the ambit of digital lending, not only do we scope platform level harm, but also what we term fraud-like practices that get captured in user experience and accountability studies. Ali and Marisetty (2023) show that fraud-related complaints revealed in large-scale user review data constitute a meaningful share of negative experience. We suggest that fraud in lending gets experienced as deception, abusive practices, and exploitative platform behaviour by users.

Ramesh and co-authors (2022) study extends the accountability literature by showing how financially stressed users can be nudged into risky choices and unfair terms, thus revealing vulnerabilities that the technical fraud detection models may not capture. The research therefore considers lending-related fraud risk to be a confluence of platform governance issues, consent and privacy risks, and user vulnerability.

This study's scope also clearly shows social engineering fraud to be a cross-cutting category as literature clearly states that scammers often succeed as a result of manipulation of human behaviour and not software. Within the scope, Debnath and Chakraborty's work on phishing and vishing is used to explain how impersonation and psychological manipulation are becoming central to contemporary FinTech fraud. According to a report released today, social engineering is not seen as an 'additional topic' but as the key binding mechanism for payment fraud, banking fraud and lending fraud.

Simultaneously, at the same time, the study has clear boundaries in order to keep it academically workable within the chosen evidence base. This report does not carry out new penetration testing or reverse engineering beyond what publicly available security research offers, and it does not claim access to confidential transaction-level banking data. It draws conclusions from published studies together with documented evidence and validated research findings.

CHAPTER 3: RESEARCH METHODOLOGY

3.1 Introduction

The current research employs a study of secondary data and a systematic study of FinTech frauds in India. As the topic of interest is already extensively documented in the existing literature (research articles, official reporting systems, and regulatory papers), and as detailed fraud datasets at the transaction level are not available in the public domain for a direct primary investigation, this approach is considered to be appropriate. As a result, instead of undertaking a new survey or field study, the research makes use of existing evidence to understand the nature of FinTech fraud in India, its trend and vulnerabilities unique to the ecosystem.

The study objectives are directly addressed and aligned in the methodology. To this end, the fixed set of 20 selected research papers is used as core evidence. The papers span UPI and the security of digital payments, fraud in e-banking and awareness of consumers, digital lending and loan-app related harms, and legal-regulatory issues. In addition to these sources, official secondary reports and records have been used as necessary to establish a year-wise pattern and level of ecosystem fraud risk.

The study doesn't involve collection of primary data so the research process is a structured review, comparison and interpretation of available evidence. The methodology aims to ensure a clear classification of categories of fraud while also acting as tools to trace broader fraud trends through available indicators and cataloguing the major vulnerabilities

that cut across user, platform, institutional and regulatory levels. Therefore, the chapter discusses how secondary data has been chosen, organized, and analysed in a manner that meets the overall objectives of the study.

3.2 Research Design

The design of the research is descriptive and analytical. It is descriptive as first fraud types and their classification in Indian FinTech were explained. The review is analytical because it compares study findings, links fraud types to vulnerabilities, and employs available secondary information for an interpretation of year-wise patterns.

3.3 Data Collection Methodology

Data is collected via a structured extraction mechanism so that each research is captured uniformly. Each document is read and information is listed under fixed headings, which are author/year, study focus, sample size and duration (if reported), key variables, tools used by authors, findings and recommendations.

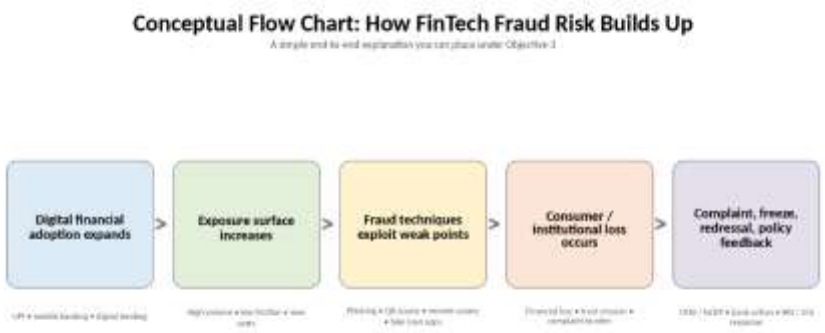
3.3.1 Survey Instrument

This research relies on previously collected secondary data and does not carry out a fresh field survey. In this report, the "survey instrument" refers to a data extraction sheet that is used for taking information from the researched paper and official source. The extraction sheet is a very handy tool. It acts like a checklist and ensures that the same information is taken from every paper. Further, it is done in a consistent and unbiased manner.

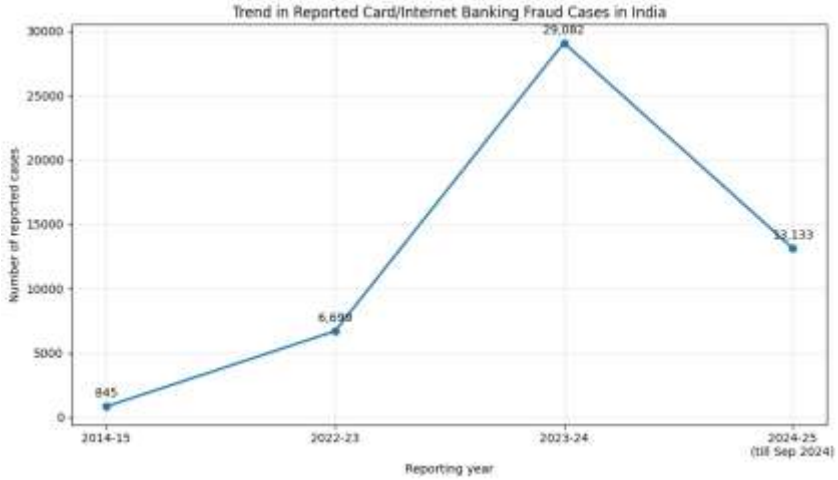
3.4 Sampling Technique and Sample Size

This is secondary data based research, hence sampling is purposive. The chosen set of 20 research papers together covers UPI and digital payments, e-banking frauds, digital lending/loan-app risks, consumer preparedness, and legal/regulatory aspects. We selectively include official documents wherever useful for an understanding of the year-wise trend and ecosystem response.

3.5 Conceptual Framework



3.5.1 Data Analysis Framework



Content analysis is applied to create a classification of FinTech frauds in India for Objective 1 (Fraud types). The documents' fraud descriptions are being coded into categories (payments/UPI, e-banking and lending/loan-app related fraud and harm, social engineering as a cross-cutting mechanism. A single fraud classification scheme with respect to Indian scenario.

Mapping vulnerabilities related to Objective 3 (Ecosystem vulnerabilities) is carried out in layers. Vulnerabilities arise at the level of consumers (awareness, risky behaviour, delayed reporting), at the level of the platform/technology (design gaps, weak controls, risky permissions), at the institutional level (process gaps, grievance and response delays, coordination issues) and at the regulatory/market level (oversight gaps, enforcement lag, accountability issues).

3.5.1 Statistical Analysis Using SPSS

The primary goal of SPSS is to analyse and present patterns from the literature review. It can produce frequency tables and cross tabulations, e.g. how many studies address each fraud category, which methods dominate the literature (survey, technical, qualitative, text analytics) and which vulnerabilities themes get most frequent mention.

3.6 Ethical Consideration

This research is based on secondary sources and thus will not collect personal data such as bank details, phone numbers, OTPs and private case records. The manner in which the research is constructed and framed emanates from not blaming the victim or victims. Many frauds are successful not just because the offender is clever but also because the failure is at the level of the system. The findings have been reported in the form of themes and patterns, not identifying individuals. The aim of the study is also to represent each paper correctly without distorting the meaning of the conclusions drawn by the authors.

3.7 Summary of Research Methodology

Research Design	Descriptive + Analytical design. Descriptive = classifies fraud types. Analytical = compares findings across studies and links fraud types with vulnerabilities and trend signals.
Data Collection Methodology	Data collected in two parts: (1) 20 research papers extracted in a standard format, (2) select official secondary reports/records used only to support trend and ecosystem context.
Survey Instrument	No primary survey is conducted. The "instrument" is a data extraction sheet (coding format) used to record uniform details from each paper/source.
Sampling Technique and Sample Size	Purposive sampling. Sample = fixed set of 20 research papers (core dataset). Additional official sources included only when necessary for trend and ecosystem response understanding.

Data Analysis Framework	Three-step analysis: (1) Content analysis to classify fraud types, (2) Trend interpretation using available time-linked evidence and reporting indicators, (3) Vulnerability mapping across consumer/platform/institution/regulatory layers.
Statistical Analysis Using SPSS	SPSS used for descriptive summaries: frequency tables (study types, fraud categories), cross-tabs (fraud type × vulnerability layer), and theme counts across papers. No advanced modelling.

CHAPTER 4: OBJECTIVE-WISE DATA ANALYSIS AND INTERPRETATION

4.1 Introduction

This chapter presents an objective-wise analysis of FinTech frauds in India by combining the conceptual framework of the study with the empirical signals available in the uploaded data file. The quantitative evidence is drawn from RBI payment system indicators and domestic payment fraud statistics contained in the provided dataset. The chapter therefore uses the data in two ways: first, to explain the scale and concentration of India's digital payment ecosystem; and second, to interpret how that expanding ecosystem creates a larger exposure surface for payment-related fraud.

Because the uploaded dataset is strongest on payment systems, the numerical analysis is most detailed for Objective 2 and partly for Objective 3. Objective 1 is addressed through an analytical classification table that aligns the major fraud types discussed in the paper with their channels and modus operandi. Throughout the chapter, the interpretation remains tied to the paper's three objectives: classification of frauds, identification of year-wise patterns, and mapping of ecosystem vulnerabilities.

4.2 Objective 1: Classification of major FinTech frauds reported in India

The first objective is to identify the major types of FinTech frauds reported in India and classify them in a way that connects the fraud to its delivery channel and operating method. Based on the conceptual framework and reviewed literature in the paper, the frauds can be consolidated into four broader analytical heads. Table 4.1 summarises this classification.

Broad head	Main channel(s)	Typical modus operandi	Analytical meaning
Social engineering frauds	UPI / digital payments, e-banking, cards, lending apps	Phishing, vishing, fake customer-care calls, collect-request fraud, refund scam, QR-code deception, impersonation	Victim is induced to disclose OTP/PIN, click a link, approve a collect request, or scan a malicious QR code.
Technical frauds	E-banking, cards, mobile devices, telecom-linked channels	SIM-swap, malware, remote-access apps, credential theft, account takeover	Attackers exploit device compromise, telecom substitution, or weak authentication to seize control of the account.
Identity-related frauds	Digital onboarding, KYC, lending apps, banking channels	Misused identity, fake KYC update, Aadhaar/PAN misuse, synthetic or stolen credentials	Personal identity data are misused to open, access, or misuse financial accounts and credit facilities.
Transaction / platform-related frauds	UPI, payment apps, cards, lending platforms	Unauthorized transfers, card-not-present fraud, fake loan apps, mule-	Fraud leverages the transaction flow or platform design itself, often after social

		account routing, deceptive app permissions	engineering or identity misuse.

Source: Author's analytical classification based on the study objectives and reviewed literature discussed in Chapters 2 and 3.

Interpretation: The classification shows that FinTech fraud in India is not confined to a single product or a single trick. Social engineering cuts across nearly every channel because users are persuaded to share credentials or authorise the transaction themselves. Technical frauds become more relevant where the attacker must bypass authentication or compromise the device, such as SIM-swap and malware-linked e-banking incidents. Identity-related frauds matter especially in digital onboarding and lending contexts, where KYC data can be misused. Transaction or platform-related frauds reflect misuse of the payment or lending architecture itself, such as collect-request scams, card-not-present fraud, fake loan apps, and mule-account routing.

4.3 Objective 2: Historical trends and year-wise patterns of FinTech fraud indicators

The second objective examines how FinTech fraud indicators have evolved over time. The uploaded data file provides two useful types of evidence: retail payment system growth and monthly domestic payment fraud statistics. Taken together, they help explain both the expansion of the digital financial ecosystem and the parallel rise in exposure to payment-related fraud.

4.3.1 Growth in major retail payment channels

Table 4.2 compares selected retail channels between October 2023 and October 2024. The comparison highlights where transaction volume is growing fastest, where transaction value is concentrated, and where average ticket sizes remain large enough to attract targeted fraud.

Channel	Oct 2023 volume (lakh)	Oct 2024 volume (lakh)	Volume growth %	Oct 2023 value (Rs crore)	Oct 2024 value (Rs crore)	Value growth %	Avg ticket Oct 2024 (Rs)
UPI	114087.90	165849.66	45.37	1715768.00	2349821.00	36.95	1416.84
NEFT	6314.53	9183.38	45.43	3262015.00	4152428.00	27.30	45216.77
Card Payments	5104.71	5774.01	13.11	230670.00	248709.00	7.82	4307.39
IMPS	4928.80	4668.23	-5.29	538239.00	629382.00	16.93	13482.24
Credit Cards	3200.48	4332.14	35.36	178569.00	201789.00	13.00	4657.95
APBS	1745.79	4021.91	130.38	19666.00	69157.00	251.66	1719.51
Debit Cards	1904.23	1441.87	-24.28	52101.00	46920.00	-9.94	3254.11

Source: Computed from uploaded Data.csv (RBI payment system indicators, retail payment channels).

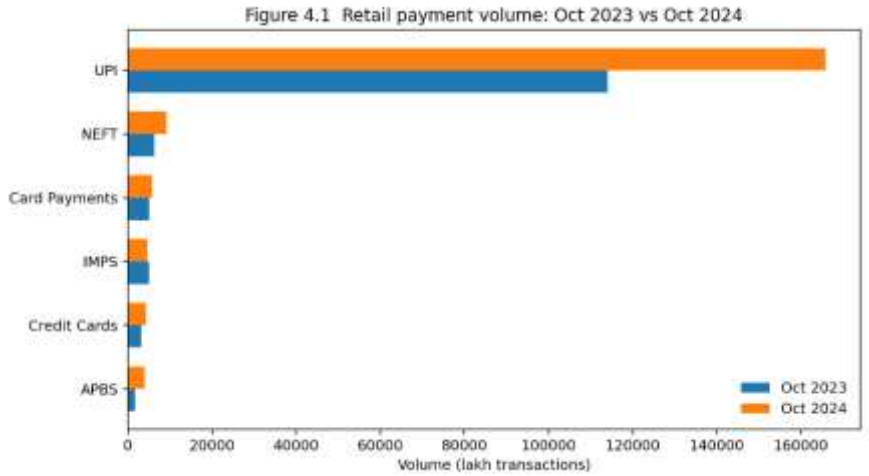


Figure 4.1 Retail payment volume in major channels: October 2023 versus October 2024

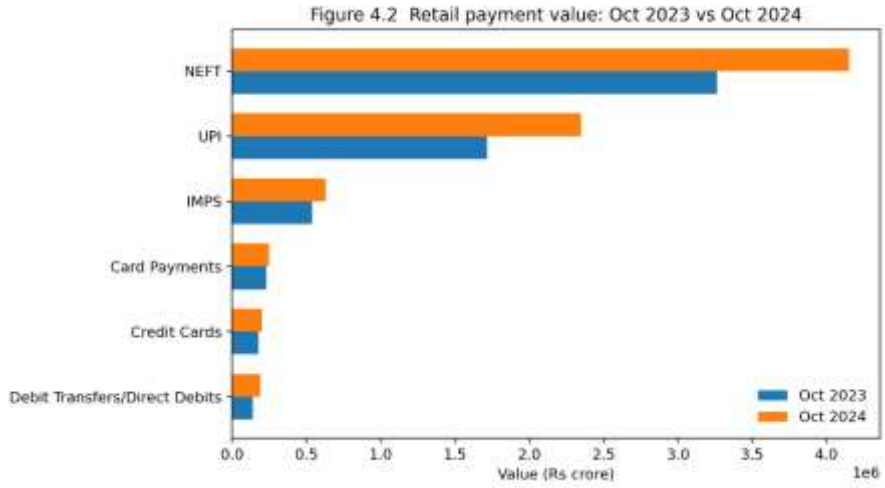


Figure 4.2 Retail payment value in major channels: October 2023 versus October 2024

Interpretation: The data show strong expansion in digital payment usage. UPI rose from 114,087.90 lakh transactions in October 2023 to 165,849.66 lakh in October 2024, a growth of 45.4 percent. NEFT increased by 45.4 percent and card payments by 13.1 percent over the same period. The value side also expanded, with UPI value increasing from ₹1,715,768 crore to ₹2,349,821 crore.

These numbers indicate that fraud risk must be read together with adoption. UPI has the lowest average ticket size among the major channels in this comparison, at roughly ₹1,417 per transaction, but its massive scale makes it especially suitable for high-frequency social-engineering frauds. By contrast, NEFT and IMPS carry much larger average ticket sizes—about ₹45,217 and ₹13,482 respectively—which means fewer successful breaches may still produce substantial losses.

4.3.2 Channel concentration and infrastructure deepening

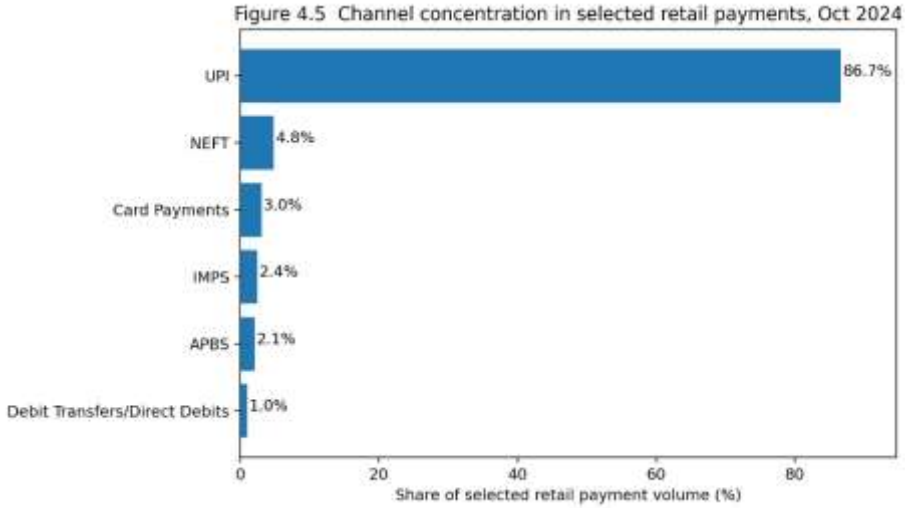


Figure 4.3 Share of selected retail payment volume in October 2024

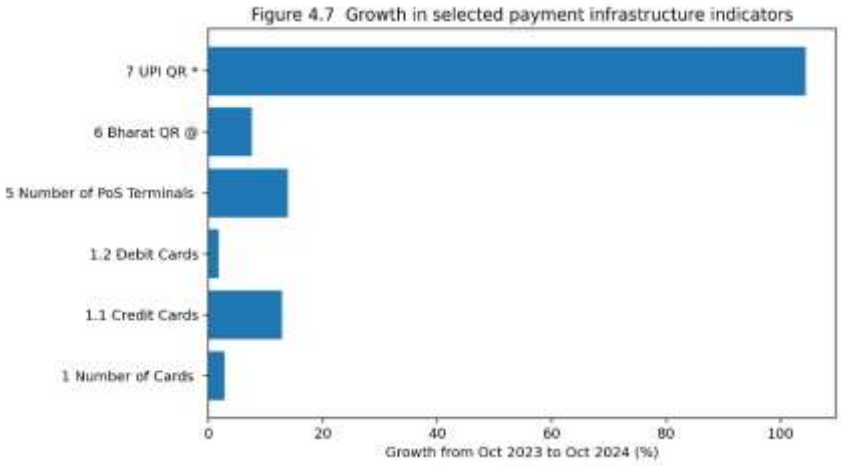


Figure 4.4 Growth in selected payment infrastructure indicators from October 2023 to October 2024

Interpretation: Among the selected retail channels, UPI accounts for approximately 86.7 percent of volume in October 2024. This confirms that India's retail digital payment ecosystem is highly concentrated around UPI. The infrastructure data reinforce this point: UPI QR installations grew very sharply between October 2023 and October 2024, signalling deeper merchant-side penetration and wider day-to-day dependence on QR-based payment acceptance.

This concentration is analytically important for fraud studies. When a payment ecosystem becomes heavily dependent on a single user interface and behavioural flow, fraud methods that exploit user confusion in that interface can scale nationally. QR-code fraud, collect-request scams, and fake payment confirmation flows become more consequential precisely because the platform is both ubiquitous and familiar.

4.3.3 Monthly domestic payment fraud trend

The domestic payment fraud section in the uploaded data provides monthly observations from September 2022 to October 2024. Although the series represents reported frauds rather than occurrence dates, it is still useful for understanding direction, peaks, and the intensity of fraud relative to the payment system.

Year	Coverage in available file	Months	Avg monthly fraud volume (lakh)	Avg monthly fraud value (Rs crore)	Avg FTS (bps)	Peak month in period	Peak fraud value (Rs crore)
2022	Sep-Dec only	4	1.77	232.50	0.12	November 2022	257.00
2023	Jan-Dec	12	2.21	319.58	0.16	December 2023	432.00
2024	Jan-Oct	10	2.48	452.70	0.19	May 2024	545.00

Source: Computed from uploaded Data.csv (domestic payment fraud statistics). 2022 and 2024 are partial-year coverage within the available file.

Figure 4.3 Monthly domestic payment fraud trend, Sep 2022 to Oct 2024

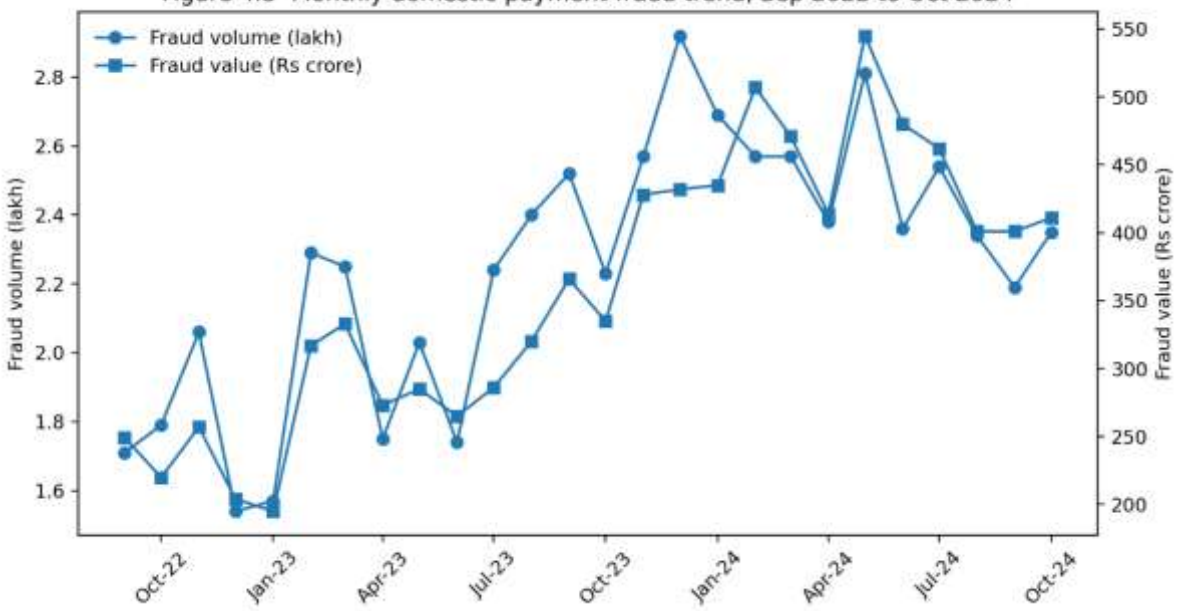


Figure 4.5 Monthly domestic payment fraud volume and value, September 2022 to October 2024

Figure 4.4 Fraud-to-payment value ratio (FTS), Sep 2022 to Oct 2024

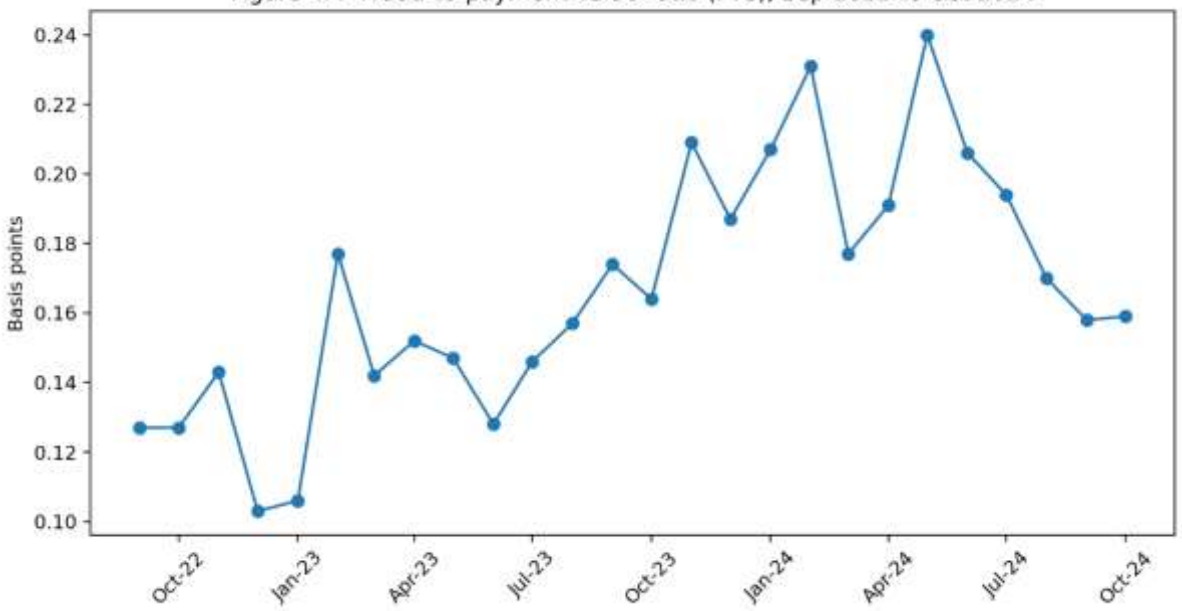


Figure 4.6 Fraud-to-payment value ratio (FTS) in basis points, September 2022 to October 2024

: The trend is upward over the available period. Average monthly fraud volume rises from 1.775 lakh in the partial 2022 segment to 2.209 lakh in 2023 and 2.480 lakh in the January–October 2024 period. Average monthly fraud value similarly increases from about ₹232 crore to ₹320 crore and then ₹453 crore.

The highest value within the available series occurs in May 2024, when reported domestic payment fraud reaches ₹545 crore. The FTS measure also trends upward from an average of 0.125 bps in the partial 2022 segment to 0.193 bps in 2024. This indicates that fraud is not merely rising in absolute value because payments are growing; its ratio to payment value is also showing stress at several points in the series.

At the same time, the file itself notes that reporting is based on when frauds are reported and does not include attempted frauds. Therefore, the figures should be read as trend indicators rather than as perfect real-time incidence counts. Even with that caution, the broad pattern remains clear: as digital payment activity expands and penetrates more user segments, the opportunity structure for fraud also widens.

4.4 Objective 3: Key vulnerabilities within the FinTech ecosystem

The third objective moves from trends to causation. The question is not only whether digital payments and related FinTech channels have grown, but why fraud risk remains persistent within that growing ecosystem. The study conceptualises vulnerability at four interconnected levels: user, platform or technology, institution, and regulation or enforcement.

Layer	Key vulnerabilities	How the vulnerability translates into fraud risk
User level	Low awareness, unsafe credential sharing, delayed reporting, impulsive approval behaviour	UPI collect-request scams, QR-code scams, phishing and fake customer-care frauds succeed because the user is persuaded to authorise the fraud.
Platform / technology level	Interface confusion, weak warnings, risky permissions, insufficient fraud detection, authentication weaknesses	High-volume UPI ecosystems and app-based lending interfaces can scale the effect of design weaknesses; weak warning design raises social-engineering success.
Institutional level	Complaint-handling delays, weak mule-account controls, fragmented response chains	Even after the fraud occurs, delayed blocking, weak tracing, or poor coordination with banks/FinTechs/payment intermediaries increases loss severity.
Regulatory / enforcement level	Reporting gaps, delayed response, accountability ambiguity, slow adaptation to new modus operandi	Fraud patterns change faster than reporting and enforcement systems; partial or delayed reporting blurs the real-time fraud picture.

Source: Author's layered vulnerability map synthesised from the study objectives, literature review, and interpretation of payment system data.

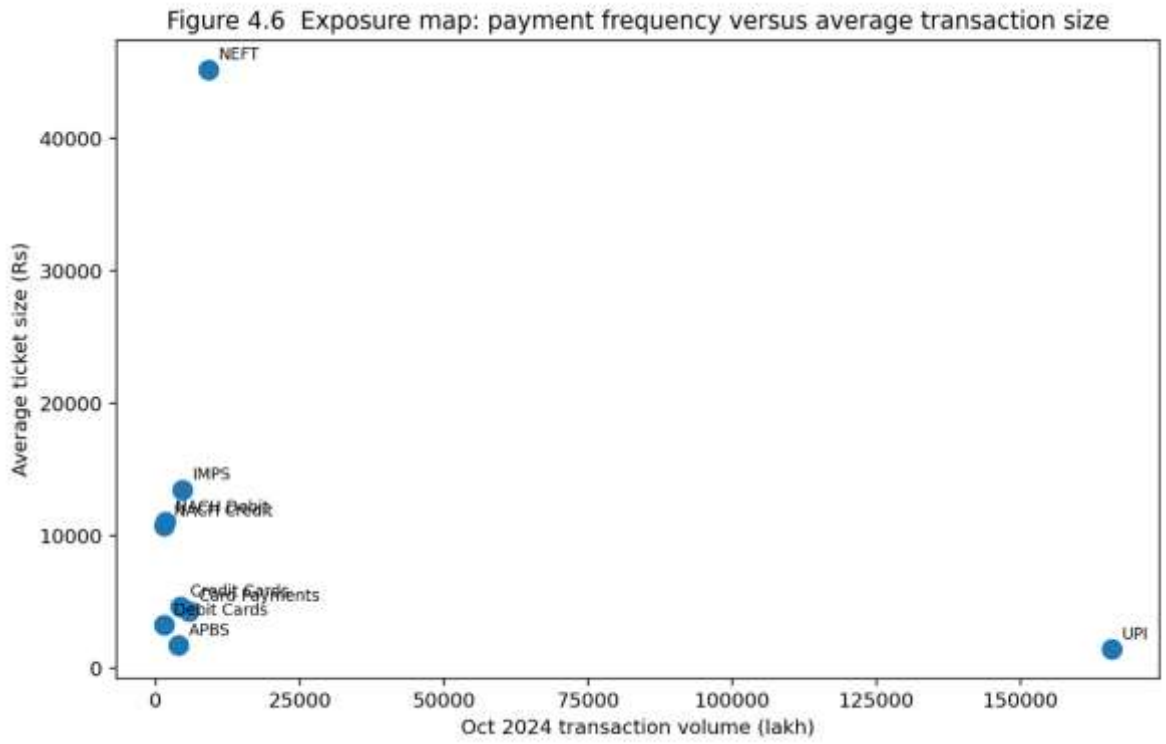


Figure 4.7 Exposure map: transaction frequency versus average transaction size (October 2024)

Interpretation: Figure 4.7 helps link payment-system characteristics to fraud vulnerability. UPI sits at the extreme high-frequency end with a relatively low average ticket size of about ₹1,417. This is the classic setting for large-volume social-engineering frauds in which many relatively small-value authorisations can cumulatively generate significant losses. IMPS and NEFT, in contrast, sit at higher average ticket sizes, which makes them more suitable for targeted account-compromise or takeover attacks where the criminal seeks fewer but larger extractions.

The layered map and the exposure chart together suggest that FinTech fraud in India is best understood as a systems problem. User awareness alone cannot solve a problem that is also shaped by interface design, warning quality, bank response speed, mule-account monitoring, and regulatory coordination. Fraud persists when weaknesses at different levels reinforce one another. A confused user, a weak warning screen, delayed complaint handling, and fragmented reporting can combine to produce a successful fraud even when any one layer by itself appears adequate.

4.5 Consolidated findings for the chapter

First, the evidence supports the paper's fourfold fraud classification: social engineering, technical frauds, identity-related frauds, and transaction or platform-related frauds. Second, the payment-system data show that India's digital finance ecosystem has expanded rapidly, with UPI dominating transaction volume and infrastructure growth. Third, the domestic payment fraud series indicates a rising pattern in both fraud volume and fraud value over the available period, alongside an upward movement in the fraud-to-payment value ratio. Fourth, vulnerability is layered rather than isolated. Fraud risk rises not simply because technology exists, but because technology, user behaviour, institutional response, and regulatory adaptation do not always move at the same speed.

Overall, Chapter 4 demonstrates that the growth of digital finance in India has strengthened convenience and inclusion, but it has also enlarged the exposure surface through which fraud can be attempted and scaled. The empirical data therefore support the central argument of the paper: FinTech fraud is not just a technological disturbance but an ecosystem problem emerging from the interaction of channels, actors, and vulnerabilities.

4.6 Result and Discussion

According to findings, the FinTech fraud in India is not a single-category problem. It rather a multi-dimensional problem which operates across digital payments and e-banking channels and digital lending environment. The classification from this study groups the major frauds into a social engineering fraud, technical fraud, identity fraud, and

transaction/platform fraud. Classifying fraud events is crucial as they generally do not occur through only one mechanism. In practice, a fraud starts with some kind of misrepresentation, followed by a compromise of identity and eventually an unauthorized transaction or use of the platform.

The expansion of India's digital financial ecosystem has created bigger opportunity structures for fraud, the study further finds. The dataset deployed in Chapter 4 depicts an impressive growth of major payment channels between October 2023 and October 2024. Notably, UPI shows high transaction growth and continues to lead the payment volume. It shows fraud's risk shall be analysed along with ecosystem expansion. As the size of a digital payment system expands, as it becomes more widely used, the number of user touchpoints, transaction opportunities and scope for success at scale of frauds based on deception grows.

The yearly and monthly trend indicators on the domestic payment fraud, in the data set, also shows uptrend. The average monthly fraud volume has increased from partial 2022 to 2023 and in January–October 2024 period further. The value of fraud also rose sharply during the period while the fraud-to-payment value ratio (FTS) movement was up. The importance of this finding is that fraud is not only rising in absolute numbers as a result of overall growth in payments, but the stress is showing also in terms of fraud intensity against payment value. The monthly series that can be constructed shows the peak fraud value is in 2024. This strengthens the story that the fraud problem remains persistent and particularly financially material as the payment landscape grows.

A key takeaway from the analysis is that in today's fraud landscape, UPI is the main focal point. According to the dataset, UPI is the most dominating channel in terms of volume of transactions selected payment. analytically crucial for this concentration When one payment interface is entrenched in day-to-day financial life, fraud which relies on behavioural confusion within the one interface can spread more easily. Frauds that use social engineering to exploit payment systems with high ticket sizes, such as UPI, are relatively low risk and very low ticket. When scaled up, frauds that in themselves are quite small can cause very large cumulative losses. In contrast, NEFT and IMPS have a higher average transaction size, resulting in greater relevance in targeted compromise of bank accounts where the size of successful breaches, albeit fewer, could still be material.

Moreover, the finding shows that the persistence of FinTech fraud cannot be explained through consumer negligence alone. The vulnerability map in Chapter 4 depicts a layered fraud risk structure at four levels: user, platform or technology, institution, and regulation or enforcement. Fraud in online banking is made easy because the user level of awareness is low, and users share their credentials unsafe. At the platform level, confusing interfaces, weak warnings, and inadequate fraud detection design increases the likelihood of users unwittingly authorising fraudulent transactions. The Institutional-Level Weaknesses Mule-account monitoring is ineffective. Complaint-handling is delayed. Response chains are fragmented. These worsen the losses after fraud. At the regulatory level, there are gaps in reporting and delays in enforcement and the failure to keep pace with changing fraud methods weaken deterrence and distort the real-time picture.

The discussion makes it clear that FinTech fraud in India is best understood as an ecosystem issue. Fraud events are not caused solely by any one actor or weakness. Instead, user manipulation, design limitations, institutional response gaps and regulatory lag interact to produce harmful consequences. For this reason, isolated solutions are not likely to be effective. Although consumer awareness is vital, it is insufficient. In a similar vein, technology may help, but it cannot substitute for swift complaint handling, better monitoring of suspicious accounts, better reporting and enforcement mechanisms.

In essence, the findings validate the core argument of the research. It states that India's digital finance growth is enhancing convenience and inclusion, simultaneously expanding the surface through which FinTech fraud can occur, scale, and monetize. As use of payment systems increases, we also see that domestic fraud indicators keep on rising as well. Together these two observations suggest that fraud risk grows with digital adoption and unless the safeguards in the ecosystem evolve in tandem, they will not be very effective.

RECOMMENDATION

Given the thorough examination of the FinTech ecosystem, and the vulnerabilities identified at user, platform, and institutional levels, the following recommendations are proposed:

Consumer Preparedness and Behavioral Resilience:

- **Practical Capability Building**: The authorities and financial institutions must not restrict themselves to generic awareness slogans but rather focus more on practical capability building.
- **Multidimensional Preparedness**: Consumer preparedness should refer to awareness of risk, active protection practices, and post fraud event response and should consist of three-dimensional capabilities.
- **Response Habit Formation**: Training should focus on cultivating habits that will help in minimizing the 'golden hour'. Such habits include first reporting the matter immediately, freezing the transaction, and escalating the issue formally.

Technological and Platform Fortification

- **Advanced Detection Systems**: To improve the integrity of all transactions, the ecosystem should utilize advanced detection systems based on anomaly detection and smart contracts enabled by Blockchain.
- **Multidimensional Preparedness**: Developers of payment apps must ensure that protocol and implementation flaws are managed through design choice. This must prevent the creation of repeatable opportunities for scammers as the user base scales.
- **Response Habit Formation**: The interface of platforms should embed interactive cues, warns and behavioural safeguards which prevents impulsive and / or coerced approval of payments by users.

Institutional Coordination and Data Governance

- **Real-time Response Networks:** There is a strong need for banks to strengthen the coordination with fintech, telecom networks and payment intermediaries for a real-time response to fraud reports.
- **Systematic Fraud Registration**: Institutions must develop uniform processes for collecting, sharing, and utilizing fraud data in advance as a conduct governance tool rather than merely post-fact.
- **Mule Account Controls:** Banks and payment service providers must enhance their monitoring and control of mule accounts to hinder the routing and layering of stolen funds.

Regulatory and Legal Reforms

- **Clearer Liability Allocation**: Legal rules need to be clarified about allocation of liability and compliance requirements to ensure consumer protection and restore confidence when system failures occur.
- **Unified Reporting Standards**: Reporting standards should be unified to close existing gaps. This can be achieved through a fragmented data-sharing approach by regulators that allow for a consistent, year-on-year analysis of the national trends.
- **Algorithmic Accountability**: The digital lending industry should be subject to tighter regulation of platform management and algorithmic practices. These rules should aim to minimize exploitative actions and harmful user consequences.

CONCLUSION

The study is looking at FinTech frauds in India through three objectives which are classification of major kind of frauds, historical and year-wise fraud pattern analysis and ecosystem vulnerabilities analysis. Fintech frauds in India, according to the analysis, have a broad scope and comprise social engineering frauds, frauds of technical nature, identity-related frauds, and transaction or platform-related frauds. While analytically useful, these categories often become overlapped in practice, which tells us that fraud is not a linear occurrence but rather a layered affair which consists of deception, tech use, identity misuse and platform abuse.

According to the trend analysis based on the uploaded dataset, India's digital financial ecosystem has seen robust growth, primarily through UPI and associated payment infrastructure. Meanwhile, domestic payment fraud indicators show that

over the available period, fraud volume, fraud value, as well as fraud intensity are on the rise. It indicates that any growth in digital payments not only enhances financial inclusion and convenience of transactions but also increases the extent and frequency of fraud exposure in the system.

The continued emergence of FinTech fraud can also be attributed to the vulnerabilities of the ecosystem. The risk of fraud arises from the interplay of low user awareness, unsafe transaction behaviour, weaknesses in interface and warning, weak institutional response mechanisms, mule-account risks, delayed reporting, regulatory non-coordination etc. As such, one cannot think of FinTech fraud as merely a technical failure or a one-off criminal event. The problem originates in many places from the interactions between users, platforms, financial institutions, and enforcement structures.

To sum up, the research confirms that FinTech frauds are becoming increasingly important in India as digitalization of finance expands. The issue is not simply about the occurrence of fraud, but also about trust, responsibility, and resilience in the digital world. Getting a safer FinTech environment in India would require a combined approach of greater consumer preparedness, more secure and intuitive design of platforms, faster systems of institutional response and a more adaptive regulatory and enforcement coordination system. With a layered approach we can optimise benefits of digital finance and keep fraud risks from growing without control.

REFERENCES

1. Renuka Kumar; Sreesh Kishore; Hao Lu; Atul Prakash (2020) — *Security Analysis of Unified Payments Interface and Payment Apps in India*.

2. Simran Kaur; Himanshu Mishra; Anuj Goyal (2023) — *Cyber-Security in UPI Payments*.

3. Shruthi M K; Ramesh B E; Harshitha N H; Nischitha Pateel H; Pavitra D; Srushti Ragi C (2025) — *UPI Fraud Detection Using Machine Learning*.

4. S. Kavitha; V. Ashwini; A. Immaculate; A. Kiruthiga; P. Kiruthiga; K. Kowsalya; G. L. Vijayalakshmi (2024) — *Fraud Detection in UPI Transactions Using Machine Learning*.

5. Srikrish Santhosh; Tanisha Parvatikar (2024) — *Fortifying Digital Payments: Responding to UPI Frauds by Leveraging AI and Blockchain Technology*.

6. Neha Priya; Jawed Ahmed; M. Afshar Alam (2020) — *Digital Payments: A scheme for Fraud Data Collection and Use in Indian Banking Sector*.

7. Ashish Sharma; Dr. Yogender Singh (2024) — *Cyber Frauds In India's Digital Payment Ecosystem: Risk, Impacts, And Regulatory Responses*.

8. Arkajit Debnath; Raghunath Chakraborty (2023) — *Phishing and Vishing Attacks: An Emerging Pitfall of Fintech World*.

9. Divya Ramesh; Vaishnav Kameswaran; Ding Wang; Nithya Sambasivan (2022) — *How Platform-User Power Relations Shape Algorithmic Accountability: A Case Study of Instant Loan Platforms and Financially Stressed Users in India*.

10. Akbar Ali; Vijaya B. Marisetty (2023) — *Are FinTech lending apps harmful? Evidence from user experience in the Indian market*.

11. Mora Saritha (2023) — *Demystifying the misery behind loan apps in India*.

12. A. Lekshmi; J. Atul; Adith J. Pillai; M. Dhanya; Sanju Kaladharan (2025) — *Risks in Instant Loan Apps: Analyzing User Perceptions Using Machine Learning Approach*.

13. Mohammed Afzal; Mohd. Shamim Ansari; Naseem Ahmad; Mohammad Shahid; Mohd. Shoeb (2024) — *Cyberfraud, usage intention, and cybersecurity awareness among e-banking users in India: an integrated model approach*.

14. Sumit Mishra; Rajeev Kumar Singh (2025) — *E-Banking Frauds in India: Critical Analysis*.

15. Nikita Johri (2022) — *E-Banking Frauds and Safety Solutions: Analysis*.

16. Dr. Rakhi Tiwari; Prof. Dr. Vivek Sharma (2021) — *Digital Banking: A Study of Fraudulent Practices in Indian Banking Sector*.

17. Anwesha Chakraborty (2024) — *Cyber Security Threats In Indian Banking Sector And Implementation Of AI As A Preventive Measure*.

18. Ameya Lonkar; Sonali Dharmadhikari; Neha Dharurkar; Kanchan Patil; Ravi Ashok Phadke (2024) — *Tackling digital payment frauds: a study of consumer preparedness in India*.

19. Dr. Roshan Lal Rohilla (2024) — *Legal Issues Involved In Electronic Payments System in India*.

20. S. Aziz; M. Dowling (2019) — *Machine learning and AI for risk management*